Always Best Connected (ABC) in Wireless Car Communications:

Erik Weiss*, Guido Gehlen*, and Andreas Kemper*

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

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

Abstract*— *The last decade was dominated by the development of new radio access technologies. The development has been driven by the great success of the second generation mobile communication. Although the third generation (3G) mobile system just started, many existing and emerging access technologies will coexist for a long time. Following the introducing of the new communications techniques, a large variation of new services are developed. Some of these services address the area of vehicular communication. One part where mobile communication is of major interest is the car maintenances and repair services at the aftersales market. This paper presents a survey of efforts on the approaching mobile internet architecture and their relations to the next generation car communication. We present a simulation tool to investigate and plan the next generation mobile internet architecture deploying WLAN and GPRS/UMTS technologies. Traffic performance is evaluated in detail by means of stochastical simulations. The impact of the horizontal handover in IEEE802.11a and the vertical handover between IEEE802.11a and GPRS on the system performance can be seen from the simulation results.

***Keywords*— IEEE 802.11a, GPRS, Vertical Handover, Horizontal Handover, Simulator Technique**

1. Introduction

Nowadays the ability to communicate on the move is becoming common and less luxurious, especially for mobile businesses the communication is becoming more of a necessity. Currently, WLAN-based systems are emerging as a new means of public wireless access. 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 Mb/s. 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 whole street or 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 increases the need for solutions to integrate the existing public wireless access systems, cellular networks, and potential new access systems.

Third Generation Partnership Project (3GPP) was intentionally formed to specify a common set of 3G cellular system specifications on behalf of the European, U.S., Japanese, and Korean telecommunication standardisation organizations. 3GPP has produced the global specifications for the Universal Mobile Telecommunication System (UMTS). Although 2G technology can meet the needs of voice communications of the typical cellular subscribers, its data communication capabilities are very limited.

The third-generation (3G, UMTS) cellular systems promise a competitive data rate, up to 300kb/s initially and increasing up to 2 Mb/s, as the same as that of always-on connectivity of wired technology. Since 2.5G cellular data technology like GPRS/EGPRS is insufficient to meet market needs for data communications, and 3G cellular data is not yet fully deployed and accepted by the customers, mobile network operators are turning to wireless local area network (WLAN) technologies. To increase the acceptance and usage of the 2.5G data communication technology and to prepare the subscriber for UMTS it is commonly believed that operators must provide seamless roaming between cellular and WLAN access network. That is in particular important for services with the need for high throughput, high reliability and security requirements, e.g. vehicular communications. Wireless local area networks (WLANs) like IEEE 802.11a that work in the 5 GHz band and support transmission rates up to 54 Mb/s will be widely used for the wireless internet access [5] at hotspots like hotels, airports or fairs. Although the coverage is very limited due to the high attenuation, wireless data services are becoming increasingly popular but are, however not ubiquitous. Consequently it is natural to use high bandwidth data networks such as IEEEE 802.11 whenever they are available and to switch to an overlay service such as GPRS network with low bandwidth when the coverage of WLAN is not available. To achieve a large coverage for mobile internet it is necessary to combine WLANs with cellular systems like GPRS.

This paper presents a survey of enhanced mobile communication architecture. The paper bases upon two of our previous publications [18][19] and shows handover method in general. First we analyzes the current IEEE handover mechanisms based upon IEEE 802.11a and compare them with the newly developed CoHCo approach and second we give an overview about different integration architectures and their impact to the service. In section II a short description of WLANs is given and section three explains the proposed improvements. Section 4 reviews integration proposal for WLAN and cellular networks. Finally section five and six present the performance evaluation of horizontal and vertical handover based on simulation results. The paper is concluded with a discussion in the last section.

2. IEEE 802.11

IEEE 802.11a describes an OFDM PHY layer at 5GHz [2]. 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.

A. Passive Scanning

In passive scanning the stations are informed of the presence 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 1 (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.

B. 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 [5]. 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 [5] and gathers all the information from the received Probe Response frames.

An example of active scanning is depicted in Figure 1 (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 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.

C. Authentication and Association

After the scanning process the STA must first authenticate with the AP and afterwards associate. 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 [3].

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.
After the authentication is 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 [3] have presented a proactive caching approach, which introduces neighbour information. Also the IEEE 802.11 task group k “Radio Resource Measurement Enhancements” [4] 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 [4] 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.

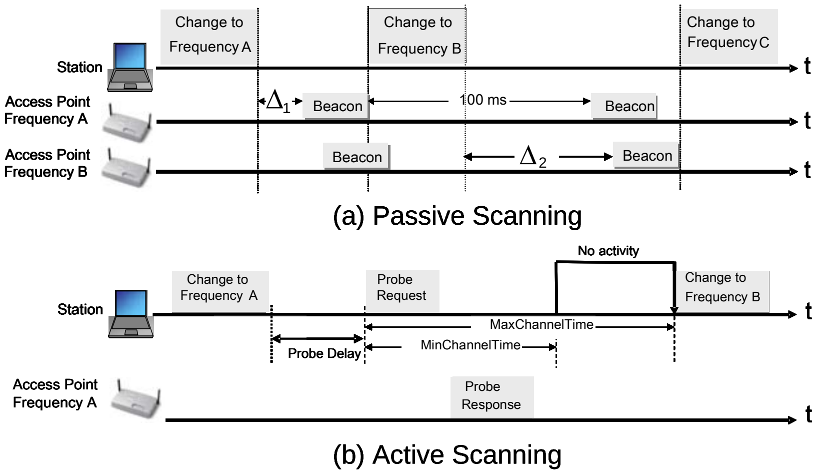

Figure 1: Different Scanning Methods in IEEE 802.11

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

Simulation results have shown that changing the AP takes a serious amount if time, especially if the mobile client is moving very fast, like a car. Thus cars will have problems to associate with an AP before they are again leaving the WLAN cell. Therefore, we emphasise the importance of fast handover for data communication to and from moving vehicles.

Thus, we propose a *Cooperated Handover Control (*CoHCO) approach 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 car on a street) need a higher frequency of extended beacons (e.g. each beacon) 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 detailed algorithm is shown in [19].

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 2. 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.

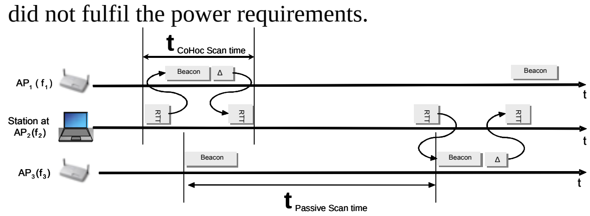

Figure 2: Control of the neighbour APs

Figure 2 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).

CoHCo enables fast cell changes in WLAN. A node /car learns about the neighbour AP of a cell, this enables the car to associate very fast with the next AP along the street.

4. WLAN and Cellular Data Networks

Cellular data networks provide up to 100~200kb/s that is a relatively low data rate, but with a very large coverage area. On the other hand WLANs like HiperLan/2 or IEEE 802.11a/g support a physical data rate up to 54 Mb/s. Further IEEE Working groups are even going toward much higher data rates; e.g. the 802.11n working group intends to have a data rate up to 1Gb/s. WLAN coverage is now only available at hotspot areas, the coverage may increase in the future but no complete coverage is expected.

Combining both systems means merging the strengths of both systems, high data rate at places with high user density and basic provisioning with cellular systems with large coverage even in rural areas. The key enabler is seen as the mobility support, user and respective terminals must be allowed to move

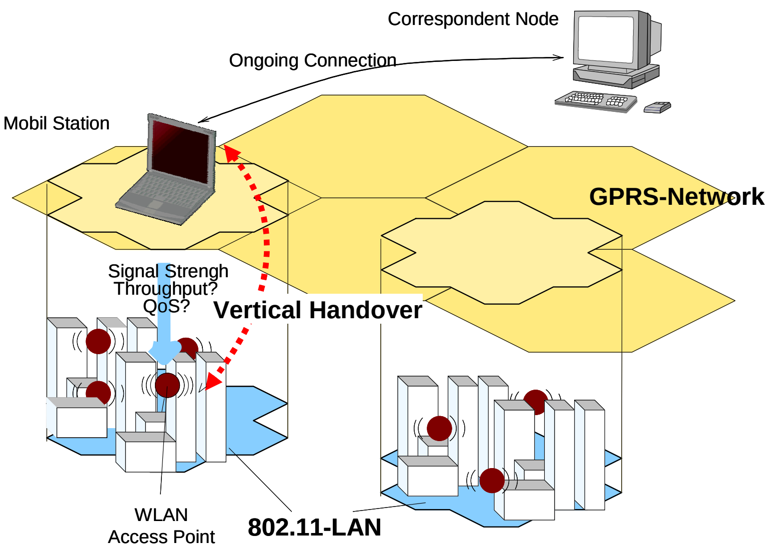

Figure 3: Architecture with WLAN and GPRS/UMTS

all around with a standard service support.

I. Keeping the Session while Moving

Session mobility is a step ahead pure roaming today common in GSM/GPRS. Existing IP data connections are secured, running applications can seamlessly be remain connected using IP mobility protocols.

D. Mobile IP

Mobile IP deals with the moving nodes and new IP addresses by mapping the newly created IP addresses to the original home IP address of the node. Each IP network needs an agent that provides the functionality of a home agent for terminals belonging permanently to this domain and supporting guest terminals as a foreign agent. A terminal at home could be reached simply by its IP address. If the terminal is attached as a guest to a foreign subnet with a different subnet IP, the node informs its home agent using a binding update (BU) message about its new location and about the new temporary foreign IP address. Thus the home agent can encapsulate and redirect packets targeted at the home IP address to the foreign IP address. Hence the node is still reachable via its home IP address and sessions set up to the home IP address are not interrupted while moving. Mobile IPv4 and Mobile IPv6 are basically similar, but Mobile IPv6 overcomes some drawbacks of Mobile IPv4. Both protocols are explained in detail in [10][11].
Furthermore extensions and enhancements [12][13] have been proposed introducing a hierarchy of agents to accelerate binding update signalling since the way to the home agent might be considerable long introducing high signalling latencies.

II. Application Scenarios

Several applications can benefit from hybrid architectures. The classical example is the email client that can skip to download a large file until a high rated WLAN is available. Streaming applications can benefit even more. During WLAN coverage a large part of the streaming data can be send in advance to the terminal. The only limiting factor is the terminal buffer. Since WLAN transmits date up to 100 times faster than cellular systems, the node is able to store during 10 seconds attached to a WLAN system data for approximately the next 15 minutes in advance. Another suited application might be a home office. While moving around, the subscriber works using a remote desktop connection, but the data is only temporarily buffered at his laptop and synchronisation with his home database is forced when WLAN connection is available. Whereas, during GPRS/UMTS connection only differential synchronisation is available.

III. Coupling Architectures

Several different coupling architectures have been present in the past. In Figure 4 five coupling points are presented. In [16] seven different integration ways are explained, although two are only business integrations ideas, like using the same bill for multiple systems but no real system integration.

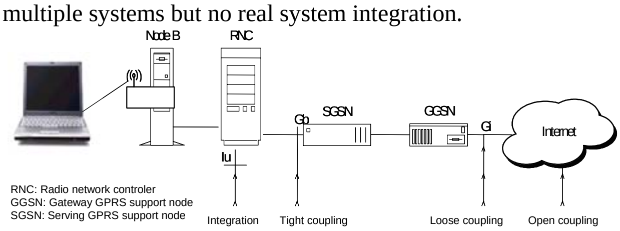

Figure 4: Different Coupling Points

E. Open Coupling

In this scenario there is no real integration between two or more access technologies. The WLAN and GPRS networks are considered as two parallel independent systems sharing a single billing scheme between them. A common database and separate authentication procedures (i.e. SIM based authentication for GPRS and simple user name and password for WLAN)[16].

F. Loose Coupling

This approach provides interworking between WLAN and GPRS at the Gi interface. The WLAN network is coupled with the GPRS network in the operator's IP network. In contrast to tight coupling, the WLAN data traffic does not pass through the GPRS core network but goes directly to the operator's IP network (and/or Internet) i.e. this approach completely separates the data paths in 802.11 and 3G networks. The high speed 802.11 data traffic is never injected into the 3G core network so the 3G backbone network could be left untouched.

G. Tight Coupling

A tight coupling architecture is proposed in [7] and provides 3GPP system based access control and charging i.e.

authentication, authorization, and accounting (AAA) for subscribers in the WLAN to be based on the same AAA procedures utilized in the GPRS system; i.e. to allow the operator to extend access to its GPRS based services to subscribers in a WLAN environment (service continuity).
A very interesting tight coupling approach has been presented in [7]. The WLAN network is deployed as an alternative RAN and connects to the GPRS core network through the standard Gb interface (cp. Figure 4). From the core network point of view, the WLAN is considered like any other GPRS routing area in the system

H. *Integration*

The integration scenario is similar compared to tight coupling regarding seamless handover. However in this case a WLAN can be viewed as a cell managed at the RNC (Radio Network Controller) level. This concept is not widespread because extensive large area network planning is uncommon for WLAN yet; i.e. interference levels are usually not considered because in today's scenarios geographical spreading of Access Points (AP) ensures lack of interference from neighbouring cells in particular in rural environments. However it should be noted that this method would be the ideal case from the end user perspective.

The most frequently discussed architectures at the moment are loose coupling and tight coupling [7]. The tightly coupled architecture integrates the WLAN backbone within the GPRS network. From the cellular point of the view the WLAN is seen as a certain routing area. VHO (Vertical handover) therefore appears as a routing area handover for the GPRS network. However all GPRS components must be able to deal with a huge amount of data traffic, since the WLAN traffic will be transported also through GPRS backbone. A closer description could be found in [7]. Operators may favour the loosely coupled architecture because of its easy deployment. The large benefit of the loosely coupled approach is that each system only needs minor changes on the deployed network components. These changes consider a common billing and authentication based on the cellular subscriber identification module (SIM) [8].

IV. Computer Simulation Technique

At the Chair of Communication Networks, Aachen University a simulation tool called SDL-based Generic Object-Oriented Simulation Environment (S-GOOSE©) has been built. This tool makes it possible to investigate intersystem aspects in a very detailed manner. Figure 6 shows the overall principle, the simulation tool consists of several different protocol stacks, and each stack is separated into single independent libraries. In the past a simulation tool for each system has been developed in great detail to study the system performance and the influence of protocol enhancements and new proposals. These single system simulators are now merged to a multi-system simulator.
All integrated systems use the same IP backbone and a combined interference engine. Abstracted traffic sources allow comparative investigations of the systems under the same load

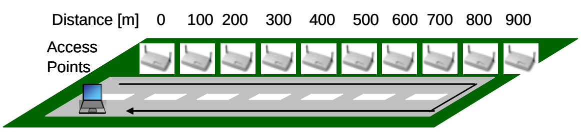

Figure 5: Street Scenario, 10 APs and one STA

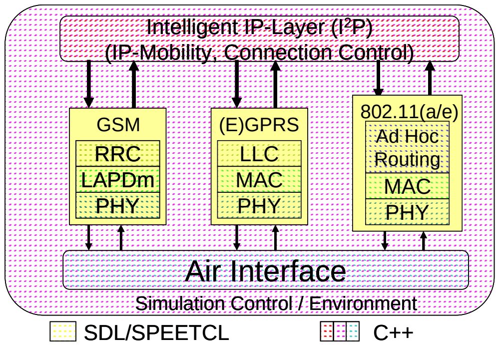

Figure 6: Simulator Structure

conditions. The channel model involves a detailed interference calculation which is essential for the investigation of interference limited systems including the scenario topology, buildings, street maps and fading effects.
This strategy gives the unique opportunity to investigate either the behaviour of a certain protocol layer within a particular system or the whole deployed system without a trade-off in accuracy. Hence the S-GOOSE can be used for intersystem cell and frequency planning or protocol investigation. Currently the simulator contains three different wireless systems, the GSM, GPRS and IEEE 802.11a/g/e (cp. Figure 6).

5. Intra-System Simulation Results

We start with the simulative comparison of different handover methods in WLAN. 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 long 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.
One terminal moves with a speed of 2 m/s along the street and returns. The offered downlink traffic to the terminal is 6 Mb/s constant bit rate (CBR) with a packet size of 256 bytes. Within our simulations the received power level P_{lim} to start the CoHCo search for neighbouring APs is set to 8 dB. Figure 5 shows the number of missed packets along the terminal's distance, where the eighteen handovers can be observed.

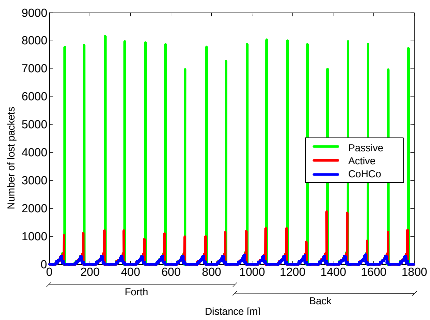

Figure 7:Number of Lost Packets per Handover

Figure 8 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 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.

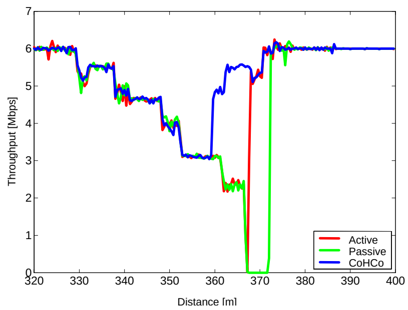

Figure 8: Detailed throughput for the handover between two different APs

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. A node using passive and active scanning waits until the current connection fails and starts the new scanning process afterwards. The drawback can clearly be seen in Figure 8. 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 [5].

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 500kb/s 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 10Mb/s. 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 kb/s, CBR with a packet size of 200 bytes. Figure 9 illustrates the simulated scenario.

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

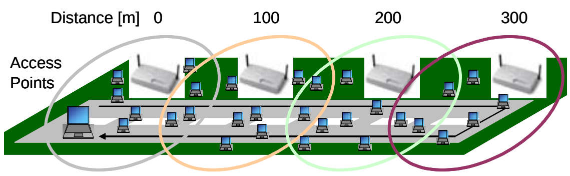

Figure 9: Street scenario with background traffic

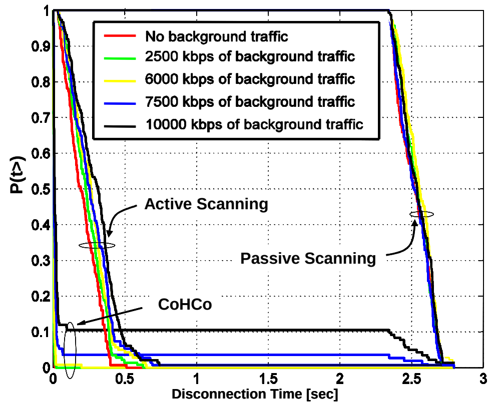

Figure 10: Complementary Cumulative Distribution Function (CCDF) of the Handover Delay with background traffic

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 Mb/s background traffic CoHCo fails with a probability of less than 5% and with 10 Mb/s 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.

6. Intersystem Simulation Results

This section presents the traffic performance in the mobile internet architecture with IEEE 802.11a and GPRS using the described simulation tool. We show a simplified scenario containing a single GPRS cell. The investigated architecture was coupled using a tight coupled approach. The WLAN system has been connected to the SGSN, when WLAN coverage is available the SGSN switches the traffic and redirects the data stream to the WLAN network (tight coupled). If it leaves the WLAN coverage, a terminal uses its GPRS interface and the SGSN switches the data stream back to the GPRS network. The GPRS cell serves as overlay network. To limit the simulation time we focus on a square area of 200m x 200m. The GPRS BTS and a IEEE 802.11 AP are place at the coordinates (100,100) and a second AP at (0,0) (cf. Figure 11). The MS starts at (0,0) moves to the square border and returns to the cell centre. This movement pattern is done forming a circle around the BTS. The MS transmits in uplink direction and uses the passive scanning to find an appropriate AP. The vertical handover is initiated after scanning failed five times. Establishing a GPRS connection took around 220 ms in the described scenario. The IEEE 802.11 WLAN interface is scanning continuously. When the MS returns under the

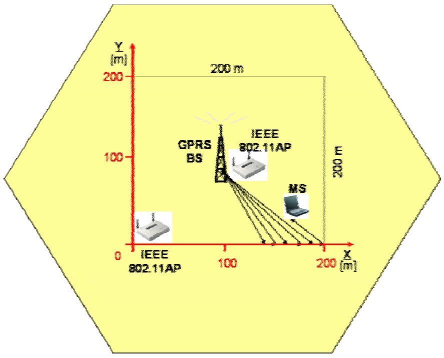

Figure 11: Scenario Combining GPRS Cell and two WLAN Access Points

coverage of an AP it starts its association and authentication with the AP. Presented are the resulted throughput and packet delay distribution over the investigated area. The IEEE 802.11a WLAN interface has been configured to use BPSK ½ [5] as its coding scheme, thus the throughput at AP is limited to 3.4 Mb/s. After switching to GPRS the throughput degrades rapidly, as shown in Figure 12. The GPRS interface uses one PDCH and the coding scheme CS-2 which provides a net data rate up to 11.4 kbps. In the presented simulation a throughput of around 7 kb/s has been observed when connected via GPRS.
This result indicates that the VHO works to avoid the interruption of the connections during the change of the access technologies. In this particular scenario only one mobile terminal has been simulated, thus no background traffic is considered.

7. Discussion and Conclusion

The paper reviews hybrid mobile internet architectures. The critical part in next generation architectures is the mobility management and how to execute horizontal and vertical handover in an efficient way. IEEE 802.11 includes 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

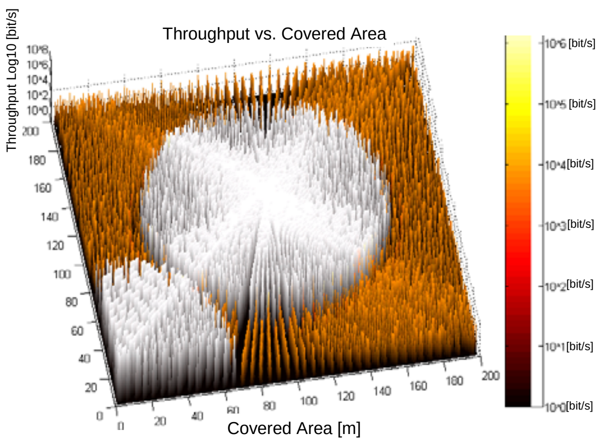

Figure 12: Throughput Results of the mobile Internet architecture with IEEE 802.11a and GPRS

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. Thus using CoHCo allows fast handover, as a consequence IEEE802.11 can also be used to connect moving cars with the internet. This feature allows the creation of new services such as addressed by the new European Project MYCAREVENT[i].
This paper presents first improvements for a horizontal handover method for IEEE 802.11 WLAN, and in the second part we present results visualizing the impact of a vertical handover between GPRS and IEEE 802.11. We developed a simulation tool that is unique for studying performance of hybrid systems. The developed tool as an intersystem simulation platform will be further developed to compare the different architectures and to add the UMTS protocol to the multi-system simulator S-GOOSE©. The paper presents the first simulation results showing the rapid service degradation when switching from WLAN to GPRS but no disrupted in the connection. The large difference between GPRS and WLAN shows impressively the need to increase to overall capacity by integrating WLAN hotspots in the existing cellular architecture. Intersystem handover cannot support QoS critical service with a data rate exceeding the cellular data network data rate. But intersystem handover might tremendously decrease the user waiting time and additionally the load in the GPRS network, since few seconds attached to the WLAN can replace minutes of a connection via GPRS.

REFERENCES

[1] B. Walke, "Mobile Radio Networks". New York, USA: Wiley & Sons Ltd., 1. ed., 1999.
[2] 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.
[3] A. Mishra, M. Shin and W.A. Arbaugh, Context Caching Using Neighbor Graphs for Fast Handoffs in a Wireless Network, Infocom 2004
[4] 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.
[5] 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.
[6] 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.
[7] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J.P. Makela, R. Pichna, J. Vallstron. Handoff in hybrid mobile data networks. *IEEE Personal Communications*, Volume: 7, Issue: 2 , April 2000.
[8] A.K. Salkintzis, C. Fors, R. Pazhyannur; WLAN-GPRS integration for next-generation mobile data networks. *IEEE Wireless Communications*, Volume: 9 , Issue: 5 , Oct. 2002, Pages:112 – 124
[9] K. Ahmavaara, H. Haverinen, R. Pichna, Interworking architecture between 3GPP and WLAN systems, *IEEE Communications Magazine*, Volume: 41 , Issue: 11 , Nov. 2003 Pages:74 – 81
[10] 3GPP Systems to WLAN Interworking, tech. report 3GPP TR 22.934 V6.2.0, September 2003; www.3gpp.org.
[11] C. Perkins, "IP Mobility Support for IPv4", IETF RFC 3220, Jan 2002
[12] D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, draft-ietf-mobileip-ipv6-24.txt, IETF, June 2003
[13] H. Soliman, C. Catelluccia, K. El Malki, L. Bellier. Hierarchical Mobile IPv6 mobility management (HMIPv6). draft-ietf-mipshop-hmipv6-02.txt, IETF, June 2004
[14] R. Koodli, Fast Handovers for Mobile IPv6. draft-ietf-mipshop-fast-mipv6-01.txt, IETF, January 2004
[15] P. Krishnamurthy, K. Pahlavan, A. ZahediA. Hatami, M. Ylianttila, J.P. Makela, R. Pichna, J. Vallstron. Handoff in 3G Non-

[i] www.mycarevent.com

Homogeneous Mobile Data Networks, Euro Microwave Week, October 1998
[16] Ye Min-hua, Liu Yu, Yang Hui-min, The Mobile IP Handoff between Hybrid Networks, IEEE PIMRC 2002 Sep. 2002
[17] 3rd Generation Partnership Project/Technical Specification Group Services and System Aspects, "Feasibility study on 3GPP system to Wireless local area network Interworking, Release 6", September 2003.
[18] E. Weiss, U. Fornefeld, B. Xu, S. Hischke, “Performance Evaluation of A Mobile Internet Architecture with IEEE 802.11a WLAN and GPRS/UMTS” Proceedings of The Seventh International Symposium on Wireless Personal Multimedia Communications, WPMC04, September 2004
[19] E. Weiss, A.Otyakmaz, E. López, B. Xu. “Design and Evaluation of a New Handoff Protocol in IEEE 802.11 Networks” In Proceedings of 11th European Wireless Conference 2005, April 2005