LOCALHOST HTTP PROXY FOR MOBILITY AND LOCATION BASED SERVICES SUPPORT

Jens Kammann
German Aerospace Center
Institute of Communications and Navigation
P.O. Box 1116, D-82230 Wessling, Germany
Jens.Kammann@dlr.de , Fax: +49 8153 281871

Abstract— **When TCP/IP was originally designed, location awareness and terminal mobility was not taken into consideration. IPv4 has a limited IP address space and IP addresses itself have no proximity relation. The IP address limitation will eventually be overcome by the introduction of IPv6, but most of the huge already deployed infrastructure for mobile Internet Access use private IP addresses and Network Address Translation (NAT) to solve the problem. This in turn inhibits the deployment of Mobile IP which would be needed for seamless handover between networks. The confinements due to NAT are usually countered by establishing tunnels from the inside-NAT devices to an outside endpoint. However, quite a few mobile access points don't support tunneling - either for security reasons or caused by design. A multitude of intra-network handover procedures are known, few also support inter-network handover. Standards like UMA require both cross-network agreements and software modifycations to the mobile devices whereas the solution proposed in this paper only requires application layer access to the networks.**

This paper is organized as follows: First we review the current network access methods for mobile devices with respect to mobility support. A chapter about location support of these networks follows. We will then present our proxy-based approach and compare it with respect of performance and practicability before we conclude with an outlook onto further work.

I. Overview of current mobile access methods

Wireless LAN

The mobile device scans the ISM band (2,4 GHz for IEEE802.11b/g and 5 GHz for IEEE802.11a) for available networks. Depending on client settings it may automatically connect to public non-encrypted networks and retrieves network settings (IP, Gateway, DNS information). Most Hotspots typically require authentication via HTTP usually via a transparent proxy which redirects the first page request to an authentication server (either local or remote). After successful authentication the user may use any TCP/IP application to access the Internet. Depending on security settings or price plans data transfer other than IPv4 (such as PPTP via GRE protocol or IPsec using ESP protocol) may not be possible. Furthermore, a transparent HTTP proxy may limit access to specific servers or may alter HTTP session data, e.g. for advertising purpose. Mobility is supported by means of layer 2 switching: Multiple access points using the same SSID are connected to the same network switch within the same operator network.

PLMN - packet switched

Using UMTS or GPRS, a user configurable APN determines the GGSN. However, this choice is limited to the allowed GGSN which are stored in the HLR – these are typically limited to a single Internet access APN provided by each operator. Although GPRS is packet oriented, a GPRS session needs to get established first. From the mobile device (e.g. mobile phone) to the end users device (e.g. PDA, Laptop) this is a PPP session in order to be compatible to standard RAS dial-up procedures. Handover between the same network should work seamlessly, though some networks will drop a GPRS session if handovers requires a change of the attached MSC, in most cases it will drop when roaming to a foreign network. In case of roaming the user may use the same APN setting, a transparent tunnel is established to the home operator who provides the Internet Access (another possibility is using a default APN such as "internet" which would attach the mobile device to a local GGSN. However this possibility is rarely available due to unsolved accounting issues).

As in the W-LAN case, the operator may employ a transparent HTTP proxy and the use of end-to-end tunnels may be restricted.

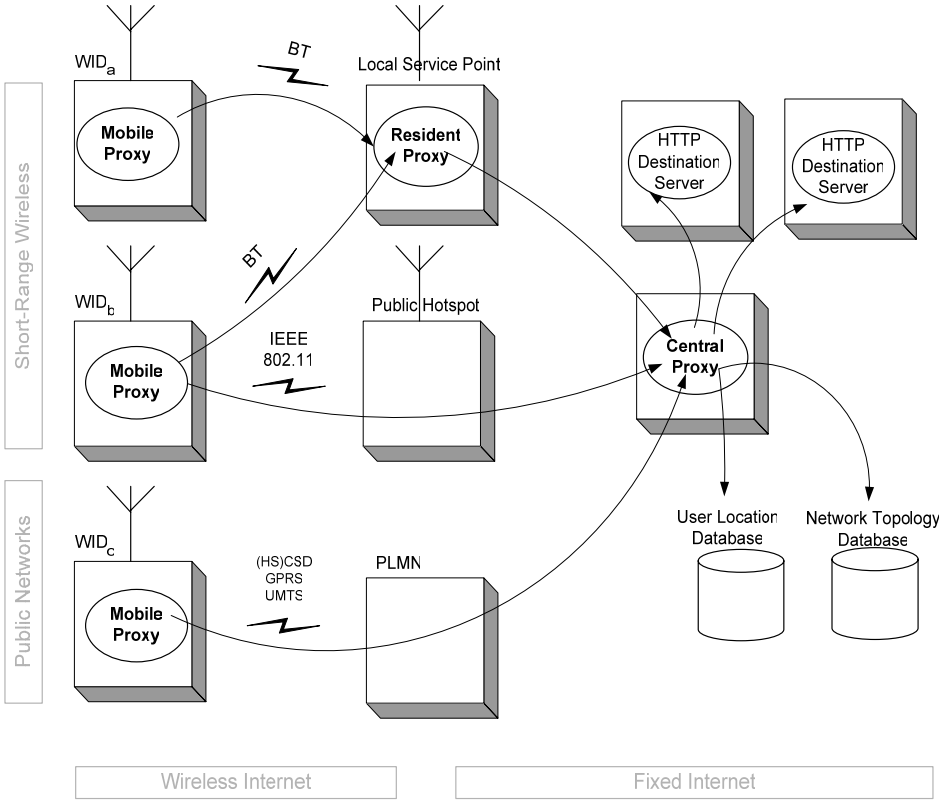

Fig. 1: Access Networks

Bluetooth

Originally designed for cable replacement, Bluetooth also can be used for network access using the LAN-Access profile or the personal area network profile (PAN). The former emulates a dial-up session using PPP protocol, the latter is still connection oriented on the Bluetooth network layer (L2cap connection), but uses Bluetooth Network Encapsulation Protocol (BNEP). PDAs and laptops typically support both profiles, but smart phones either don't or leave the feature undocumented in consideration of the mobile network operator's business case.

II. Sources of location information:

Location based services may obtain device location by several means (see Fig. 2): The least attractive method is user input as GUI interaction distracts from the application or may be not an option at all when the user is in motion. The obvious option of sharing the routing information of cellular networks by querying the mobile switching centers is difficult as any known mobile phone standard failed to specify cross-network location interfaces. Mobile operators tend to implement proprietary location information systems, most are transaction based (e.g. requesting the location of a currently assigned IP address using a XML interface). This might be a concession to event-based charging, but is unusable for applications which need continuous location information (e.g. map-based guidance).

However, in GSM and current 3GPP implementations the numerical cell id is often available to the mobile device either using special modem commands via a (sometimes virtual) serial interface or using function calls to widespread mobile operating systems such as Symbian OS or Pocket PC Phone Edition. Signal strength indicator may an – albeit coarse – replacement for the often difficult to obtain timing-advance information of TDD systems. In general, a mapping database is needed, some networks actually broadcast the geographic location of a base station (e.g. via cell-broadcast of Gauß-Krüger coordinates).

Inherent location information can be used in short range networks (e.g. Wireless LAN or Bluetooth MAC address mapped against either an managed database or public databases from wardrivers[1]). Few mobiles are already equipped with RF-ID readers – a promising technology for indoor location. As power consumption of satellite based navigation lowers, a growing number of devices is equipped with GPS (or the upcoming GALILEO) receivers, albeit sometimes confined as A-GPS solutions mainly to subject location information under operator control.

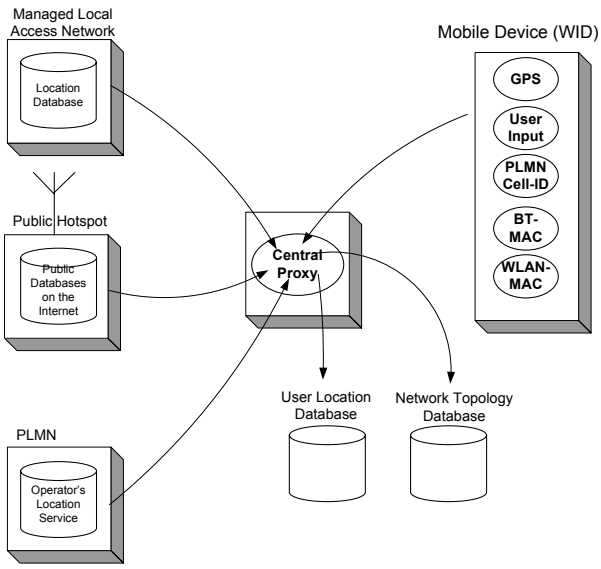

Fig. 2: Sources of Location Information

III. Proxy Approach

In the following we assume applications using the HTTP protocol[2] to communicate with servers on the Internet. This covers services such as mobile access to the WWW including streaming video, SyncML and other applications with proxy support, e.g. software agents based on MIDP platform for mobile devices.
Fig. 1 shows the outline of the split-proxy infra-structure: A *mobile proxy* (MP) residing on the mobile device, an optional *resident proxy* (RP) located anywhere within an access network and finally a *central proxy* (CP) deployed anywhere on the Internet.

The MP accepts incoming TCP sessions on a specified port, so the applications will be set up to use localhost (127.0.0.1 for IPv4 or ::1 for IPv6). Depending on the platform this done by configuring each application separately or the settings will be lodged within the configuration for network access. Some Web browsers also provide a convenient way using a proxy configuration script.

The MP connects to the CP depending on the type of network a device is attached. If the infrastructure (e.g. an WLAN or Bluetooth Hotspot) also provides an RP, it will be contacted first. Unfortunately there is no standardized method for addressing such a proxy (like *localhost* for the MP). One possibility is to assume co-location of TCP/IP gateway and proxy. If NAT is used, any other agreed private address may be used (e.g. 192.168.0.1).

One advantage of this approach is that every proxy can seamless add and evaluate information using HTTP headers. Proxy-aware applications may also add custom information, others will silently ignore unknown HTTP headers providing compatibility to theses applications.

Depending on the operating system, a MP instance has access to

- Available PLMNs
- Short range communication access points in range
- GPS WGS-84 coordinates
- RF-ID tags within range

HTTP Communication examples:

The user's web browser is set up to use localhost (127.0.0.1 for IPv4 or ::1 for IPv6) as local proxy. A request for a web page is appended by the mobile proxy's current view of the network:

GET /infotext.html HTTP/1.1
Host: www.example.net:80
X-Location: WLAN, MAC=00:30:05:49:23:C8, SSID=public

The above shows an example for a WLAN-connected device with SSID and MAC of the public access point.

When using a pure IP access network without cross-network awareness, this information is directly forwarded to a central proxy on the internet. In case of intelligent local access points (we call them local service points or LSP), the RP is added to the chain.

Since its location is fixed and known, it can add inherent location information to the requests received from the mobile proxies. The proxy chain may also optimize the payload by means of compression or content adaptation (e.g. resizing images for mobile devices with small screen resolution)

The CP extracts the piggyback location information and stores it in the user location database and fetches the requested information from a server anywhere on the internet.
So, the user location database is dynamically updated every time a user or an application requests information using HTTP.

Based on input from the Network Topology Database the response is augmented by nearby network access facilities:

HTTP/1.1 200 OK
Server: Apache/2.0.53 (Unix) PHP/5.0.3
Content-Length: *(size of infotext.html in Byte)*
Content-Language: de
Content-Type: text/html
X-Neighbor: WLAN, MAC=01:70:03:49:23:C8, SSID=public1, cost=0.2
X-Neighbor: UMTS, Network=262-01, cost=0.8
X-Neighbor: BT, MAC=08:23:33:49:2A:D1, cost=0.1, load=3
Connection: close

The network topology database gets populated by:

- PLMN information: cell-id, signal strength, Gauß-Krüger coordinates
- User input (e.g. entering street name and zip code which is mapped using a geo database)
- If the user's device is equipped with GPS, LAT/LON and precision of location information is provided
- Public Hotspot directories (Mapping Access Point MAC address and SSID to position)
- Input from managed local access networks (for Bluetooth: Mapping MAC address to position), this may be dynamic in case of a self organizing network
- Another way to obtain information about non-cooperative networks is by means of "sensor mobiles" equipped with GPS and one or more radio-interfaces. These devices may continuously scan for available access networks and report these directly to the CP.

IV. Implementation

The system was implemented for use with Symbian OS UIQ compatible devices using Personal JAVA (see Fig. 3 for a screen shot). Bluetooth & Cell-id access required system level implementation using the C++ API. As all proxies share the same code base, they can run on any JAVA-compatible platform in arbitrarily distribution.
Therefore, for development purpose it is possible to run MP, RP and CP on the same machine. The Network topology database uses a common LAMP (Linux, Apache, MySQL, PHP) web development platform whereas the User Location Database was implemented using Servlets due to extensive persistence mechanisms.

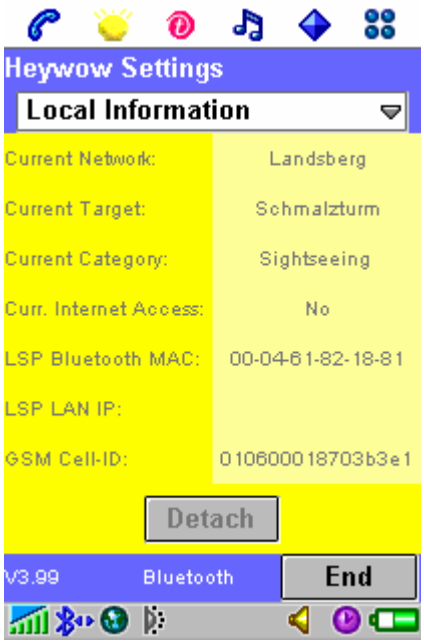

Fig. 3: Screenshot of a sample implementation of the mobile proxy for Symbian OS based mobile phones

V. System Performance

Proxies
Interposing additional data handling inevitably causes performance degradation compared to a direct client-server communication without proxies. Due to efficient handling of data streams, the throughput does not suffer significantly: On a test system physically connected via 100 MBit/s to the LAN, the maximum sustained throughput topped 35 MBit/s without any tweaking of TCP window size parameters – similar performance when using no proxies.

Due to HTTP header parsing and several protocol related overhead, the latency did increase from <10ms without proxies to some 100ms with both RP and CP in line. This causes a slightly stagnant web page reproduction if tested on a workstation compared to direct access to the server via LAN or high speed Internet access.
When used on mobile devices (tested on SonyEricsson P900 and Motorola A925) transmission delay preponderated the proxy-caused lag as a typical UMTS packed mode transmission exhibits some 300 ms delay, significantly impairing heavily fragmented web pages. Re-sorting HTTP requests at the CP, i.e. preferring text files (XML & scripts) to images did improve page reproduction.
On slow connections, such as GPRS and CSD connections, the proxies actually improved user-experience by enabling content compression, which is currently support by only few mobile web browsers natively.

Mobility Support
An application layer proxy does not aim at the same mobility standards than e.g. mobile IPv6. In fact, it assumes an HTTP request to be indivisible and need to be transferred via the same network. On the other hand, it allows for cross-network handovers even if the networks are not aware of each others, i.e. belonging to different administrative domains.
All network information visible to the mobile device gets transferred to the CP on each HTTP request (to minimize overhead, both MP and CP perform a diff in order to only transfer actually changed information) and each response from the CP carries information about nearby networks enabling the mobile device limit the search for networks to few known ones resulting in shorter handover times. E.g. a full scan of available Bluetooth access points takes some 3-10 seconds, whereas connecting to an access point with known MAC address takes less than 200 ms.
In case different types of networks are available at the same time, the estimated cost of transfer for each network can be announced, allowing the mobile to switch networks based on user preference.

Location information
Location based services can be classified into services which need absolute position and those who recognize a certain location. The latter ones can work with non geographic information such as cell-ids and MAC addresses. If just coarse location information is requited, e.g. the country a mobile user is currently in, the MCC of a cell-id will do: Fig. 3 shows a mobile device located in Germany, because the MCC is 0x106 – U.S. GSM networks have an assigned MCC of 0x136.

Depending on privacy settings of the user, the location information is forwarded along with the page request to the destination server which may further evaluate this information. More precise location information requires to geo-code the location of network base stations and their – possibly changing – cell ids. Since location information may be obtained from multiple sources with different characteristics with respect to validity and precision, resulting location may be obtained by applying a probabilistic framework [5].

VI. Conclusions & Outlook

The presented application layer approach towards location based services and mobility support provides a working solution on today's 2.5/3G networks without the requirement of setting up partnerships with public network operators. As all location information is collected at the mobile, the user remains in control of this data when using 3rd party services.
Currently public networks evolve towards all-IP networks (e.g. 3GPP IMS), but this does not necessarily mean that advanced IP features such as mobile IPv6 will make their way to the end user's device. Also a large investment in public IEEE 802.11 based wireless LAN infrastructure with mostly proprietary accounting indicate significant problems in deploying network-layer based location & mobility solutions causing application layer approaches to expand.
Finishing I would like to thank my colleagues of the *Heywow* [4] project team who contributed to the development of the presented platform.

References:

[1] WiFiMaps.com - Wardriving Maps and Hotspot Locator
[2] R. Fielding, "Hypertext transfer protocol – http/1.1", RFC 2616, June 1999
[3] M. Angermann, J. Kammann, "Cost Metrics for Decision Problems in Wireless Ad Hoc Networking", IEEE CAS, Pasadena , August 2002
[4] T. Strang, J. Kammann, P. Robertson, M. Angermann, T. Dorsch, C. Wasel, K. Wendlandt "Experiences from Ramping Up an Environment for Mobile Information Access", Workshop on Mobile and Ubiquitous Information Access (MUIA 2004) Glasgow (Scotland), September 2004
[5] M. Angermann, J. Kammann, P. Robertson, A. Steingaß, T. Strang: "Software Representation for Heterogeneous Data Sources Within A Probabilistic Framework", Locellus 2001, Munich, February 2001