THE IP MICRO MOBILITY APPROACH

Bernd Gloss *Christian Hauser*

University of Stuttgart, Institute of Communication Networks and Computer Engineering (IND)
Pfaffenwaldring 47, D-70569 Stuttgart, Germany
e-mail: {gloss,hauser}@ind.uni-stuttgart.de

ABSTRACT

Mobile IP is a powerful protocol which supports Internet mobility and scales reasonably with the number of users within a system. Due to the high roundtrip delay of the Internet and due to Mobile IP's control overhead, Mobile IP causes connections of a mobile node to be interrupted for up to 5 seconds for each change of its attachment point to the Internet. This interruption induces TCP to run into its slowstart procedure or disturbs real-time multimedia transmissions in a significant way. Thus Mobile IP is more applicable for nomadic computing than for mobile computing. Resulting from this weakness recently some micro mobility approaches have been proposed within the IETF, which support mobility in a well defined area, e.g. in an access network, and interact with Mobile IP in a hierarchical way. Those protocols do not scale as well with the number of users as Mobile IP does but behave much better for handovers. In the near future those micro mobility protocols will gain much attention, especially for the "All-IP Approach" of future mobile cellular networks where everything (data traffic, signalling and circuit switched services) shall be transported in IP packets. This survey introduces two very similar micro mobility protocols called Cellular IP and HAWAII and presents their mechanisms to support mobility.

1. INTRODUCTION

With the upcoming third generation cellular systems for data communication, computers will become an ubiquitous part of our life. Today's cellular phones will migrate to personal digital assistants (PDAs) and we want to use them anytime and anywhere to provide us with information, communication facilities and entertainment.

To satisfy this *"anytime and anywhere"* scenario in conjunction with the scarce resources of the wireless interface it is expected that third and fourth generation cellular systems are packet switched and have a micro- and pico-cellular network structure. Those expectations and requirements in connection with the success of the Internet lead to the task to provide the Internet Protocol (IP) with a powerful and scalable mobility support which is capable of coping with hundreds of millions of mobile users.

Mobile IP [7,13] pursues the approach of inserting the mobility agents at the edges of the Internet, namely in the home network of each mobile host, in the foreign networks the mobile hosts can visit and on the mobile hosts themselves. In case of the absence of a mobile host from its home network, it obtains a temporary care-of address which it signals to its home agent in its home network. The home agent then forwards all IP packets destined for the mobile host through an IP-in-IP-tunnel to this care-of address. Handovers from one foreign network to another foreign network are handled the same way.

Due to the distribution of the mobility agents, Mobile IP scales quite well with the number of users. On the other hand, in an environment of a micro- and pico-cellular network infrastructure Mobile IP would have to cope with a high handover rate; e.g. in a Bluetooth [10] environment with 20m cell diameter a pedestrian walking with 5km/h would have a handover at least every 14.4seconds.

In an *"always on"* scenario, which fits quite well to the packet switched communication of IP, those handovers have to be done even if the mobile host does not want to transmit data but might receive data. For each handover, signalling has to take place between the mobile host and its home agent, which

takes a lot of time and generates a lot of signalling load to the network. Particularly this signalling load is proportional to the number of users and their level of mobility and not to their demand for transmission bandwidth. The simplest way to improve this weakness is to introduce hierarchies to the mobility infrastructure. With this hierarchy the user mobility shall be handled where it originates: in the access network.

This survey is ordered as followed: In chapter 2 the micro mobility protocols *Cellular IP* from the Columbia University New York and *HAWAII* from the Lucent Bell Labs are presented as examples for micro-mobility protocols. In chapter 3 the presented protocols are reflected and their impact to network architectures and mobility support are discussed. In chapter 4 some statements about the usability of the protocols and aspects for future work are given.

2. DOMAIN BASED MICRO MOBILITY SUPPORTING PROTOCOLS

In this chapter, two very similar domain based layer 3 micro-mobility protocols are presented as examples among some others [3,4,5,6]. Both protocols employ the approach of changing IP routing mechanisms to provide mobility and handover support and both interwork with Mobile IP in a hierarchical manner.

Specialized path setup schemes are used to install host based routing information in specific routers. These schemes operate locally to a specific access network so they reduce the amount of global location updates and mobility-related disruptions to users. For achieving reliability, routing information is maintained as soft-state entries.

Due to the size and the distributed management of the Internet, the approach of changing IP routing can only be applied in limited access networks best under the control of a single authority. The impact of such an approach to a network infrastructure is that no ordinary IP routing hardware can be deployed. However, due to the current rare deployment of wireless access networks this may be an approach that suits well.

Both protocols follow the approach of hierarchical mobility support in conjunction with Mobile IP, as illustrated in figure 1. They provide mobility in a well defined area, e.g. an access network, and let mobility between different access networks be handled by Mobile IP as macro-mobility solution. If a mobile host is in its home network, both Cellular IP and HAWAII act as a simple routing protocol without the impact of Mobile IP. Then the only impact is, that host based routing is used. When a mobile host moves to a foreign access network running Cellular IP respectively HAWAII, Mobile IP gets engaged to forward the packets to the foreign network.

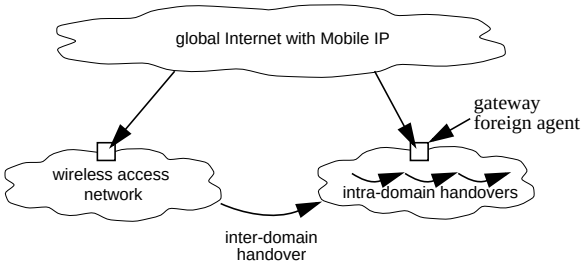

Figure 1. Domain Based Wireless Access Networks and Mobile IP

2.1. Cellular IP

Cellular IP [1,11] is a proposal to the IETF made by researchers from Columbia University, New York and Ericsson in 1998 and 1999. Besides the Mobile IP protocol engine, Cellular IP mobile hosts have to run a special Cellular IP protocol engine that controls the mobility support of the network to a mobile host.

2.1.1 Network Architecture, Routing and Paging

A Cellular IP network, see figure 2, comprises a gateway router that connects the Cellular IP network to the Internet as well as several Cellular IP nodes that are responsible for the Cellular IP routing and mobile hosts which support the Cellular IP protocol. The Cellular IP nodes can be a wireless access point at the same time.

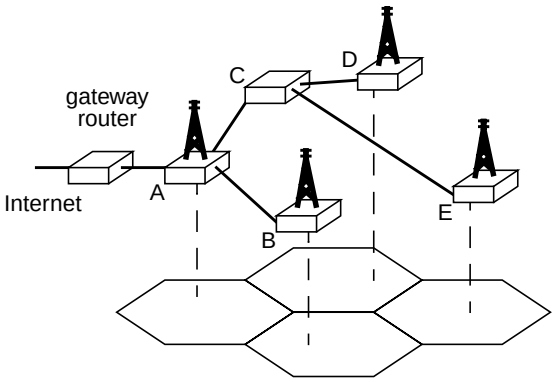

Figure 2. Cellular IP wireless access network model

A mobile host is connected to a wireless access point, also called base station, to which it relays the packets it wants to transmit and from which it receives the packets destined for it. Each Cellular IP node has an *uplink neighbour* to which it relays the packets originating from the mobile hosts and one or more *downlink neighbours* to which it relays the packets destined for a mobile host. This network structure is either preconfigured by the network management or

set up by a special *uplink neighbour selection algorithm* running after each change of network topology.

After power up a mobile host has to register to the Cellular IP network, which means that it has to set up a routing path from the gateway router to its current attachment point. This is done in a reverse manner by sending a *route update message* from the mobile host to the gateway router. The route update message is received by the base station and forwarded hop-by-hop following the uplink neighbours of each Cellular IP node towards the gateway router. Each Cellular IP node maintains a *route cache* in which it holds host based routing entries. Whenever a route update message passes a Cellular IP node, a routing entry for the related mobile host is written in the cache. The so called host based entries map a mobile host's IP address to the interface from which the packet arrived at the node. When the route update message arrives at the gateway router, it is dropped after the gateway router added a routing entry to its route cache. After that, the chain of cached host based routing entries referring to a specific mobile host constitutes a reverse path for packets addressed for that mobile host.

The routing entries in the Cellular IP nodes are soft state. This means, after a certain expiration time they are not valid any more. This is necessary since due to a link loss a mobile host might not be able to tear down its routing entries before leaving the network. In order not to lose its routing path, a mobile host has to refresh its routing entries periodically. In Cellular IP this is done by a regular data packet or by sending a route update message if the mobile host has no data to transmit.

Mobile hosts that are not actively transmitting or receiving data but want to stay reachable, have the opportunity to let their route cache entries time out and to maintain paging cache entries. A mobile host with outdated route cache entries but with valid paging cache entries is said to be in *idle state*, while a mobile host with installed route cache entries is said to be in *active state*. The difference between the route cache and the paging cache is, that paging caches are not necessarily maintained on each Cellular IP node and have longer timeout values. On Cellular IP nodes, where both a route and a paging cache are maintained, packet forwarding in downlink direction is done in the same way for routing and paging with priority to the route cache entries. If a Cellular IP node, that does not maintain a paging cache, receives a downlink packet for a mobile host for which it has no routing entry in its route cache, it broadcasts the packet to all its downlink neighbours. By this mechanism groups of several, usually adjacent base stations are built in which idle mobile hosts are searched when a packet has to be delivered to them. Those groups of base stations are called *paging areas*. To minimize paging traffic, an idle mobile host has to set up its route cache entries immediately after receiving a packet by paging.

When a mobile host is in active state, the Cellular IP location management has to follow its movement from base station to base station to be able to deliver packets without searching for the mobile host. As a consequence active mobile hosts must notify the network about each handover. For idle mobile hosts exact location tracking is less important, instead minimizing communication to save battery power has higher priority.

In Cellular IP networks, a mobile host retains its IP address whether it is in its home network or in a foreign network. This is possible due to the host based routing of Cellular IP that maintains separate routing entries for each host and does not use IP inherent routing information. When a mobile host is in a foreign Cellular IP network it uses the gateway router as endpoint of the Mobile IP tunnel and therefore uses the IP address of the gateway router as its care-of address, see figure 3.

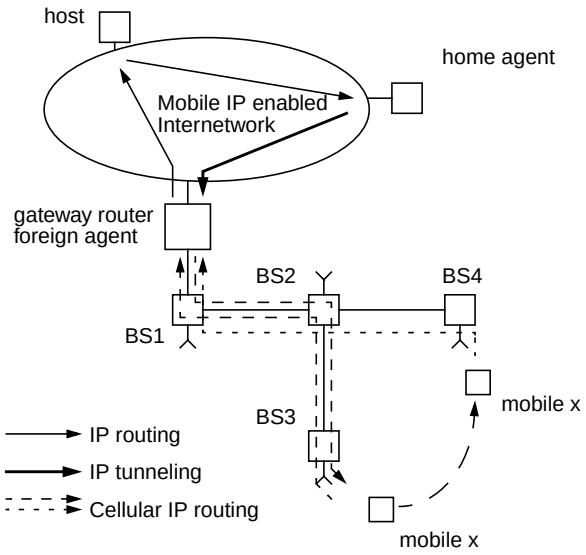

Figure 3. A Cellular IP Access Network Interconnected to a Mobile IP enabled Internet

2.1.2 Handover Mechanisms

In Cellular IP a handover is always initiated by the mobile host sending a route update message to the new base station. This route update message then travels in the already described hop-by-hop manner from the base station to the gateway router and reconfigures the route cache entries in the Cellular IP nodes along its way. The path from the gateway router

to the new base station may overlap with the path to the old base station. Route cache entries on the part of the path to the old base station that does not overlap with the path to the new base station simply time out due to the soft state mechanism. They are not explicitly cleared by a tear down signal.

Cellular IP provides two handover mechanisms: A *hard handover* and a *semi-soft handover* mechanism. Both mechanisms are for wireless interfaces that can maintain connection to only one base station at the same time. The two mechanisms differ in the way a mobile host changes from one base station to another base station.

For a hard handover, the wireless interface of a mobile host changes from one base station to another at once. The Cellular IP protocol engine of the mobile host recognizes this event either by a notification from layer 2 of its device driver or by receiving a beacon signal from the new base station with a different base station ID than the last one it was attached to.

If the Cellular IP protocol engine on the mobile host can influence the handover of the underlying network interface, the mobile host can perform a semi-soft handover. In this case the mobile host switches to the new base station, transmits a route update message with a flag indicating the semi-soft handover and returns immediately to the old base station in order to listen for packets destined to it. The route update message reconfigures the route caches on the way to the gateway router as usually, except for the route cache on the so called cross-over node, where the new path branches off from the old path. In that node an additional entry is added to the route cache, so that downlink packets for the specific mobile host are duplicated and sent along both paths, the new one and the old one. After a fixed amount of time, the mobile host finally migrates to the new base station and then sends another route update message to complete the semi-soft handover. This second route update message sets up a proper path to the new base station and stops the cross-over node duplicating packets.

If the path to the new base station is longer than to the old base station or if it takes a non negligible amount of time to switch to the new base station, then some packets may not reach the mobile host. To overcome this problem, packets sent along the new path can be delayed during semi-soft handover. This way, a few packets may be delivered twice to the mobile host, but in many cases this results in better performance than a few lost packets.

On a hard handover data packets on their way to the old base station respectively data packets arriving at the cross-over node before the route cache entry is changed are misdirected and will be lost since the mobile host is already attached to the new base station. On a semi-soft handover only data packets that arrive at the old base station while the mobile host transmits the first route update message are lost. In both cases fewer packets will be lost as on a standard Mobile IP handover which is a hard handover and takes much more time than a Cellular IP hard handover.

2.1.3 Security

Cellular IP provides a security mechanism for protecting against malicious mobile hosts stealing links by sending route update messages for another mobile host. This mechanism is based on a session based shared secret between a mobile host and the Cellular IP network.

Each Cellular IP network has a secret network key which is known to all Cellular IP nodes including the gateway router but not to any mobile host. Each mobile host initially has to register and to authenticate to the Cellular IP network. This is handled by the gateway router using any known symmetric or asymmetric method. After a successful registration, the gateway router calculates a Personal Identification (PID) for the specific mobile host based on the network key and the mobile host's IP address and transmits this to the mobile host using a public key method. Hereafter the Cellular IP network and the mobile host have a shared secret they can use to authenticate control messages. The PID remains the same during handover and can be easily computed by each base station.

Only control messages are protected by this mechanism. Data packets are not protected against any attack. To protect user data another protocol, e.g. IPSec [9] has to be employed.

2.2. HAWAII

In this section another domain-based approach for supporting micro-mobility called Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) is presented. HAWAII was proposed to the IETF in [8,12] by researchers from Lucent Bell Labs in 1999. Like in Cellular IP, HAWAII is responsible for the intra-domain mobility limited to an administrative domain of an access network while the inter-domain mobility is handled by Mobile IP.

2.2.1 Network Architecture, Routing and Paging

In HAWAII a hierarchy based on domains is used like depicted in figure 4. The gateway into each domain is called *domain root router.* Further a HAWAII domain comprises several routers and base stations running the HAWAII protocol, as well as mobile hosts.

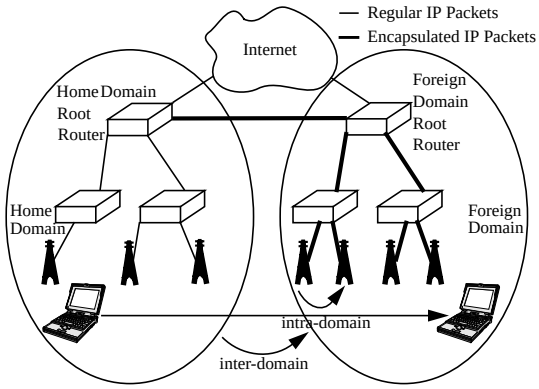

Figure 4. HAWAII Hierarchy of a HAWAII-based Network

A mobile host in a HAWAII environment runs a standard Mobile IP protocol engine with Network Access Identifier (NAI), route optimization and challenge/response extensions. HAWAII intends not to cause great modifications to the Mobile IP protocol engine running on a mobile host to prevent mobile hosts from having two protocol stacks implemented.

The processing of Mobile IP messages is split in two sections. The first one reaches from the mobile host to the base station and the second one from the base station to the Mobile IP home agent of the mobile host. Since some Mobile IP messages are translated to HAWAII messages and are processed locally within the HAWAII domain, less mobility updates have to be transmitted to the home agent compared to standard Mobile IP protocol. Additionally this results in reduced disruptions to running data transmissions during handovers and base stations can even provide a better handover support e.g. by forwarding data packets if necessary.

There are three types of HAWAII path setup messages: power-up, update and refresh. On power up a mobile host sends a *Mobile IP registration request message* to the corresponding base station. The base station then sends a HAWAII *path setup power-up message* to the domain root router which is processed in a hop-by-hop manner. On all routers on its way to the domain root router this power-up message adds a routing entry for the concerned mobile host. The domain root router finally acknowledges this path setup power-up message to the base station which finally notifies the mobile host with a *Mobile IP registration reply.*

If a router knows multiple paths to the domain root router, it can use any of them but it always has to use the same route for a specific host. The routing entries in the routers are soft-state, i.e. they have to be refreshed periodically by *path setup refresh messages*, which are sent independently by each network node and which can be aggregated.

Routers, not passed by a path setup message related to a mobile host, don't have any knowledge about its whereabouts. Whenever a router receives a packet for such an unknown mobile host, e.g. from another mobile host within the domain, it uses a preconfigured default interface pointing towards the domain root router. This packet will be forwarded in this direction until it will arrive at a router knowing a route to the addressed host. In worst case this will be the domain root router.

Notifying the network on each handover regardless whether the mobile host is active or not consumes a lot of battery power. Since in a mobile environment this might not be desirable mobile hosts can switch to a *standby state*, in which they do not have to notify the network on each handover. In this case the network does not have to keep exact location information of those mobile hosts, but only information about the approximate location, the so called *paging area*. Typically a domain includes a couple of paging areas each built of several base stations. HAWAII does not require a specific definition of a paging area. It supports hierarchical areas as well as fixed areas or even personalized paging areas.

Mobile hosts in standby state only have to notify the network on a change of paging area and not on each base station handover. When a packet arrives for a mobile host in standby state, the network has to page it before it delivers the packet. This paging induces the mobile host to switch to active state immediately. For using HAWAII's paging support, it is necessary to have link-layer paging functionality on the wireless link which means that the mobile host is able to identify its paging area and to detect paging requests. A typical solution for identifying the paging area is, that base stations periodically send beacon signals including the paging area identities on a broadcast channel, so a mobile host listening to this channel can easily detect a change. The paging requests of the base stations can be sent on separate paging channels to which the mobile hosts are listening.

The network has to maintain paging information for each mobile host and has to deliver paging requests for these hosts up to the base stations from where on link-layer paging mechanisms are responsible. One way to achieve this is to deliver the paging requests to each base station within the area using a unicast message to each one. Because that would be a waste of bandwidth, HAWAII relies on the IP multicast routing protocol. Each paging area is assigned a multicast group address and all base stations within

that paging area join this multicast group. Because these multicast groups are within one single HAWAII domain, an address from the allocated range for administratively scoped IP multicast addresses can be used.

Each mobile host has assigned a home domain as well as a unique IP address. While moving within the home domain the mobile host retains its IP address which can be assigned statically or dynamically. When data packets for a specific mobile host arrive at the domain root router, they are forwarded on the previous described, dynamically established routes directly to it. Thus no home agent is involved. On moving to a foreign domain, the Mobile IP home agent of the mobile host's home domain gets involved by using classical Mobile IP mechanisms. If the foreign domain is HAWAII-based, the mobile host will be assigned a co-located care-of address (CCOA) from the address space of the foreign domain. From now on the mobile host's home agent tunnels packets to the mobile host via this CCOA. While moving around within the foreign domain, the mobile host retains the same CCOA as it retains its native IP address when moving around in its home domain. As in home domain dynamically established paths to the mobile host will be used in foreign domain, too. The mobile host's home agent is not notified on handovers of these intra-domain migrations.

2.2.2 Handover Mechanisms

A handover in HAWAII will take place, when the mobile host's next hop IP node changes. For discussion in this paper we assume base stations have IP routing functionality. Additionally, we use a tree-based topology for clarity, but the schemes pointed out will also provide for non-tree-based topologies.

For describing re-establishments of routes after intra-domain movements a so called cross-over router has to be defined. This is the one closest to the mobile host at the intersection between the path from the domain root router to the old base station and the path from the old base station to the new base station.

There are two different path setup schemes for updating routing information, which is held decentralized in the different concerned routers. One for networks with mobile hosts that can only maintain connection to one base station (e.g. TDMA networks) and the other one for networks with mobile hosts that can be connected to two or more base stations simultaneously like in CDMA networks for example.

The first scheme is called *forwarding path setup scheme* and its functionality is depicted in figure 5. In case of a handover, which is indicated by a discrepancy between the advertised NAI of the actual base station and the NAI of the old one, the mobile host sends a Mobile IP registration request to its new base station. This new base station then sends a HAWAII *path setup update message* directly to the old base station which address was transmitted by the mobile host. The old base station performs a table look-up for a route to the new base station and determines the next hop router. It adds a routing table entry for the mobile host pointing to that next hop router and forwards the path setup update message. From now on the old base station forwards all data packets for the concerned mobile host to the new base station according to the new forwarding entry.

The next hop router performs similar actions and in that way the packet is forwarded up to the cross-over router which changes the moved mobile host's routing entry, too. From now on the cross-over router diverts new data packets to the new base station. This mechanism can lead to some mis-ordered packets. The cross-over router then forwards the path setup update message completely to the new base station that also adds a forwarding entry and sends a Mobile IP registration reply to the mobile host.

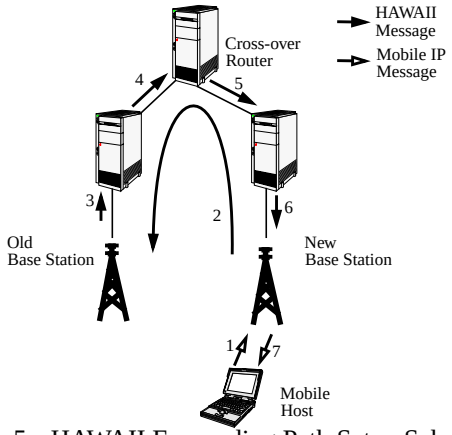

Figure 5. HAWAII Forwarding Path Setup Scheme

In the second scheme called *non-forwarding path setup scheme* the data packets are diverted at the cross-over router from that time on, when the path setup update message first passes the cross-over router. In this path setup scheme the old base station does not forward any packets to the new base station.

On receiving a Mobile IP registration request, the new base station adds a forwarding entry for the mobile host pointing to the interface on which the registration request was received. Then it looks for a path to the old base station and sends a path setup update message on the determined interface. The next router performs similar actions and forwards the message, too.

When the message reaches the cross-over router, it updates its routing table resulting in diversion of new arriving data packets. Then the message is forwarded to the old base station which changes its forwarding entry and sends back an acknowledgement to the new base station which in turn sends the mobile host a registration reply. This scheme is depicted in figure 6.

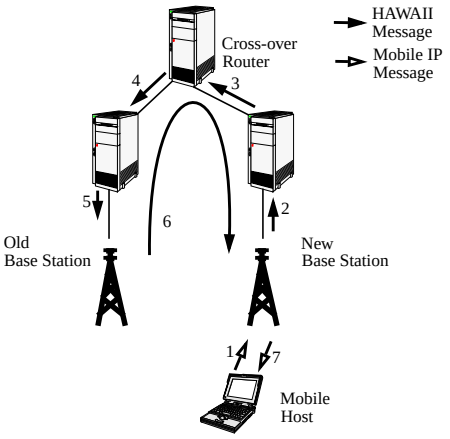

Figure 6. HAWAII Non-Forwarding Path Setup Scheme

In audio and video experiments with UDP packets for example, the non-forwarding scheme performs slightly better, but the differences are rather small.

2.2.3 Security

Regarding security of the protocol, there are two important issues. The first one is user authentication while assigning the co-located care-of addresses via DHCP and the second one is about security and authentication of the Mobile IP and HAWAII protocol messages.

Concerning the Mobile IP protocol messages a trust model is proposed. The mobile hosts have to trust the registration replies and the home agents have to trust the registration requests from the foreign agents. Therefore it is necessary to distribute temporary session-keys to all involved entities. Moreover the home agents are able to allow certain base stations to serve its mobile hosts, by this.

Because HAWAII messages are generated and processed within a single administrative domain, their authentication is easy to tackle e.g. by using a password field.

3. PROTOCOL REFLECTIONS

In chapter 2 of this survey, the two micro-mobility supporting protocols Cellular IP and HAWAII have been presented. In this chapter their basic mechanisms and design principles are outlined and discussed.

3.1. Host Based Routing and Paging

Both Cellular IP and HAWAII use host based routing within a limited access network. The IP inherent routing information of networks and subnetworks is ignored. The impact of such an approach to a network infrastructure is that no ordinary IP routing hardware can be deployed and that an approach with host based routing does not scale very well on the number of users. However, due to the current rare deployment of wireless access networks this may be an approach that suits well.

In addition to the routing mechanism both protocols offer the possibility for mobile hosts to be paged. Paging in Cellular IP is done in the same way as routing is done, except that not all network nodes maintain paging caches. Nodes that do not maintain a paging cache simply broadcast packets destined for a mobile host that is not listed in their route cache. Thus paging areas in Cellular IP depend on network topology. In Cellular IP paging is done with data packets themselves. After an idle mobile host has received a packet by paging, it immediately has to set up an active route towards it, since more packets are likely to arrive. In HAWAII paging is realised by IP multicast groups. As in Cellular IP some network nodes maintain paging caches that map mobile host IP addresses to IP multicast groups. Each multicast group corresponds to a specific paging area. If a packet shall be delivered to a mobile host that has no active route the packet is buffered in a specific network node and a paging message is transmitted to awake the mobile host. After the mobile host has activated a route leading to it, the buffered packet is delivered.

In order to manage link failures gracefully, both protocols employ soft-state routing and paging entries.

3.2. Path Setup Schemes and Signalling

In both protocols special signalling between nodes is used to establish host based routing information within the access network. To improve scalability and not to flood the whole access network with signalling messages only those nodes involved in a path to a specific host maintain routing information concerning this host. The other nodes in the network are unaware of that mobile host.

Cellular IP employs special signalling even for the mobile hosts while HAWAII tries to keep HAWAII signalling apart from the mobile hosts. In HAWAII the mobile host simply runs Mobile IP signalling and the messages are interpreted by the base station. As signalling of HAWAII and Mobile IP are not completely identical, the base stations have to

maintain a state machine, that coordinates the additional signalling for each mobile host. Within the access networks paths are set up in the same way in Cellular IP and HAWAII.

3.3. Interaction with Mobile IP

In Cellular IP the gateway router acts as Mobile IP foreign agent for the mobile hosts within the Cellular IP network. Thus the Mobile IP tunnel ends at the gateway router which decapsulates the packets and delivers them to the mobile hosts using Cellular IP routing. In HAWAII, each mobile host is assigned a co-located care-of address from the address space of the visited HAWAII network. Thus each mobile host has two IP addresses, namely its home IP address and the co-located care-of address. Thus the Mobile IP tunnel ends at the mobile host itself.

4. CONCLUSIONS

The discussed protocols support the micro mobility approach based on two main hierarchy levels in conjunction with Mobile IP as solution for the macro mobility. They diminish the necessity for long range signalling paths in terms of network distance that a single Mobile IP solution will cause. On the rare handovers between two micro-mobility networks the same impacts are regarded as on every Mobile IP handover.

The presented protocols are very similar to layer 2 switching in many aspects but provide independence of network technologies (LAN, WAN, Wireless LAN, etc.) through an All-IP approach. Drawbacks of this independence are some problems in handover control which is in the nature of Layer 3 protocols.

The protocols described above are based on IPv4. As the "Systems Architecture Group S2" of the 3rd Generation Partnership Project (3GPP) [14] decided in May to use IPv6 for future mobile cellular networks perhaps the presented protocols will gain limited attention for cellular networks but they are still very interesting for investigations on the micro mobility approach.

ACKNOWLEDGEMENTS

We would like to thank Rolf Sigle and Ulrich Weiss for the fertile discussions we had.

This work was partially funded by the DaimlerChrysler AG.

REFERENCES

[1] A. T. Campbell, J. Gomez, C-Y. Wan, S. Kim, Z. Turanyi, A. Valko, *"Cellular IP"*, IETF Internet Draft <draft-ietf-mobileip-cellularip-00.txt>, December 1999, Work in Progress

[2] A. T. Campbell, S. Kim, J. Gomez, C-Y. Wan, Z. Turanyi, A. Valko, *"Cellular IP Performance"*, IETF Internet Draft <draft-gomez-cellularip-perf-00.txt>, October 1999, Work in Progress

[3] C. Castelluccia, *"HMIPv6: A Hierarchical Mobile IPv6 Proposal"*, ACM Mobile Computing and Communication Review (MC2R), April 2000

[4] S. Das, A. Misra, P. Agrawal, *"TeleMIP: Telecommunication Enhanced Mobile IP architecture for Fast Intra-Domain Mobility"*, to be published in IEEE PCS Magazine, August 2000

[5] E. Gustafson, A. Jonsson, C. Perkins, *"Mobile IP Regional Registration"*, <draft-ietf-mobileip-reg-tunnel-02.txt>, March 2000, Work in Progress

[6] K. Malki, H. Soliman, *"Hierarchical Mobile IPv4/v6 and Fast Handoffs"*, <draft-elmaki-soliman-hmipv4v6-00.txt>, March 2000, Work in Progress

[7] C. Perkins, *"IP Mobility Support"*, IETF RFC 2002, http://www.ietf.org/rfc/rfc2002.txt, October 1996

[8] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, L. Salgarelli, *"IP micro-mobility support using HAWAII"*, IETF Internet Draft <draft-ietf-mobileip-hawaii-00.txt>, June 1999, Work in Progress

[9] R. Atkinson, *"Security Architecture for the Internet Protocol"*, IETF RFC 1825, http://www.ietf.org/rfc/rfc1825.txt, August 1995

WEB RESOURCES

[10] The Bluetooth Special Interest Group, http://www.bluetooth.com/

[11] Cellular IP Homepage, Columbia University, http://comet.ctr.columbia.edu/cellularip/

[12] R. Ramjee's Homepage, Bell Laboratories, http://www.bell-labs.com/user/ramjee/

[13] IETF Working Group IP Routing for Wireless/ Mobile Hosts (mobileip), http://www.ietf.org/html.charters/mobileip-charter.html

[14] The Third Generation Partnership Project, http://www.3gpp.org/