Design and Evaluation of a New Handoff Protocol in IEEE 802.11 Networks

Erik Weiss*, Arif Otyakmaz*, Eva López* and Bangnan Xu+

* : Communication Networks, Aachen University of Technology, Kopernikusstr.16, D-52074 Aachen, Germany

+: SSC ENPS (Technologiezentrum), T-Systems, Am Kavalleriesand 3, D-64295 Darmstadt, Germany

Ph: +49 241 8028575, Fax: +49 241 8022242, Email: erik.weiss@comnets.rwth-aachen.de

***Abstract*: Nowadays IEEE 802.11 is the most used WLAN standard. Many hotspots composed of many different Access Points (AP) are deployed today. 802.11b varies between 2-11Mbs. The next step is 802.11a/g, supporting data rates up to 54Mbps. 802.11a/g is based on more complex coding schemes to ensure high data rates. The physical layer improves but the protocol basics are the same since legacy 802.11. This paper presents a detailed analysis of the handover mechanisms described in the IEEE 802.11 standard. Based on the analysis we present an enhanced handover mechanism, utilising the wired infrastructure and the gained knowledge about the neighbourhood. We present an approach called "Cooperated Handover Control" (CoHCo). This paper compares CoHCo with the basic handover methods of IEEE 802.11 by computer simulations.**

1. Introduction

The number of hotspots increases permanently, many city centres all over the world are already covered by hotspot technologies. Internet access is becoming increasingly important. Furthermore, the trend is towards the wireless world, providing public access to the Internet via wireless devices at high data rates. The widest distributed Wireless Local Area Network (WLAN) product 802.11 is standardized by the Institute of Electronics and Electrical Engineering (IEEE). IEEE 802.11b/g works at the 2.4 and 802.11a works at the 5 GHz band. IEEE 802.11a/g supports transmission rates up to 54 Mbps. Due to the high attenuation at 5 GHz the coverage is limited. Hence, the installation of a large number of access points is necessary to cover a city centre. To maximize the performance of the built infrastructure and to minimize the destructive influence of the neighbour AP, each AP within coverage uses a different frequency. This paper analyzes the current IEEE handover mechanisms based upon IEEE 802.11a and compares them with the newly developed CoHCo approach. The 5 GHz unlicensed band comprises frequency bands between 5.15 GHz and 5.825 GHz. A spectrum of 300 MHz has been released in the U.S. for the Unlicensed National Information Infrastructure (U-NII) band. A spectrum of 455 MHz is available in Europe. Different centre frequencies f_c are defined for the 5 GHz unlicensed band. In the U.S., three U-NII bands are defined between 5.15 GHz and 5.825 GHz leading to 12 frequency channels for operation (cf. Figure 1). In Europe, current regulations allow the operation of wireless LANs at 19 frequency channels in the two defined frequency bands between 5.15 GHz and 5.725 GHz [1][2]. European hotspots using 802.11a may use up to 19 frequencies to establish a maximum coverage. The 5 GHz band for wireless LANs in Japan is set between 5.15 GHz and 5.25 GHz. Fig. 1 shows the 5 GHz IEEE 802.11a spectrum allocation.

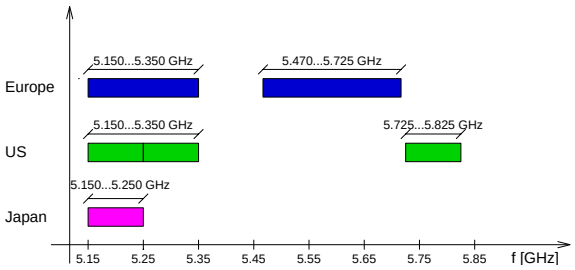

Figure 1: IEEE 802.11a spectrum allocation

A user carrying his mobile device crosses several different cells, while moving around, e.g. as pedestrian, car driver or taking a bus. Whenever the user departs from a cell, the connection towards the current AP interrupts. The mobile device must change from the current AP to another AP within its range.

While changing the user experiences an interruption. The standard handover interruption varies between around 2.5 and 0.5 seconds. The handover interruption depends on the number of available frequencies and the handover approach. Many city centres accommodate a WLAN hotspot and particular in urban environments the connection conditions change very fast. The goal of WLAN hotspot deployments is to cover as much area as possible providing line-of-sight conditions. Line-of-sight conditions enable in most cases a good connection quality. However, when the user turns around a corner, and loses line-of-sight to the access point, the connection is interrupted and will drop shortly after. Most handover approaches start searching for a new AP when the old connection is lost. To recognize a connection interruption introduces already large delays. The new CoHCo approach presented in this paper limits the search to the neighbour APs and allows a smooth change from the old to the new AP with minor interruptions, if any.

2. IEEE 802.11

IEEE 802.11a describes an OFDM PHY layer at 5GHz [3]. The Medium Access Control (MAC) layer is equal to 802.11b and legacy 802.11. 802.11a mainly introduces higher data rates. IEEE 802.11a offers eight coding and modulation schemes, so called "PHY Modes". The MAC protocol used in IEEE 802.11 is called Distributed Coordination Function (DCF). 802.11 describes also a Point Coordination Function (PCF). PCF is used for centrally controlled access. However, no vendor ever implemented it. The DCF is based on carrier sense multiple access with collision avoidance (CSMA/CA). As mobile stations (STA) are not able to monitor the air interface while transmitting, the DCF uses backoff and request/clear to send (RTS/CTS) mechanisms to avoid collisions due to hidden stations.

2.1 IEEE 802.11 Handover Mechanisms

The handover on link layer comprises four main steps:

1.) The terminal must recognize the lost connection
2.) Scanning for new APs
3.) Authenticate with the chosen AP
4.) Associate with the chosen AP

A terminal looking for an access point firstly has to undergo the scanning phase. During the scanning time the terminal checks all valid frequencies for activity. The terminal scans all frequencies, unless it finds an AP. If the terminal discovers several APs, the AP with the strongest signal will be chosen. This concludes the scanning phase and the node starts to authenticate and to associate with the AP.

2.1.1. Passive Scanning

In passive scanning the stations are informed of the existence of APs by Beacons which are sent by the APs periodically. A Beacon consists of the AP's Basic Service Set Identifier (BSSID) and Service Set Identifier (SSID), likewise information about the supported PHY Modes. In passive scanning a STA listens to each channel at least once and stay on the same channel until it either receives a Beacon or has listened to the same channel for the duration of a Beacon period (the time between two Beacons). After that the STA starts to listen to the next channel. In Figure 2 (a) the station changes to frequency A waiting for a Beacon. After the reception of the Beacon, the station changes to frequency B. At station A the station has only to wait a small fraction of 100ms (Δ_1). But at frequency B the STA must wait almost 70% of 100ms (Δ_2). This way the STA gathers information about all the APs and how well they are heard. According to the strength of the Beacon signal the STA chooses its new AP and starts authorisation / association.

2.1.2. Active Scanning

In active scanning the STA broadcasts a Probe Request on each frequency, in hope of receiving Probe Responses from the APs in the nearby vicinity. Probe Response frames have similar structures and information as Beacons. The active scanning process consists of the following sub tasks:

- A STA changes to a new frequency and waits a Probe Delay to make sure that the frequency is not active.
- The STA sends a Probe Request as broadcast.
- The STA stays on the channel for the length of MinChannelTime that is recommended to be less than 1 msec in [9]. If the STA does not notice any activity on the channel, it starts the active scanning on the next channel. If the STA has detected activity on the channel, it listens to the channel for the duration of MaxChannelTime, defined in [9] and gathers all the information from the received Probe Response frames.

An example of active scanning is depicted in Fig. 2 (b), where after changing to frequency A the station waits a Probe Delay before sending a Probe Request. The detection of activity, due to the Probe Response

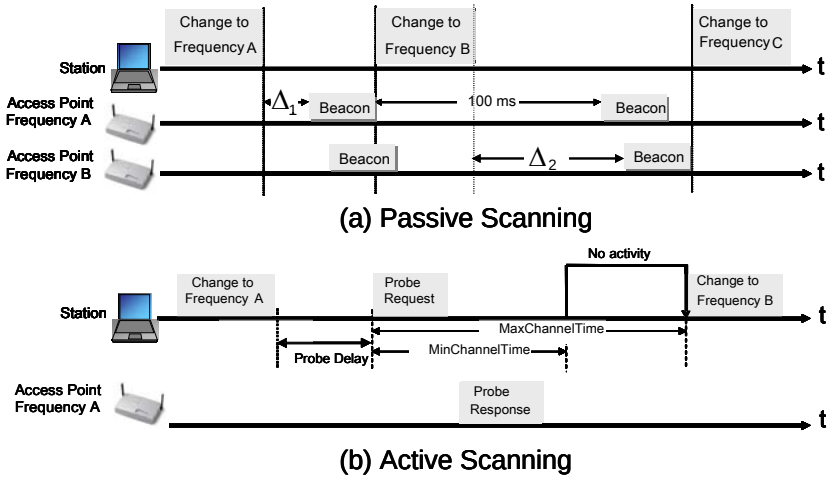

Figure 2: Different Scanning Methods in IEEE 802.11

of the Access Point, causes that the station remains on frequency A for *MaxChannelTime* waiting for further responses from other APs. After the STA has scanned all available frequencies, it chooses the AP with the strongest received signal. If no AP was found the STA continues the scanning process until it discovers an available AP.

2.1.3. Authentication and Association

After the scanning process the STA must first authenticate with the AP and afterwards associate as depicted in Figure 3.

The 802.11 standard specifies two authentication algorithms: “open system” and “shared key”. The open system is the default authentication and equals the null authentication algorithm. It involves the exchange of two frames, while the shared key algorithm requires a four step transaction. Measurements have shown that the execution phase of the authentication is in general slightly over 1 ms. Thus reducing the execution phase using pre-authentication will not significantly reduce the total handover time [7].

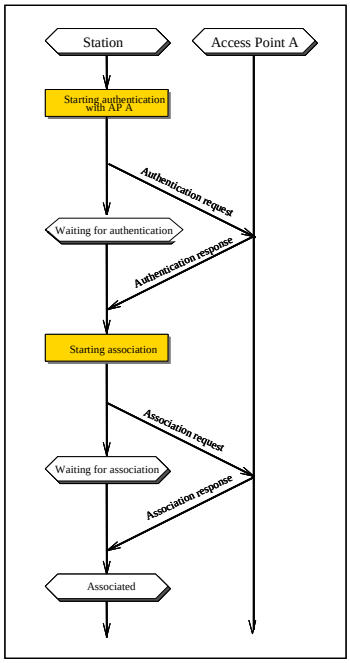

Figure 3: Open authentication and association

Once the authentication has completed successfully, the STA can associate with an AP. A STA can be associated with no more than one AP at the same time. This ensures that the distributed systems can track with which AP the STA is currently associated. Hence, frames destined for the STA can be forwarded to the correct AP. The association is performed in two steps.

First the STA sends a management frame called Association Request. There are four information elements in the body. First, the Capability Information that indicates if the STA is pollable. Second the Listen Interval is used to indicate to the AP how often a STA awakes to listen to Beacon management frames. Third, the Service Set Identity (SSID) indicates the identity of an Extended Service Set (ESS) or an Independent BSS. And fourth, the Supported Rates describe a single supported rate in units of 500kbps.

The AP processes the Association Request and responds with an Association Response. It has four information elements. First, the Capability Information indicates if the AP acts as a point coordinator, with or without polling. Second, the Status Code indicates the success or failure of the Association Request. Third the Association ID (AID) represents the 16-bit identifier of a STA. And fourth, the supported rates are described.

After these steps are fulfilled the station performs its handover and is able to send and receive data again. Our investigations show that most of the handover time is consumed while scanning for an appropriate AP. Passive scanning and as well active scanning exceed the limit for real-time or voice-over-IP traffic. The main reason is the large number of possible frequencies. Mishra at all [7] have presented a proactive caching approach, which introduces neighbour information. Also the IEEE 802.11 task group k “Radio Resource Measurement Enhancements” [8] investigates the potential of Neighbour Reports that contain information on APs, which are roaming candidates for STAs. The terminal requests to its associated AP a Neighbour Report of a specific SSID that indicates an ESS within the administrative domain of the associated AP. The information contained in the Neighbour Reports is recommended in [8] and the IEEE 802.11k working group to be accomplished by:

- Configuring an AP with a list of BSSIDs that are neighbours.
- Utilizing Beacon reports in order to determine which APs can be heard by STAs in a certain service area.

The Beacon reports are sent by a STA informing about the conditions of received Beacons for a BSSID like received channel power, Beacon Interval, channel number.

3. Cooperated Handover Control

The approach we use is similar to the topics discussed in the 802.11k group. The handover with CoHCo is only possible between APs belonging to the same ESS. Whenever a terminal performs a handover between APs belonging to the same ESS, the terminal informs its new AP about the MAC Identifier of its old AP. Thus, the new AP is able to inform the old AP about its settings. This information includes MAC Identifier, the frequency, the current AP time, the beacon interval, the frequency of extended Beacons, the work load supported by the

AP and the AP provider.

The new AP collects the settings of the old APs in its table of neighbouring APs. Each AP broadcasts a special Beacon, called Extended Beacon, which includes its table of neighbouring APs, additionally to the usual information contained in a Beacon. The sequence of the neighbour APs within the neighbour list of the Extended Beacon starts from the neighbour whereto most terminals change. The sequence in the list represents the commonness of an AP as destination for a handover. The Extended Beacons are sent in regular intervals. The frequency of these Extended Beacons has to be chosen considering the deployment area; in particular the speed of the stations is important for the extended Beacon interval. Environments with faster terminals (e.g. a street scenario) need a higher frequency of extended Beacons because they perform handovers more frequently than slower terminals. Each terminal stores the table of neighbour APs after the reception of an extended Beacon from the current AP. After the association with a new AP the terminal erases its old table of neighbour APs. The searching for neighbour APs starts when the terminal receives a Beacon with signal strength lower than a certain limit, called P_{lim}. The terminal starts to check all neighbours from the list in descending order.

$$P_{lim} < P_{current} \qquad (3.1)$$

The found signal strength of the neighbour AP's Beacon, P_{found} is compared with the signal strength of the current AP's last received Beacon, called $P_{current}$. The search for neighbour APs is performed according to the table of neighbour APs, as long as one neighbour AP is received with a signal strength 3dB stronger than the current AP (cp. Figure 4). When the STA receives an AP with 3dB stronger signal strengh than its current AP (cf. (3.2)), its starts authentication and association with this AP:

$$P_{found} > P_{current} + 3dB \qquad (3.2)$$

After finishing the first search without finding an AP that fulfils the power requirements, the search threshold is adapted.

$$P_{lim} = P_{min} - 3\ dB. \qquad (3.3)$$

To avoid unnecessary scannings the new threshold is reduced by 3dB (cf. (3.3)). However it might happen that under high load conditions the beacon is shifted or collided, thus the CoHCo approach might fail under high load conditions. When CoHCo scanning fails the passive scanning is used as fall back solution.Figure 4 shows the signal strength received by a terminal from AP 1, with which it is currently associated and from neighbour AP 2, included in the terminal's table of neighbouring APs. When the signal strength of the AP 1 is less than P_{min} (3.1) the terminal looks for AP 2, but P_{found} does not fulfil (3.2), then no change to AP 2 is performed. The terminal looks for AP 2 again, but now when the signal strength fulfils (3.3). The second time, P_{found} fulfils (3.2) and therefore a handover to AP 2 is performed.

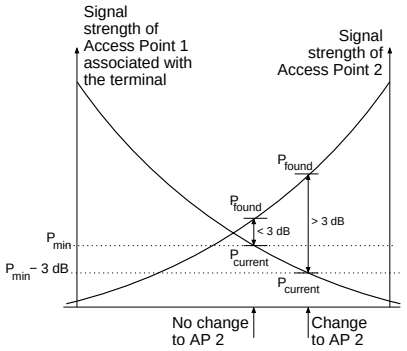

Figure 4: CoHCo Decision

For each neighbour AP included in the neighbour APs table a STA calculates when the adjacent AP will send its next Beacon. The calculation bases on the information included in the extended Beacon An example of searching for neighbour APs is shown in Figure 5. The STA is associated with AP 2 and changes first to frequency 1 expecting to detect the neighbour AP 1. Since the signal strength of AP 1 was not sufficient, the STA changes to frequency 3 expecting to detect the neighbour AP 3. After the Beacons of AP 1 and AP 3 are received the terminal returns to frequency 2 because the received Beacons did not fulfil the power requirements.

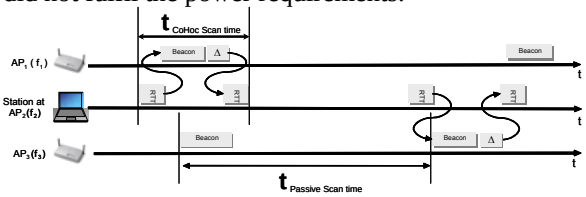

Figure 5: Control of the neighbour APs

Figure 5 shows how the search time is assembled for CoHCo. Each STA needs a certain time to change the frequency (receiver turn around time (RTT)). Plus the duration of the beacon and additionally a certain time frame in case that the beacon is delayed. Thus, the time on one frequency ($t_{CoHCO\ Scan\ Time}$) is composed of two RTT, plus beacon duration and plus a certain delta (Δ).

The old scan time ($t_{Passive\ Scan\ time}$) for passive scanning is one beacon period (100 ms).

4. Simulation Results

We compare active scanning, passive scanning and CoHCo by means of simulations. We present our results for two scenarios. First we start with a demonstration using a street scenario. Our scenario is composed of ten APs along a street placed every 100 meters. All of them are using different frequencies and belonging to the same Extended Service Set (ESS) as shown in Fig. 6. To avoid large scenarios and log simulation durations we reduced the transmission power to 50mW. The simulation tool bases upon a two-path propagation model over a reflecting surface [1]. We chose the propagation

factor gamma to ($\gamma = 2.8$), whereas $\gamma = 2.0$ represents line-of-sight.

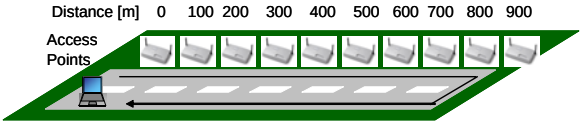

Figure 6: Street Scenario, 10 APs and one STA

One terminal moves with a speed of 2 m/s along the street and returns. The offered downlink traffic to the terminal is 6 Mbps constant bit rate (CBR) with a packet size of 256 bytes. Within our simulations the value P_{lim} to start the CoHCo search for neighbouring APs is set to 8 dB. Fig. 7 shows the number of missed packets along the terminal's distance, where the eighteen handovers can be observed.

Figure 7 presents all experienced handover on the way down the street and the way back. The first nine handover represent the way down and the second nine the way back. This emphasis the differences between the standard scanning approaches compared to CoHCo. At each AP exchange the handover using passive scanning loses around up to 8000 packets. The active scanning improves the situation but loses around 1000 packets also. CoHCo does not lose one packet due to the handover. In advance to the handover all three approaches suffer from the increased distance to the current AP. The link adaptation (LA) decreases the transmission modes and the offered load can not be submitted to the terminal. This effect is basically equal for all approaches, but CoHCo normally improves the situation since the handover is initiated earlier.

In Fig. 8 the detailed throughput over the distance is shown when a handover between two APs (changing from AP_4 to AP_5) is processed. Under good transmission condition the STA is able to receive the offered load. As soon as the STA is going to leave the cell the LA adapts the transmission modes to ensure the connectivity. This behaviour is similar for all three cases. Passive and Active scanning wait until the current connection fails and start the new scanning process afterwards. The drawback can clearly be seen in Figure 7. Whereas passive and active scanning loses completely the connection, CoHCo seamlessly switches from AP_4 to AP_5. The STA changes even before the LA must use the last applicable transmission mode BPSK ½[9].

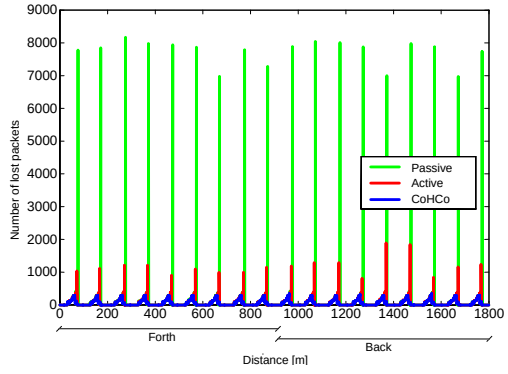

Figure 7:Number of Lost Packets per Handover

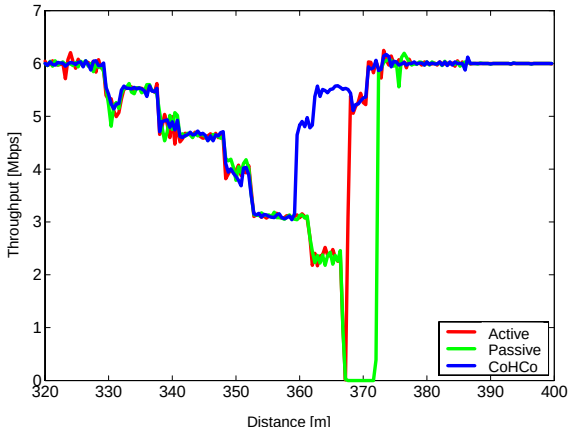

Figure 8: Detailed throughput for the handover between two different APs

The scenario described above represents best case assumptions. To test the CoHCo protocol under more realistic situations, we also evaluate our approach under high load conditions. The following scenario consist of four APs each operating on a different frequency. Again one terminal is moving down the street and returns. However this time each AP is associated with further STAs. These STAs are fixed and each is burdened with 500kbps downlink traffic, CBR with a packet size of 2300 bytes. We vary the number of additional STAs (0, 5, 7, 12, 15 and 20) per AP. Hence, each AP has to transmit up to 10Mbps. We evaluate the time without connection for one STA moving along the street with a speed of 10 m/s. The evaluated STA is burdened with 256 kbps, CBR with a packet size of 200 bytes. Figure 9 illustrates the simulated scenario.

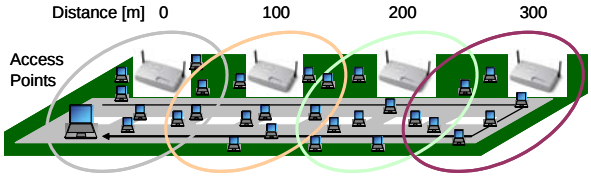

Figure 9: **Street scenario with background traffic**

The time without connection is understood as the duration between the last received packet before a handover is performed and the moment when the terminal finishes the handover. In Figure 10 the time without connection is compared between the three presented methods. In passive scanning the background traffic does not increase the time without connection noticeably. The passive handover takes up to 2.5 sec. On the other hand considering active scanning it can be observed that the background traffic influences the disconnection time which has an average value of approximately 0.4 sec. Whereas CoHCo allows to change APs with minor delays. CoHCo turns out to be sensitive to the background traffic. With 7.5 Mbps background traffic CoHCo fails with a probability of less than 5% and with 10 Mbps background traffic CoHCo fails with a probability of approximately 10%. The reasons are shifted beacons and disconnections based on

collisions. In case the connection is interrupted passive scanning is used as fall back solution. Thus a small percentage recognizes a link break and CoHCo was not able to search for AP before. Hence under high load situations some handovers take the same disconnection duration as passive scanning.

In most cases CoHCo provides a connection with minor and short interruptions. The cells are seamlessly changed.

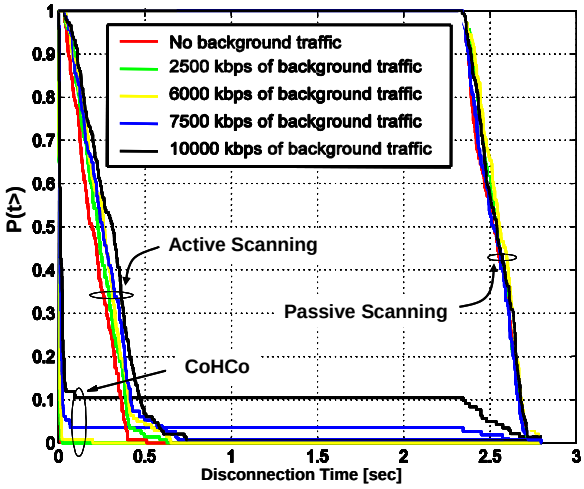

Figure 10: Complementary Cumulative Distribution Function (CCDF) of the Handover Delay with background traffic

5. Conclusions

In this paper the IEEE 802.11a handover procedure has been studied. IEEE 802.11 presents two different methods for the handover: active and passive scanning. A new method for the handover, the so-called Cooperated Handover Control (CoHCo) has been proposed. In the simulations CoHCo has been compared with active and passive scanning. The simulation results show that CoHCo is able to support mobility management on a very high level. In most cases CoHCo avoids large interruptions and provides a seamlessly handover. CoHCo out-performs in all cases the IEEE 802.11 handover mechanism.

6. Acknowledgement

This work was supported by T-Systems, Deutsche Telekom and the German research project IPonAir, funded by the German Ministry for Education and research (BMBF). The authors would like to thank the members of the project for the valuable discussion.

REFERENCES

[1] B. Walke, “Mobile Radio Networks”. New York, USA: Wiley & Sons Ltd., 1. ed., 1999.

[2] S. Mangold, “Analysis of IEEE 802.11e and Application of Game Models for Support of Quality-of-Service in Coexisting Wireless Networks”. Aachen, Deutchland: Wissenschaftsverlag Mainz, 1 ed. 2003

[3] IEEE LAN/WAN Standards Committee, “Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in 5 Ghz Band” IEEE Std 802.11a-1999, IEEE, New York, Nov. 1999.

[4] M. Engels. “Wireless OFDM Systems, How to make them work?” Boston, USA: Kluwer Academic, 2002

[5] E. Weiß, K. Kurowski, S. Hischke, B. Xu. “Avoiding Route Breakage in Ad Hoc Networks using Link Prediction”. Antalya, Turkey: International Symposium on Computers and Communications 2003

[6] G. K. Hector Velayos. “Techniques to reduce ieee 802.11b mac layer handover time”. Technical report, 4 2003.

[7] A. Mishra, M. Shin and W.A. Arbaugh, Context Caching Using Neighbor Graphs for Fast Handoffs in a Wireless Network, Infocom 2004

[8] IEEE LAN/WAN Standards Committee, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 7: Radio Resource Measurement” IEEE P802.11k / D1.0, New York, July 2004.

[9] IEEE, “IEEE Wireless LAN Edition - A compilation based on IEEE Std. 802.11 1999(R2003) and its amendments,” IEEE, New York, Standard IEEE 802.11, Nov. 2003.