Location Aware Communication

Master's project for Speechtime and Columna AB

By Johan Eckerström

June 2003

KTH Microelectronics
and Information Technology

Abstract

Automotive telematic systems will be as common in future cars as ABS and airbags are in current cars. These systems will provide services such as navigation aid, automatic emergency alerts, traffic and road information, information about parking possibilities, tourist information, and personalized news. All these services need a communication link to the mobile Internet to be able to work properly. In this master's thesis General Packet Radio Service, GPRS will be investigated and evaluated as a bearer for these kinds of services. A test application was built to test the location aware communication on the field. Upstream and downstream delays, possible bottlenecks in the network, connection set-up time, characteristics of different operators, and connection breakdowns where analyzed.

The tests showed high network delays, and that many connection breakdowns occurred. The operators did not differ much when it comes to performance. One mayor drawback with GPRS is the low scalability with respect to operator's lack of IP addresses, which will be discussed.

Conclusions of the evaluation were that only certain location-based services are suitable over GPRS with the quality of today.

Table of Contents

1 Introduction

In this master's project a location aware service system will be investigated. The system is supposed to work both in vehicles (cooperating with hardware/software in the car) and via a mobile phone where the user can request location aware information when not in the vehicle. The system should be able to provide navigation, traffic- and security information, and fastest route, among other location aware services.

The project's aim is to investigate how communication between a GPRS mobile station and a server works when sending data in predefined intervals via a continuous connection. Centrally you shall be able to request context information about the client's location. Context information includes: images, temperature, and velocity. The client shall also be able to request information from the server.

The main parts of the project are the system in the vehicle and the communication via GPRS.

The project concerns development of a system architecture, implementation (if time allows) of a demo system, and a thorough analysis of the solution-with a focus on the functionality it enables.

In this report I will try to explain the relevant subjects, background, and introduce some of the issues in building such a system. The main topics are: a generic overview of location services, related work, privacy, different wireless network technologies with a focus on GPRS, and different positioning technologies.

1.1 About this Master's Project

This literature study was written as part of a master's project in the Department of Microelectronics and Information Technology at the Royal Institute of Technology, (KTH), in Stockholm.

The master's project is performed for Columna AB in cooperation with SpeechTime AB.

Columna have been a significant collaborator in many important transportation projects, for example, at the Swedish National Rail Administration, (Banverket) and the Swedish National Road Administration, (Vägverket). Within Columna there is a broad competence in road and railway network models. They also have a high degree of business competence within the road and railway areas, including road transport telematics (ITS) and traffic management, traffic safety, and environment. The company has offices in Stockholm, Borlänge, and Sundsvall.

SpeechTime is one of the leading providers of voice services in Sweden. Several such services have been developed. Examples are stock information for Svenska dagbladet and other newspapers; weather information for SMHI; the Swedish national weather bureau, road information for Vägverket, and traffic information in Gothenburg for Göteborgsposten.

The master's project is performed at SpeechTime's office in Stockholm.

1.2 Examiner and Advisors

Examiner and advisor KTH, IMIT: Gerald Q. Maguire Jr., maguire@it.kth.se
Industrial advisor Columna: Lars Åke Asplund, larsake.asplund@columna.se

2 Location-Based Services

Location-based services are services that depend on a (mobile) user's geographic position and perhaps also context. This context may include: weather, temperature, and images.

The convergence of geographic information systems (GIS), Internet, wireless communications, location determination, and portable devices has given rise to exiting new types of information utilities that may be simply referred to as location services. Also called mobile location services, wireless location services, or location-based services [13].

Location services are doing for the real world what search engines did for the Internet. The real world is similar to the Internet in that it has millions of addresses, and each address can be linked to specific information [19]. Through the use of location services, end users can easily find selected geographic locations and related information. Location services are not dependent on the existence of a wireless network. The Internet already provides location services, e.g. yellow pages or request for a map of a specific location. However, when you use a portable device, which can communicate via a wireless network, then location services become even more interesting.

2.1 Location service applications

There are numerous possible applications for the location service market. I will focus on applications suitable for vehicles communicating via a wireless network. One can imagine a system containing of a server, a positioning mechanism, a box that extract information from the Control Area Network-bus, (CAN) [26] in the vehicle, and a mobile station that will provide data communication between vehicle and server.

2.1.1 Emergency response

This feature is one of the most desirable services according to a consumer interest survey made by ATX technology Inc [1].

In the car you have sensors that sense what is happening in the car. This possible information is available via the CAN-bus. One example is when the airbag is deployed, a signal can automatically be sent to a service provider's centre, indicating a possible traffic accident. The signal can be sent via any suitable wireless network, for example, GPRS, and Mobitex [22].

OnStar System

OnStar, a wholly owned General Motors subsidiary, is the provider of an in-vehicle safety, security, and information services. The system is completely integrated into the vehicle. The user-interface is a three-button keypad located on the dashboard or adjacent to the rear-view mirror. These three buttons enable you to send or receive a call or data from the Onstar centre, or send an emergency call.

OnStar uses existing emergency service providers, as well as cellular telephone and the Global Positioning System (GPS). It operates alongside the electrical system in your vehicle and is powered by your vehicle's battery. If the vehicle's battery is damaged or disconnected, the service will not function. Currently, analogue cellular technology is used in the OnStar system because it provides the broadest geographic coverage in the United States. OnStar has worked to "clear" the OnStar emergency-button call through all analogue cellular phone companies. The call should go through no matter which carrier you use. This is something digital systems cannot offer [23].

The GPS allows the position of any vehicle to be determined accurately to within 100 metres [23].

The system provides the user with the following services:

- Help guide you to your destination if you are lost
- If an Air bag deploys, the OnStar centre is alerted and a trained advisor will attempt to contact you and contact the assistance you need.
- In case of an emergency you can press the emergency button. You will then be put in contact with the OnStar centre, which helps you with the necessary emergency services needed.
- If your instrument panel displays a warning light, OnStar can perform remote diagnostics and advise you accordingly.
- If you are locked out of your car? OnStar can remotely unlock the driver's door.
- An OnStar advisor can also provide assistance with hotel and restaurant reservations, and provide several concierge services.

Privacy
The advisors will relay vehicle information to subscribers only when the correct Personal Identification Number or Security Code Word is provided. At the subscriber's request, vehicle information will be provided to authorized 911, police, fire, ambulance, or roadside-assistance providers.

Generally only when the driver presses the OnStar button located in the vehicle does OnStar detect your location. However, OnStar also can query for the vehicle location if your air bags deploy or if you report your car stolen.

Pricing
The dealer-installed three-button system costs approximately $700. The service-packages cost between $200 per year for the basic package up to $800 per year for the full service package.

Volvo On Call system
The Volvo On Call system [24] is a crash-robust telematic system. Volvo On Call is activated by either deployment of in-vehicle air bags or other in-car sensors, or from an emergency SOS and road assistance button provided to the driver. In either case, Volvo On Call sends a text message to a Volvo On Call Alarm Centre via the integrated WISMO (wireless module) [25]. On receipt of the text alert, a voice line is opened for communication between the car and the alarm centre operator; the wireless connection also enables the remote activation of other functions.

The alarm centre operators have access to the car data, GPS-satellite based location data, and direct connections to emergency services such as ambulances, fire, and police departments.

The Volvo On Call button puts you in contact with a service operator who can provide you with a number of services. Like helping you make hotel reservations, unlock your car if you have lost your key, among other services.

Comparison
The services offered by the two systems are in principle identical. The communication differs in the way that OnStar uses an analogue communication network while Volvo On Call uses GSM.

Conclusion
Both these services would provide a precise location of the accident and enable faster response for assistance.

2.1.2 Traffic warnings, notifications, and road information

If cars send their position in intervals so a server can collect their locations, the server can track the car's position and speed. From this information the server can predict traffic jams and inform drivers about various dangerous situations or provide other crucial information.

The server could contain information about all the roads in a country. Information such as route numbers, speed limits, road quality, traffic signs, and other information that would be useful can be provided to the driver. The driver can also request info from the server or receive push notifications if the server detects something significant, for instance, you have exceeded the speed limit or there is a traffic jam about 2 km in front of you. The system could even warn a driver that a car (that is using the system) is standing in the verge in front of you. The server senses that this car is standing still, while it normally would be moving at 110 km per hour. This service is a vision that could be true with the new mobile wireless networks e.g. 3G. However, the delay and reliability must be investigated to provide a service like this.

The unique feature of having the position and route planning handled by a central server means that the server would have instant information about a very large number of cars Information from other road databases should also be available. From this data traffic information can be extracted and fed back to the users. A traffic information system like this would have accurate and up-to-date information. As an example of additional possibilities the ABS sensors of a car could detect a slippery road, then alerts can be sent out to all vehicles entering the same area.

Centrally (from the server side) you **might** be able to request information about the context of a car being in a special position of interest. The car can be equipped with a digital camera and thus the road authority can decide if it must plough this section of highway or not, based on a picture of the road and the sensor data. Thus two-way communication is important.

2.1.3 Routing information/ Navigation

Combining knowledge of ones position with map data can enable us to provide a user-friendly route-assistance service. While driving you should keep your eyes on the road and therefore hands free voice input would be the best alternative to give destinations, and ask questions. The route can be presented as a map, directions by arrows, or voice instructions.

Built-in car navigators are available from numerous companies such as, Blaupunkt, Visteon, Audiovox, Alpine, Clarion, Garmin, Magellan, Geosat, and Pronounced. For more information about these systems visit the respective company's website.

2.1.4 Mobile information/Tourist information

This service gives the user instant information when he is on the move or near some point of interest. For instance the user can be informed of the nearest/cheapest gas station before they run out of gas, or be guided on a tour that tells the user about everything from architecture to history.

One example of a tourist information system is the **Guide project** [27]. This project was developed at the University of Lancaster for visitors to Lancaster. The Guide project developed hand-held computer based tourist guides. These guides are context-sensitive and have knowledge of their physical location and their user's preferences. The units obtain all of their information via a wireless communications link. This enables the units to support interactive services such as ticket booking or enquiries, communications with other users and with the tourist information service, and access to the Internet. The project builds on recent developments in mobile computing technology. In particular, the emergence of relatively cheap PC (formerly PCMCIA) cards providing wireless communications and GPS access enabling the creation of end-systems, which have mobile connectivity and context-awareness.

2.1.5 Weather information

Why should you have to listen or read weather forecasts that do not affect you? With location dependent weather information you always get the most updated and relevant weather forecast. Even if you do not know exactly where you are, the correct (location-dependent) forecast will be provided.

Today Telia is providing this kind of service in Sweden. The user sends a code word via SMS to a specific number or chooses the weather service via WAP. The local weather forecast is automatically sent in a reply [28]. The service is only available for Telia customers.

2.1.6 Yellow pages services

A search query for an address, phone number, or a product can automatically generate a route to that destination or respond with the closest alternative relative to the user's position.

The Swedish company Gula Sidorna offers such a proximity search service. Based on mobile positioning a user can request address information about approximately 25000 stores, restaurants, and services. The service is available via SMS or WAP and is exclusively for Telia customers. [29]

2.1.7 Roadside assistance

Imagine your car break down in the middle of nowhere. You don't have a clue where you are and you need a breakdown truck. This is no problem when you have access to location services. As noted earlier such a service is provided both by the OnStar system and Volvo On Call.

2.1.8 Conclusion

Different location services have different requirements for accuracy and timelines. In tourism and store location services, investigations in Europe show that an accuracy of up to 60 meters and a retrieval time from request to response of about three seconds does not feel inconvenient to a user [9]. This puts rather strict requirements on the system, not only the positioning technology used (as not all can fulfill this requirement), but also on

the way the service is designed. Mobile users are impatient and do not want to wait for the information to be displayed on their mobile phones.
A key issue is to cut down the amount of visible information as much as possible and to show only the information of definite interest [9].

3 Privacy

Privacy is a very important issue when developing location-based services. In most Western countries, it is illegal to use data for purposes other than those for which it was collected [9]. The collection and transfer of location information about a particular device and/or user can have significant privacy implications. Central to a user's privacy are (1) the identity of entities that have access to location data and location information, and (2) whether those entities can be trusted to know the user's policy. However, the interest in convenience-services is big. Users are therefore willing to give up a great deal of privacy, provided they can trust the service providers. If a user is using a GPS receiver, the user can request positioned information without giving out any identifiable information. But if the user sends their position along with their telephone number, via for example a GPRS phone, the identity of the subscriber is known and the service knows the user's location. Thus, to benefit from personalized location information the user may have to give up some privacy.

A number of organizations have defined rules/raised issues regarding protecting user's privacy in location-based services.

Internet Societal Task Force (ISTF):
1. who collects the information?
2. what information is collected?
3. how is this information being collected?
4. where does the information go?

European Union:
1. obtain the subscriber's explicit consent
2. inform about the use and storage of data
3. only use data for the purpose for which it was collected
4. erase personal data after use or make it anonymous
5. possibility to restrict or prevent transmission of personal data
6. no transfer data to a third part without the user's consent

The rules overlap to a significant degree. However, they do not have the force of law everywhere. For example in a location-based service: if you are roaming from one country in which the privacy protection is contractual into another in which there is a legal requirement on privacy protection, how do you make sure that the requirements are satisfied? (This example is from [9]).

The issue of how the user gives their consent to be located is also important. A locating process shall always be initiated by a specific user granting other specific users or applications permission to locate them, never by users requesting permission to locate other people.

Cryptography is a tool to realize the rules to protect privacy. The use of cryptography can maintain confidentiality, authorization, secret key exchange, and digital signatures. A location-based system using such cryptographic mechanisms is for instance the BESTYR project described in the master's thesis by Ulrik Karlsson [31].

In the GPRS standard there exists the possibility to access the network totally anonymously, even from the operator [30]. The feature is thought to work together with road pricing. It is German law that demands full anonymity [30]. To guarantee anonymity neither the IMEI nor the IMSI are sent to the network. While the user is anonymous for the operator the subscriber can be charged via a pre-paid card instead of an ordinary SIM card.

4 Wireless Networks

Wireless networks enable the user of location services to be mobile. Now the user can really take advantage of location services. There are many different types of wireless networks and they each have their own pros and cons. In this project I will focus on GPRS because it best suits the applications that I am targeting. The benefits of GPRS are that you are always connected, but you just pay for the data that is transferred, and because the GPRS network is built on GSM it is wide spread over the world.

4.1 GSM

Global System for Mobile communication (GSM) is a globally accepted standard for digital cellular communication. The advantages of digital systems over analogue systems include ease of signaling, lower levels of interference, integration of transmission and switching, and increased ability to meet capacity demands. The concept of cellular service is the use of low-power transmitters where frequencies can be reused in a cellular pattern over a geographic area [3]. Each transmitter/receiver attached to the fixed network defines a cell.

The GSM circuit switched data service is not really suitable for sending data on a continuous connection or sending of data over long time since the subscriber pays for the time they are connected whether they send any data or not.

Location services via SMS or Cell broadcast is an alternative, but you will then lose the benefit of being always connected. Another drawback is the cost of SMS, which is very high relative to the amount of data that is sent. GSM also provides positioning techniques within the network, which I will come back to later in section 5.2.

4.2 GPRS

General Packet Radio Service (GPRS) is a packet based communication service for mobile devices that allows data to be sent and received across the GSM radio network. GPRS is a step towards third generation (3G) mobile telephony and is often referred to as 2.5G. Here are some key benefits of GPRS:

Speed	GPRS is packet switched. Higher connection speeds are attainable (around 56–118kbps), a vast improvement over the circuit switched GSM networks 9.6 kbps. By combining all GSM time slots in a radio channel theoretical speeds of 171.2 kbps are attainable. However, in the very short term, speeds of 20-50 kbps are more realistic. Finally is it the GPRS operators who are deciding the maximum speed.
Always on connectivity	GPRS is an always-on service. There is no need to dial up like you have to for a circuit switched service. This feature is not unique to GPRS, but is an important and no doubt key feature for migration to 3G. Packet based services also makes multiple services simultaneously available to a device.

New and better applications	Due to its high-speed connection and always-on connectivity GPRS enables full Internet applications straight to the mobile device. Users are able to explore the Internet or connect with their own corporate networks more efficiently than they could when using GSM. There is often no need to redevelop existing applications.
GSM operator Costs	GSM network providers do not have to start from scratch to deploy GPRS. GPRS is an upgrade to their existing GSM network. This makes it easier to deploy, there is little or no downtime of the existing GSM network whilst implementation takes place, most updates are software so they can be made remotely and it allows GSM providers to add value to their business at relatively small costs. The GSM network still provides voice and the GPRS network handles data, because of this voice and data can be sent and received at the same time (depending on the terminal's class).

4.2.1 GPRS Terminal Classes

The term simultaneous (attach and traffic.) is the requirement to simultaneously support GSM GPRS services and GSM circuit switched services and SMS. Note that SMS is a packet switched service, which uses the GSM control channel.

Three GPRS MS classes are identified:

Class A Supports simultaneous attach, simultaneous activation, simultaneous monitor, simultaneous invocation, and simultaneous traffic. The mobile user can make and/or receive calls/traffic on the two services simultaneously subject to QoS requirements. A minimum of one time slot shall be available for each type of service (circuit switched and GPRS) when required. [6]

Class B Supports simultaneous attach, simultaneous activation and simultaneous monitor. Supports only limited simultaneous invocation. Simultaneous traffic shall not be supported. The mobile user can make and/or receive calls/traffic on either of the two services sequentially, but not simultaneously. The selection of the appropriate service is performed automatically, i.e. an active GPRS virtual connection is put on hold, if the user accepts an incoming circuit switched call or establishes an outgoing circuit switched call. [6]

Class C Supports only non-simultaneous attach. If both services (GPRS and Circuit Switched) are supported then a Class C MS can make and/or receive calls only from the manually or default selected service, i.e., either GPRS or Circuit Switched service. The capability for GPRS-attached class-C MS's to receive and transmit SMS messages is optional. Non-voice only MS's do not have to (but may) support emergency calls. [6]

4.2.2 Changes in the GSM Public Land Mobile Network (PLMN)

GPRS introduces two new network nodes in the GSM PLMN. The PLMN is the complete network that an operator manages and owns. The nodes and interfaces of the PLMN are showed in Figure 4.2.2.1.

1. Serving GPRS Support Node (SGSN), which is at the same hierarchical level as the MSC, keeps track of the individual MS's location and performs security functions and access control. The SGSN is connected to the base station system via a Frame Relay connection.

2. Gateway GPRS Support Node (GGSN) provides interworking with external packet-switched networks, and is connected with SGSN's via an IP-based GPRS backbone network. The Home Location Register (HLR) is enhanced with GPRS subscriber information, and the Short Message Service-Mobile Switching Centres (SMS-Gateway MSC and SMS–Interworking MSC) are upgraded to support SMS transmission via the SGSN. Optionally, the Mobile Switching Centre/Visit Location Register can be enhanced for more-efficient co-ordination of GPRS and non-GPRS services and functionality: e.g., paging for circuit-switched calls which can be performed more efficiently via the SGSN, and combined GPRS and non-GPRS location updates. The GGSN is to packet data what the Gateway Mobile Switching Centre (GMSC) is to circuit switched service.

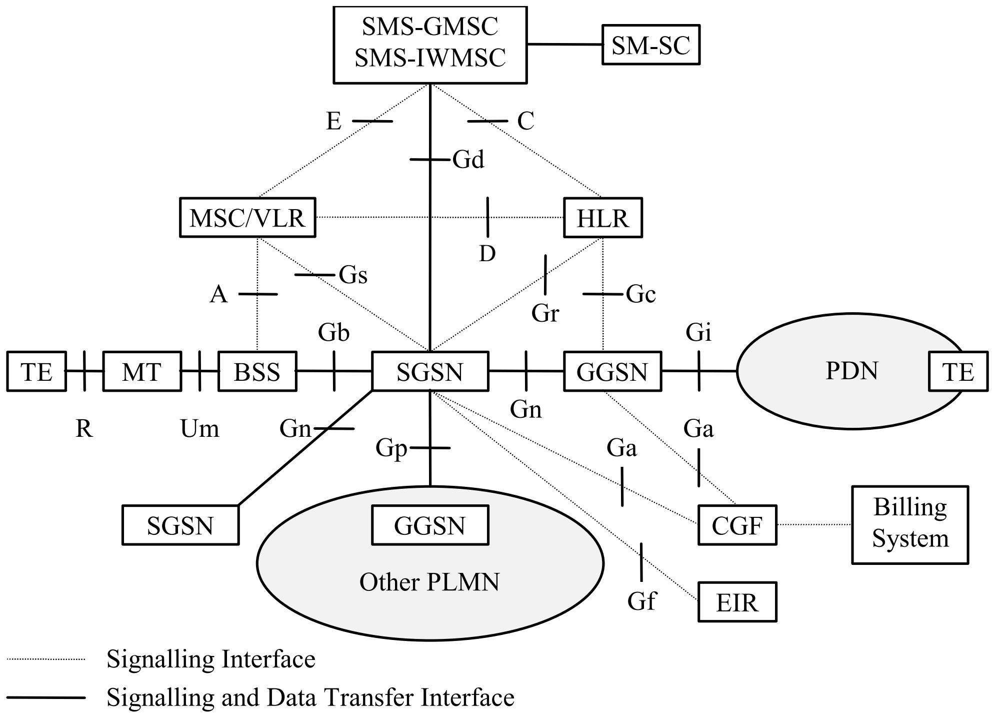


Figure 4.2.2.1. Overview of the GPRS Logical Architecture [7]

4.2.3 Radio Resources

GPRS uses the same radio channel as voice calls, a channel that is 200 kHz wide. This radio channel carries a raw radio stream of 271kbit/s which, for voice calls, is divided into 8 separate data streams, each carrying approximately 34kbit/s. After protocol and error correction overhead, 13 kbit/s is left for each voice connection or about 14 kbit/s for data. Circuit-switched data today uses one voice channel. GPRS can combine up to 8 of these channels. GPRS does not however, use the bits in the timeslot the way circuit switched GSM data does. The net result is that users will be able to enjoy rates over 100 kbit/s. But not all eight-voice channels have to be used. In fact, most phones will be limited to 56kbit/s [5]. The GPRS standard defines a mechanism by which a mobile station can request the amount of bandwidth it desires at the time it establishes a data session [5]. The bandwidth can also vary dynamically. The GPRS user can then benefit from the unused capacity in the network when there are few circuit switched users [30]. GPRS does however, has lower priority in the network than GSM voice calls and GSM data.

4.2.4 PDP context

To make an association between an MS and a GGSN a Packet Data Protocol (PDP) address has to be activated. The PDP-address is an address in a packet data network, for instance IP-address or X.25-address. PDP-addresses can be either static or dynamic addresses

Static address	The operator provides the MS with one or more **permanent** PDP-addresses.
Dynamic addresses	The GGSN assigns the subscriber one or more PDP-addresses based on their **current need**. The subscriber gives back the dynamic PDP address when finished with the data session. In that way many subscribers can use the same PDP address.

A data field (PDP context) includes the address of the MS, SGSN, or GGSN. The PDP context indicates if the address can be used for data transmission or not. There are two different states for a PDP context:

- ACTIVE: PDP-address activated and can be used for data transmission.
- INACTIVE: PDP- address not active.

To activate the PDP context the *PDP context activation* is used, see Figure 4.2.4.1 below.

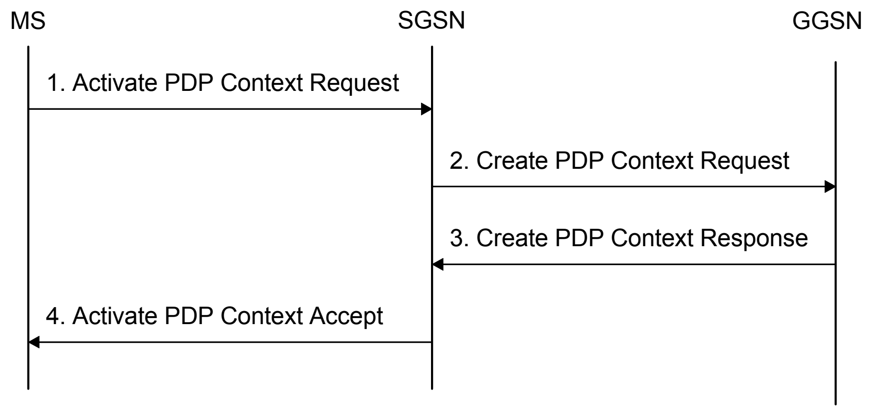


Figure 4.2.4.1. PDP context activation

For static addresses, the PDP context activation can be initiated from the GGSN if an incoming packet arrives and no address is activated. The GGSS can request that the MS, via the Home Location Register, does a PDP context activation.

In the Telia's GPRS network it normally takes 1-2 seconds to establish a PDP-context. The distributed PDP-context is then kept as long as you don't choose to disconnect. In Telia's Mobile Online System the IP address, which will be provided is a dynamic private IP-address. But if you communicate on the Internet you will be provided with a public IP-address. This public IP-address has a time-out of about 6 minutes, and then you will be provided a new public IP-address. The reason is that Telia has a limited number of public IP-addresses in their address pool in the Network Address Translator (NAT), placed in the interface between the GPRS network and Internet. [33]

4.2.5 Conclusions

The benefits of GPRS when dealing with location services is the "permanent" connection; that you only pay for the data you send or receive, not the time you are connected; and the wide spread GSM network

4.3 Third Generation Cellular (3G)

3G is the third generation of mobile telecommunication. IMT-2000 is the term used by the International Telecommunications Union (ITU) for a set of globally harmonized standards for 3G mobile telecom services and equipment. 3G services are designed to offer broadband cellular access at speeds of 2Mbps when stationary, which will allow mobile multimedia-services to become possible [11]. ITU has proposed that IMT-2000 is a CDMA-based standard [11].

In Code Division Multiple Access (CDMA), every transmitter will be allocated an entire frequency band all of the time. CDMA uses codes to create multiple links. In Europe the 3G standard is Wideband-CDMA. WCDMA is often used as a synonym for UMTS.

The advantages of CDMA are [21]:

- There is no plan needed for frequency re-use
- The number of channels is greater than for time and frequency multiplex systems
- Protection against fading of the signal
- Better protection from interference
- Optimum utilization of the bandwidth
- Confidentiality of communication because the two correspondents are the only ones to know the coding algorithm.

The disadvantages are:

- Transmission power must be finely controlled
- The other channels are noise sources (is also an advantage).

UMTS is one of the major new 3G mobile communications systems being developed. Most of the European countries and some other countries around the world have already issued UMTS licenses either by beauty contest or auctions [16].

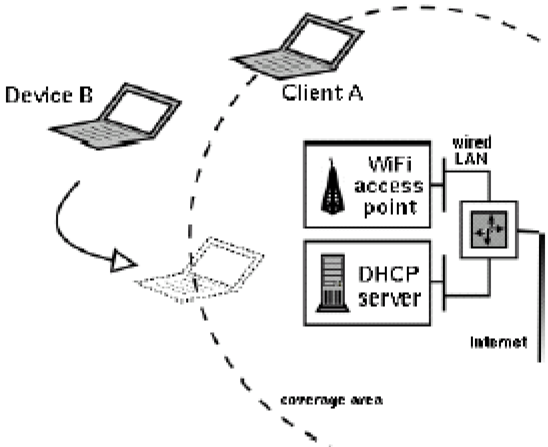
4.3.1 Conclusion

Location-based services are considered to be one of the key features of the third generation networks since it allows higher bandwidth and multimedia services that is suitable for location-based services.

The drawbacks of UMTS are the high investments for licenses and building up the network.

4.4 Wireless Local Area Network (WLAN)

The IEEE 802.11 standard covers the communication and deployment of a WLAN. The standard defines two modes: infrastructure mode and ad hoc mode. In the infrastructure mode, mobile devices connect to and use the network via access points. A single access point can support a small group of users and can has a range of from less than 30 meters up to a couple of hundred meters [12]. The infrastructure mode is shown in Figure 4.4.1 below.



WiFi = Wireless Fidelity, DHCP = Dynamic Host Configuration Protocol

Figure 4.4.1. IEEE 802.11b technology, infrastructure mode [2]

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network, see Figure 4.4.2. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention centre, airport, or where access to the wired network is barred (such as for consultants at a client site).

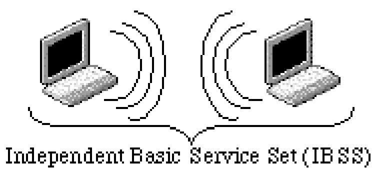


Figure 4.4.2. Ad hoc mode [32]

Public WLANs have been said to be a threat to 3G [17]. So-called hotspots are planed (and many are already installed) to provide access to wireless networks in coffee bars, motorway service stations, airports, and exhibition centres. The aim is for business users to be able to access corporate data and the Internet while on the move.

Although the standards body of the IEEE 802.11 wireless LAN did not standardize location awareness, several research projects use this technology to build location aware systems [2]. Most projects use some sort of triangulation mechanism to determine the exact position of a device.

A drawback for WLAN is its limited coverage. It will be hard to cover whole countries. In certain places though, like San Francisco [17], there is already reasonable coverage today.

5 Positioning technologies

In this section different positioning technologies will be described to get an overview of how the position can be provided for the location based services.

5.1 Global Positioning System (GPS)

GPS is based on 24 satellites and 5 monitoring stations around the world that enable the satellites to broadcast a signal that can be used as a reference in determining the position of a user [9]. The GPS was first made only for the U.S military but since 2000 the full accuracy GPS signal was made available to all users.

GPS works when the user's receiver can acquire a sufficient number of satellites (a minimum of three) and triangulate its distance to them by using the travel time of the radio signal from the satellite. GPS is not only used for navigation, it also gives an unambiguous reference (in time and position) for sensors. GPS uses these "man-made stars" as reference points to calculate positions accurate to a matter of meters. In fact, with advanced forms of GPS you can make measurements to better than a centimetre!

To calculate the distance you need to know the travel time for the radio signal from the satellite in orbit and the speed of the radio signal, which is near the speed of light. The orbits however are affected by the Earth's magnetic field, the solar wind, and the gravitation pull of the sun and moon and will therefore causes some drift over time. The orbits are monitored of by U.S. Department of Defence monitoring stations, using high-precision radar to check the speed, altitude, and position of each satellite. The errors are called ephemeris errors and are relayed back to the satellite, which then can correct the signal by the error so that the precision is maintained. Typically ephemeris data is updated hourly [9].

Because of very short travel time of the radio signal (because it travels with nearly the speed of light) you will not only need a very precise clock, but you will also need to know the time from four different signals. The clock in each satellite is an atomic clock and is extremely precise. The clock in the receiver is not an atomic clock so it uses the four signals to synchronize itself to universal time.

Because the satellite signal (1.575 GHz) is weak, the system works badly indoors, in tunnels, under bridges or near high buildings. Another problem is the multipath error that occurs when the satellite signals reach the receiver along an indirect path, after having bounced off some nearby structure, or the ground. Because the path is not straight, the time delay will be longer, and the distance from the satellite will therefore seem to be longer.

SiRF has developed a GPS receiver that handles these problems: Low level reflected signals bouncing off of far-away objects are simply eliminated. Errors caused by nearby reflected signals are filtered. SiRF's SingleSat positioning mode allows positioning calculations, for short periods, when only a single satellite is visible. SingleSat positioning works by using a single satellite's data to determine how far along a current path the car has traveled. Any errors in position can be corrected as soon as three or more satellite signals are reacquired. SiRF GPS receiver also allows for receiving a signal that is much reduced in power. The sensitivity is 20 dB lower than the threshold standard of –160 dBW. Thus, signals that are indistinguishable for other GPS receivers are detectable for the SiRF GPS receiver. [34]

5.1.1 Assisted GPS

Assisted-GPS (A-GPS) technology overcomes many of the disadvantages of the conventional GPS solution, and achieves high location accuracy at reasonable cost. The assistance to the mobile phone trying to determine its own location comes from the network over the air-interface, and this distributed approach leads to performance levels that exceed those of conventional GPS. What makes this technology work so well is that the wireless network, using its own GPS receivers, as well as an estimate of the mobile's location (within a cell/sector), can predict with great accuracy the GPS signal the handset will receive and convey that information to the mobile. With this assistance the size of the search space is greatly reduced, and the time-to-first-fix (TTFF) shortened from minutes to a second or less. In addition, an A-GPS receiver in the handset can detect and demodulate signals that are much weaker than those required by conventional GPS receivers because of support signals in the network. Only a partial GPS receiver is required in the handset to achieve this functionality, but legacy terminals cannot be used and new handsets are required for this technology to operate.

	Pro	**Con**
Assisted GPS	Superior accuracy, availability, and coverage. Very short TTFF. Maps and databases increase location accuracy (if processing done in network). Minimal impact on battery life. Implementation cost shared by mobiles and the network. System evolves with network upgrades. Location data shared between users and network operator - users can withhold data for privacy reasons, and the operator can restrict assistance to subscribers of this service. Air-interface traffic optimized by distributing data and processing between network and mobiles Accuracy of 10-20 m.	Network assistance increases signaling load. Interoperability between network and mobiles requires additional standards, delaying deployment. New or upgraded handsets needed for initial deployment.

5.2 Network based positioning

All mobile telephone networks today are organized in cells around the antennas of the base stations. As the user moves, the network must keep track of the current location of the user. This information is managed by network databases, so-called Service Control Points (SCP), e.g. the Home Location Register (HLR) and the Visit Location Register (VLR).

5.2.1 Cell ID-Based Positioning, Cell Global Identity, CGI

One of the easiest means of positioning the mobile user is to leverage the SS7 network to derive the user's location. SS7 is a communications protocol that provides signaling and control for various network services and capabilities [20]. When a user invokes a service that requires the MSC to send a message to a location-based service residing on a SCP, the MSC may send a SS7 message containing the Cell Of Origin (COO) or cell ID (of the corresponding cell site currently serving the user). While potentially covering a large area, the COO may be used by location-based services to approximate the location of the user. This type of positioning therefore has a large degree of uncertainty that should be taken into account by the location-based services application in terms of required quality of service.

5.2.2 Timing Advance (TA)

In GSM (and other TDMA systems), each mobile station is allocated a specific frequency and time slot to send and receive data. By measuring the time it takes for the signal to go from the mobile station to the base station, or the reverse, you can derive the position of the user. This is used in GSM to make sure the time slot management is handled correctly [9]. TA typically gives a range resolution of 550 meters [9].

5.2.3 Hybrid of Cell ID and Timing Advance, (CGI+TA)

Timing advance only gives a distance; cell ID only identifies a cell. Combining the two makes it possible to determine the user's distance from the base station in the cell the user is location. Using TA the mobile system can calculate the range in which sector of the cell a mobile station is located i.e. a segment of a shell. Depending of the cell size, the accuracy can be between 100 meters in urban areas and 35 kilometres in rural areas.

5.2.4 Measuring the power from the handset

When a mobile station connects to the base station, in GSM it will measure the power needed to connect to the base stations near it. This measurement can be used to measure the distance from the base station to the mobile station. The precision varies with the cell density and is between 5 and 550 meters [9]. One disadvantage is that the received power may be influenced of factors other than the distance.

5.2.5 Uplink Time of Arrival (UL-TOA)

Signals from the handset are detected at receivers, which can be the base stations, but are usually separate equipment located in the same place as the base station. The propagation from the terminal to the receiver is measured, and the position of the handset is estimated by triangulation. The accuracy for UL-TOA is about 50-150 meters.

5.3 Enhanced Observed Time Difference (E-OTD)

E-OTD is another time-based method, where the handset makes TOA measurements from signals transmitted from more than 3 Base Transceiver Stations, BTS's. The calculation takes place in the handset and the position is then signalled back to the network. Signals from the broadcast control channel (BCCH) are detected at the handset [14].

Some modifications of the mobile station are required. The handset needs to know about reference base stations and neighboring base stations, identity signals, and timing information [9]. It also needs the coordinates for each of the base stations.

If the network really uses the same signal, then E-OTD will work without anything but extra software. If it does not, it will require measurement receivers in the network in the same way as in TOA. But compared to TOA the measurement receivers are much simpler and can be deployed at to serve 3-5 BTS's. Typically, an accuracy of 60 – 200 meters can be expected.

5.4 NIRA's Map aided Positioning (MAP)

MAP developed by NIRA Dynamics [15] is a positioning system that combines smart use of in-vehicle information and digital map information with GSM positioning. The system calculates the absolute position of the vehicle using advanced sensor data fusion of dead-reckoning information and digital map information. GSM positioning is used for initialization after memory loss and self-diagnosis during normal operation. Using commercially available map databases, MAP gives a positioning accuracy comparable or better than GPS based systems – without external support other than GSM positioning for initialization.

The independence from GPS means that MAP does not run into problems in situations like when driving in tunnels, in parking garages, near high buildings, and so on. Further, MAP provides the system integrator with a cheaper solution than GPS based systems since the GPS-antenna, cabling and installation is not necessary. Even more savings are possible with a server-based solution where the map databases and most of the computations are done on a central server hosted by the service provider. Due to its flexible system design MAP is very well suited for distributed solutions. The disadvantages of this system are the increase of communications and signal load and the loss of location privacy.

6. Test Method

This section describes how the test application works and different parts of the test system.

6.1 Goals

The project task in this master's thesis was to evaluate and investigate GPRS communication for navigation-, traffic information-, and other location aware services. The project goal was to investigate whether GPRS is an appropriate communication link for these location-based services.

The investigations will be carried out and evaluated using an implemented test application. The application on the mobile node side sends and receives data (GPS coordinates) to a server over GPRS. Doing so one can see several interesting aspects of the GPRS link, such as delays, IP-addresses, and connection establishment and breakdowns. In the server the coordinates will be compared with a list of points of interest, POI's. If there is a match an information string will be sent back to the mobile node.

Questions to be answered in this thesis are

- What kind of obstacles can occur?
- Does GPRS work or not for the specified services what are the demands for future/ other technologies?
- Is there a different between Telia and Comviq as operators (no availability to Vodafone SIM card)?

The scalability of location services in the GPRS network will also be discussed.

Location-based applications and services are likely to be some of the next killer applications in the telematic industry and the 3G services industry. Positioning and route planning are already planned to be a part of the 3G operator Three's [35] service focus. GPRS has similar capabilities as 3G when it comes to the always-on connectivity. Therefore is GPRS's ability to act as communication link for location aware services important to investigate as a step towards 3G.

In a system that will provide everything from navigation to emergency alerts the reliability of the communication link is crucial. The interesting aspects of GPRS that I am going to investigate are: delays in sending and receiving information, delay in activating a Packet Data Protocol-context (connection set up, see Section 4.2.4) and acquisition of the communication channel (e.g. in an emergency situation you must know that the communication will work.).

In location-based services the position is often dependent on time. For slippery road detection and traffic jam prediction the time can be crucial. In three seconds a vehicle moves almost one hundred meters when driving 100 km/h.

When requesting photos or video streams of road segments the position must be accurate to the reported position.

To be able to investigate these aspects I will look deeper into the packets that are sent over the communication link. An application was built to send and receive GPS-coordinates. To analyze the packets I use the traffic analyzer tool Ethereal [36]. Thus I can see the packet timestamps, IP-addresses, and what happens when a connection breaks down. The application logs all the data that is sent into a log file and saves it in a laptop. The log file contains the GPS coordinates and the packet timestamp. If an error occurs and no data is transmitted an error message is written instead containing the coordinates. The laptop log file can later be compared to the Ethereal log file and the web server log file, to find possible errors and problems, and reasons for errors with the communication. The transmission delay, upstream and downstream, between the nodes should also be measured.

6.2 Mobile node

The mobile node is a Compaq Armada M700 laptop running Microsoft's Windows 2000 operating system, GPS receiver, and Nokia D211 GPRS PC card. The application is built in Visual Basic and uses WinHTTP [37] to communicate with the web server. The main tasks for the application are:

1. Read and decode GPS data
2. Communicate with the web server
3. Save log data in the mobile node
4. Show information of POI if in the proximity of POI

6.2.1 Handling the GPS Data

The GPS receiver transmits data using the National Marine Electronics Association, NMEA, 0183 protocol [44]. The NMEA 0183 Standard, first released in March of 1983, has become a standard protocol for interfacing navigational devices, e.g. GPS receivers. It is based on the RS232 interface [45]. NMEA information is transmitted from a "talker" device to a "listener" device in "sentences" with a maximum length of 80 characters. Each NMEA sentence starts with '$' and ends with [CR][LF].
Example:
$GPRMC,154232,A,2758.612,N,08210.515,W,085.4,084.4,230394,003.1,W*43[CR][LF]

The first 5 characters following the '$' are called the address field. The rest of the line consists of the comma-delimited data fields. The first 2 characters of the address are the so-called Talker-ID, in this example the sender identifies as a GPS device (GP = GPS device). The Talker-ID is followed by 3 characters describing the type of the sentence (type RMC = Minimum Navigation Information in this example). Data fields, which are undefined at send time, are left empty (two commas with nothing in between). An optional checksum can be added to the sentence. This checksum must be preceded by a '*'. Most devices send only a small subset of NMEA sentences. Their sequence and frequency depends on device type and device status. A period of one second is typical.

The application will show latitude, longitude, GPS time, speed, and number of satellites being used. In order to learn this data some specific sentences must be read and decoded from the GPS receiver, see table 6.2.1.1 below. The GPS sentences are read from the USB port where the GPS receiver is connected.

NMEA sentence	Information
$GPGLL	Geographic Position - Latitude/Longitude
$GPZDA	Time & Date
$GPVTG	Ground speed
$GPGSA	Active satellites

Table 6.2.1.1 Read sentences from GPS receiver.

6.2.2 Communication with the Web Server

The second task of the application is to communicate with the web server. It uses WinHTTP (Microsoft Windows HTTP Services [37]), which provides a server-supported, high-level interface to the HTTP/1.1 Internet protocol. Since the mobile node communicates with a web server the WinHTTP service is a fast and simple way to implement the communication channel. The drawback is that the overhead becomes large relative to the load. This investigation will however not be affected by the packet size and cost. For future work however, a more efficient protocol (transmitting method) must be used to reduce the cost for the user. The communication with the web server from the mobile side is showed in Figure 6.2.2.1.

Another problem is that HTTP runs over TCP and TCP is a connection-oriented protocol that guarantees that all the packets arrives in correct order. This implies that each sequence that is sent must be acknowledged and thus the traffic increases. One approach to solve this would be to send data over UDP, that does not acknowledge every sequence, but the company's firewall did not accept such UDP traffic so I had to try with the TCP. However, for future work it must be said that a relay outside the company's firewall could be used so that HTTP could be run over UDP, and the data traffic could then pass through the firewall.

The communication between the mobile node and the web server will strictly be over GPRS. The reason for why GSM DATA and SMS was not investigated was that these communications would result in very high cost compared to GPRS and the bit rate are much lower, 9.11 kbit/s for GSM DATA and 160 characters per SMS message. Investigations show that an SMS message take about 7-8 seconds to transmit [48]. When sending small amount of data GPRS is very cheap because you pay only for data bits sent compared to GSM DATA where you pay for the time you are connected.

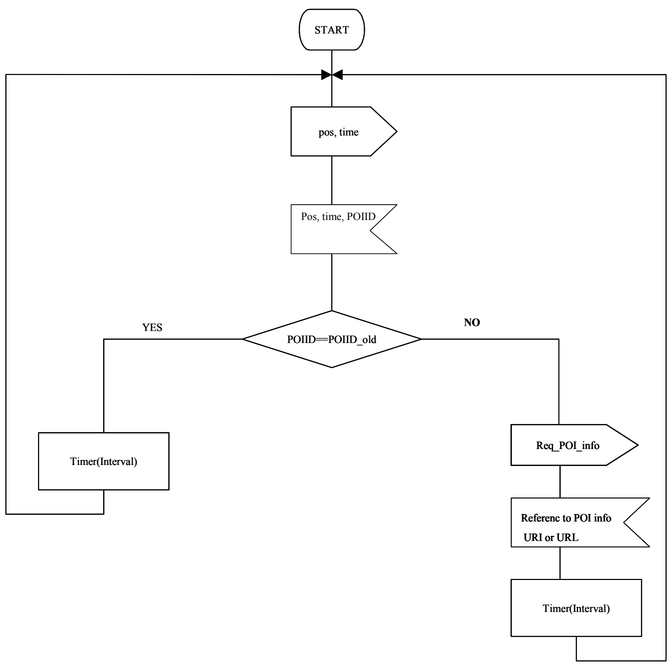


Figure 6.2.2.1 Flowchart showing communication with web server from mobile node

6.2.3 Saving Log Data

The time was synchronized before the experiment was started. The synchronization was made with a program called Tardis [38], which uses the Network Time Protocol, NTP [39], to synchronize the system clock. The Tardis software was installed both at the mobile node and at the web server. The Tardis program could also utilize the GPS protocol NMEA 0183 to synchronize the system clock but unfortunately the server was out of reach for GPS acquisition. Instead I had to exploit timeservers on the Internet and synchronize the system clocks over the company LAN just before the experiment began. I used the same timeserver, time1.stupi.se located in Stockholm, for both nodes.

The application logs the time when packets are sent and received and the time it takes for the data to propagate downstream and upstream. These log times are saved in a text file. If an error occurs the error description is written next to the time.

6.2.4 Show POI Information

A Point of Interest Identification, POIID number is attached along with the time and position. The application tests if this number changes every time data is received. If the POI ID has changed a POI flag is set to request info related to the POI ID from the data base next time data is received. The POIID is negative when no position can be found in a database that was developed. The checking of if you enter a new POI is handled locally in the mobile node so the web server does not have to process that check for every potential user every time data is received, see the example in Figure 6.2.4.1. When the web server see that the POI flag is set it finds the related info as a URL in the database and returns it to the mobile node. The mobile node then request the web page of position related info. This info could for an example notify a traffic accident or traffic jam ahead of you.

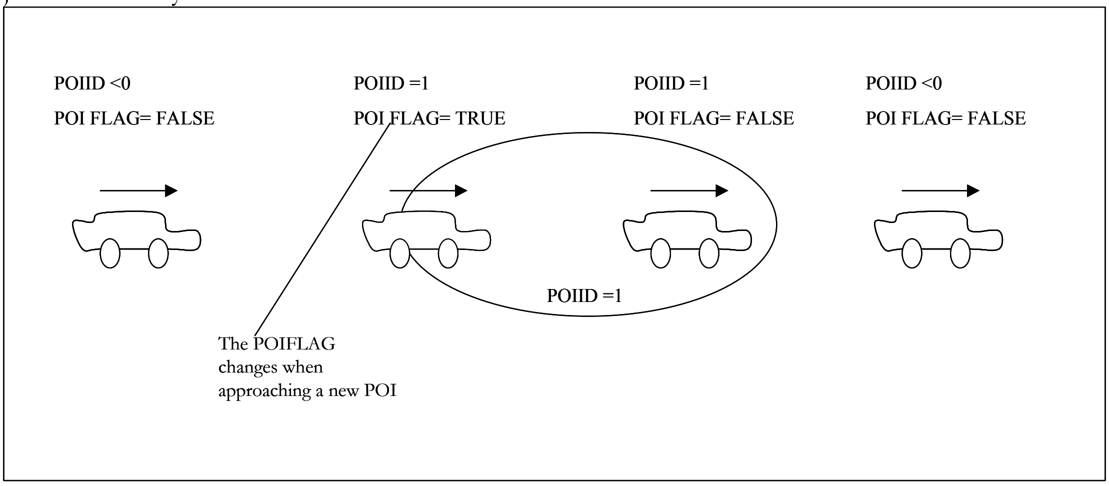


Figure 6.2.4.1 Changing of POIID

6.2.5 Nokia D211 GPRS Module

The GPRS module is a Nokia D211 with data communication capabilities via GPRS, HSCSD, GSM-Data, or WLAN. In this thesis only GPRS will be investigated.

To activate a GPRS data session I use the software Nokia D211 Manager [40] enclosed with the GPRS module. To get a GPRS connection you must enter some settings in "network and dial-up connections" in the control panel, see table 6.2.5.1 below.

GPRS Operator	Telia	Comviq
Phone number	*99#	*99#
IP address	Obtain automatically	Obtain automatically
DNS server Address	Obtain automatically	130.244.127.161 130.244.127.169
User name	-	gprs
Password	-	internet

Table 6.2.5.1 Settings for the Nokia D211

The '*99#' is a special phone number that instructs the phone to go into GPRS data mode.

The Nokia D211 allows 3 timeslots downstream and 1 timeslot upstream which gives a theoretical maximum speed of 40.2 Kbits/s downstream and 13.4 Kbits/s upstream.

Telia is user-friendlier than Comviq since you don't have to enter specific properties to connect to the GPRS network.

6.2.6 The Ethereal Traffic Analyzer Tool

In Windows, Ethereal uses WinPcap to capture traffic. The WinPcap 3.0 alpha 4 was used.

At first I had a problem to get Ethereal to capture the packets. Ethereal uses WinPcap to capture packets. WinPcap is normally not able to work with dial-up connection such as the PPP (Point- to-Point Protocol) in Windows 2000. The cause is the Microsoft NdisWan intermediate network driver (see section 7.1.2) that avoids the protocols to receive packets from PPP links. A trick to bypass this problem is to create the MS Network Monitor system device [41]: WinPcap will be able to utilize this device and work on dial-up links.

7 Evaluation

Running the application and testing the communication generated a lot of data in a number of files and databases, see Figure 7.1. These data were subsequently evaluated and analyzed. The tests where carried out both on the bench and while driving around Stockholm by car. The application always shows the 'Request' and 'Answer' times´, if an error occurs the error and time is written in the application display. Tests were made to see how GPRS behaves in different situations and see if or how often errors occur and why. During the test the traffic analyzer tool Ethereal runs simultaneous with the application. The traffic captured through the GPRS module can then be examined and saved. In the server the database and log statistics from web server can be studied.
All these data can then be compared and investigated in order to find out:

1. Network delay – the mean time to send the position data from mobile node to server and back will be calculated. The log file generated by the application is imported into an Excel data sheet and the average is calculated for each operator and under different circumstances. Differences in the GPRS behavior in rural and urban areas and when driving fast or slow are measured.
2. The PDP context activation delay will be determined. Based on the time from requesting a GPRS data session until getting an IP address. This can be determined from the Ethereal log file.
3. Private or public IP address in the mobile node. Use of NAT or not, change of IP address, will be determined by reading the log statistics from the web server based on which IP-addresses have been sent to it at specific times. Thus I can see if the IP address is same as the mobile node's and therefore a public IP address at the MN, or different from the MN's and therefore a private IP address at the MN. Change in IP address following a period of inactivity can also be examined. A comparison of these behaviors for several operators was made.
4. Error detection – when an error/connection breakdown occur all four files will be investigated to determine the cause.
5. Where do packets spend most of their time? Using tracert I will trace the path packets take in the network.

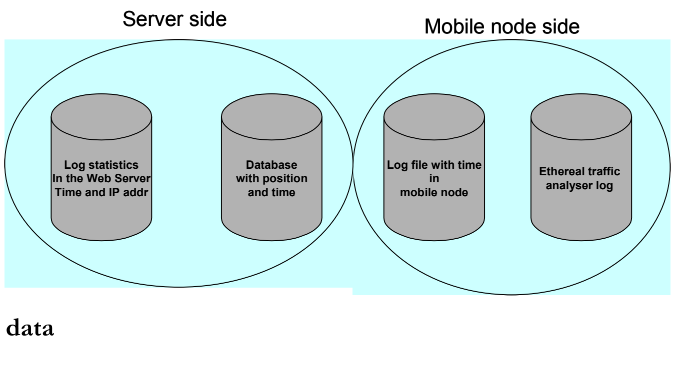


Figure 7.1 Generated data

7.1 Analysis of Data

The analysis where done by studying the generated log files and data. Delay distribution graphs and Tcptrace time sequence plots were made. In the Ethereal logs timestamps and interruptions were examined. The feature of showing info of POI's was also examined.

7.1.1 Network Delay

The timestamp of the IP packet is read and saved in the log file when data is sent to the sever side. The time stamp is then read again when the answer, containing the time when the packet arrived at the server, is returned.

A mean value is calculated for the observed time-differences. By looking at the delays, they do not seem to change significantly when being in rural or urban areas, nor does high-speed movement affect the delay. Comparisons between the operators Telia and Comviq were made. The results from the experiments are summarized in Tables 7.1.1.1 and 7.1.1.2

Telia				
Movement	Fixed location		Mobile	
Direction	Upstream	Downstream	Upstream	Downstream
Median delay	1.5	1.4 s	1.0 s	1.9 s
Average delay	1.5 s	1.5 s	1.2 s	2.3 s
Max delay	2.6 s	4.3 s	8.7 s	20.7 s
Min delay	0.9 s	1.3 s	0.4	1.6 s
Nr of samples	495	495	275	275
Nr of errors	0		0	

Table 7.1.1.1 Test results for Telia

Comviq				
Movement	Fixed		Mobile	
Direction	Upstream	Downstream	Upstream	Downstream
Median delay	0.9 s	1.4 s	1.1	1.2
Average delay	1.7 s	1.8 s	2.0 s	2.2
Max delay	27 s	15.4 s	23 s	15 s
Min delay	0.6 s	1.1 s	0.9 s	0.7 s
Nr of samples	476	476	137	137
Nr of errors	1		4	

Table 7.1.1.2 Test results for Comviq

The Delay distributions are plotted in Figures 7.1.1.2 – 9. They show that the GPRS delay is high, around 1.5 s for the uplink and 2 s for the downlink on average. The maximum upstream delays are up to 27 s, which is totally unacceptable when being mobile. From the Ethereal one can see that delays were generated from several causes:

1. Entering a POI area and requesting POI-info from an external web server simultaneously as sending positioning data (see section 7.1.6).
2. While communicating with the web server, it stops responding on the current port number. A new TCP 3-way handshake must be done with same IP address but different port number. See Figure 7.1.1.1, there is a change from port 1072 to port 1073. The web server has IP address 195.17.228.20 and the mobile node 213.101.169.240.
3. Other undefined delays in the network

195.17.228.20	213.101.169.240	HTTP	HTTP/1.1 100 Continue
213.101.169.240	195.17.228.20	TCP	1072 > http [ACK] Seq=152450847 Ack=613538969 Win=17408 Len=0
213.101.169.240	195.17.228.20	TCP	1072 > http [FIN, ACK] Seq=152450847 Ack=613538969 Win=17408 Len=0
213.101.169.240	195.17.228.20	TCP	1072 > http [FIN, ACK] Seq=152450847 Ack=613538969 Win=17408 Len=0
213.101.169.240	195.17.228.20	TCP	1073 > http [SYN] Seq=195369711 Ack=0 Win=16384 Len=0 MSS=1460
213.101.169.240	195.17.228.20	TCP	1073 > http [SYN] Seq=195369711 Ack=0 Win=16384 Len=0 MSS=1460
213.101.169.240	195.17.228.20	TCP	1072 > http [FIN, ACK] Seq=152450847 Ack=613538969 Win=17408 Len=0
195.17.228.20	213.101.169.240	TCP	http > 1073 [SYN, ACK] Seq=657602499 Ack=195369712 Win=17520 Len=0 MSS
213.101.169.240	195.17.228.20	TCP	1073 > http [ACK] Seq=195369712 Ack=657602500 Win=17520 Len=0
213.101.169.240	195.17.228.20	HTTP	POST /storepos.asp HTTP/1.1

Figure 7.1.1.1 Example from the Ethereal log

The delay distribution plots from Telia and Comviq did not differ much.
During the recorded experiment with Telia no breakdowns occurred, however breakdowns did occur during other tests, which were not registered. The breakdowns were of the same nature as for Comviq.

Tests were also made to see the delay contribution from the server, but the results were so small, around 10 ms, that the contribution could be neglected and a more thorough investigation was therefore not made.

In the following figures the delay distribution and the cumulative distribution for the network delay under different circumstances are showed.

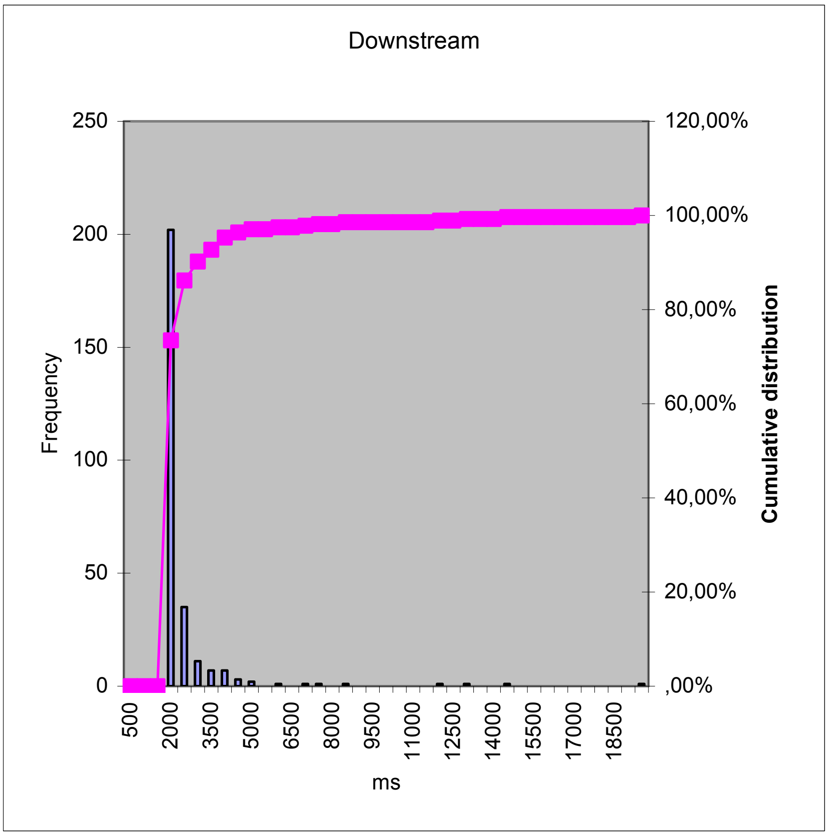


Figure 7.1.1.2 Downstream delay distribution, mobile movement, Telia

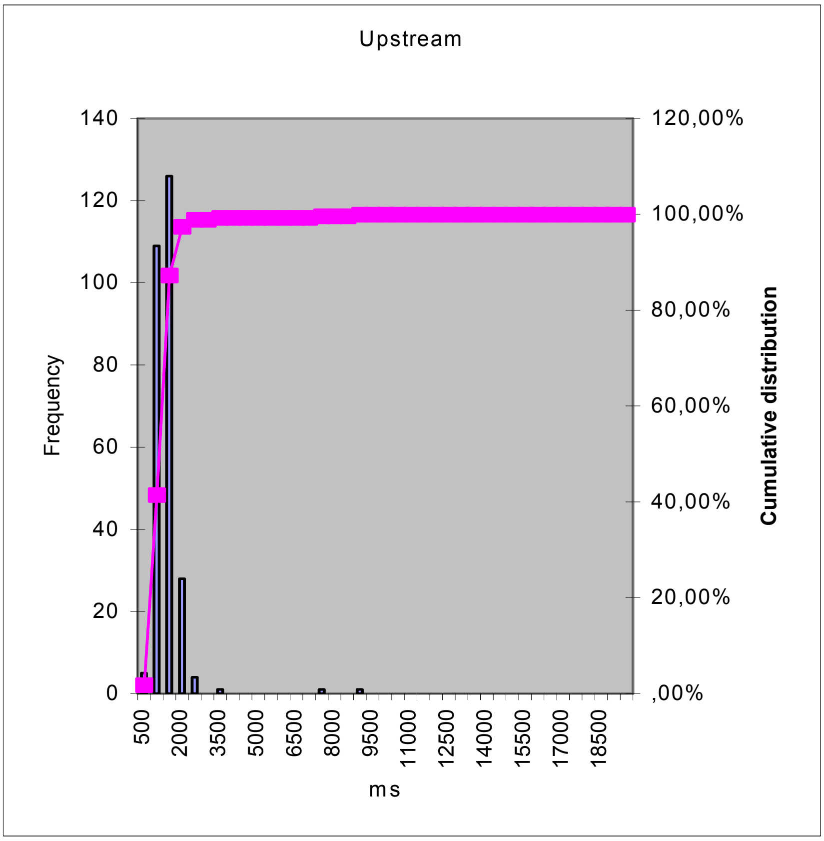


Figure 7.1.1.3 Upstream delay distribution, mobile movement, Telia

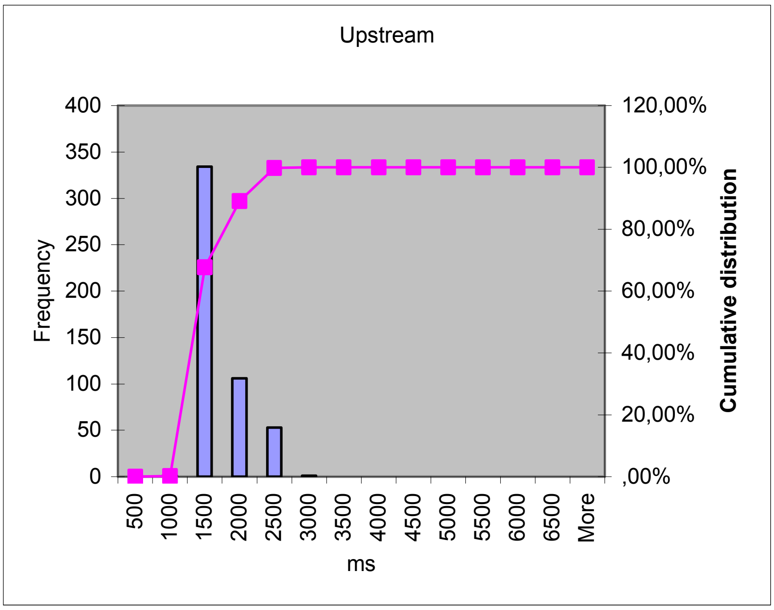


Figure 7.1.1.4 Downstream delay distribution, fixed location, Telia

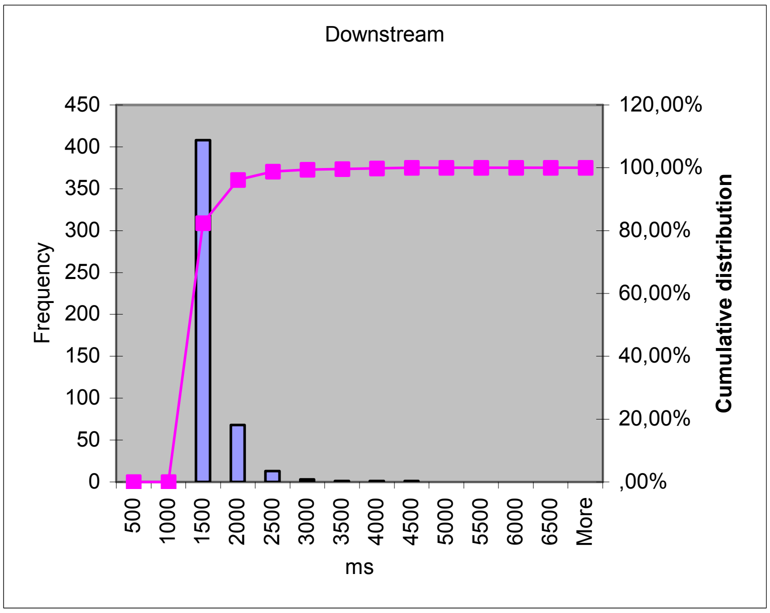


Figure 7.1.1.5 Upstream delay distribution, fixed location, Telia

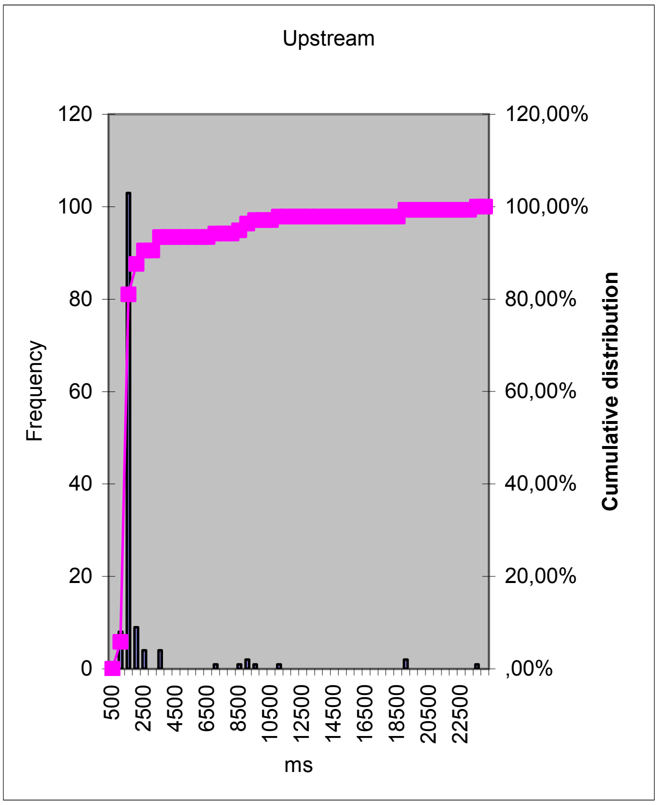


Figure 7.1.1.6 Downstream delay distribution for Comviq, mobile movement

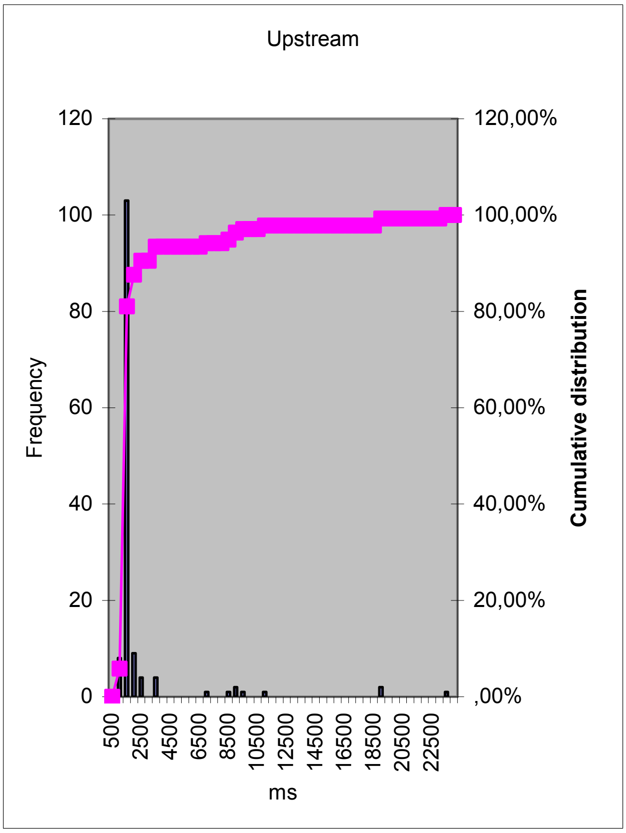


Figure 7.1.1.7Upstream delay distribution for Comviq, mobile movement

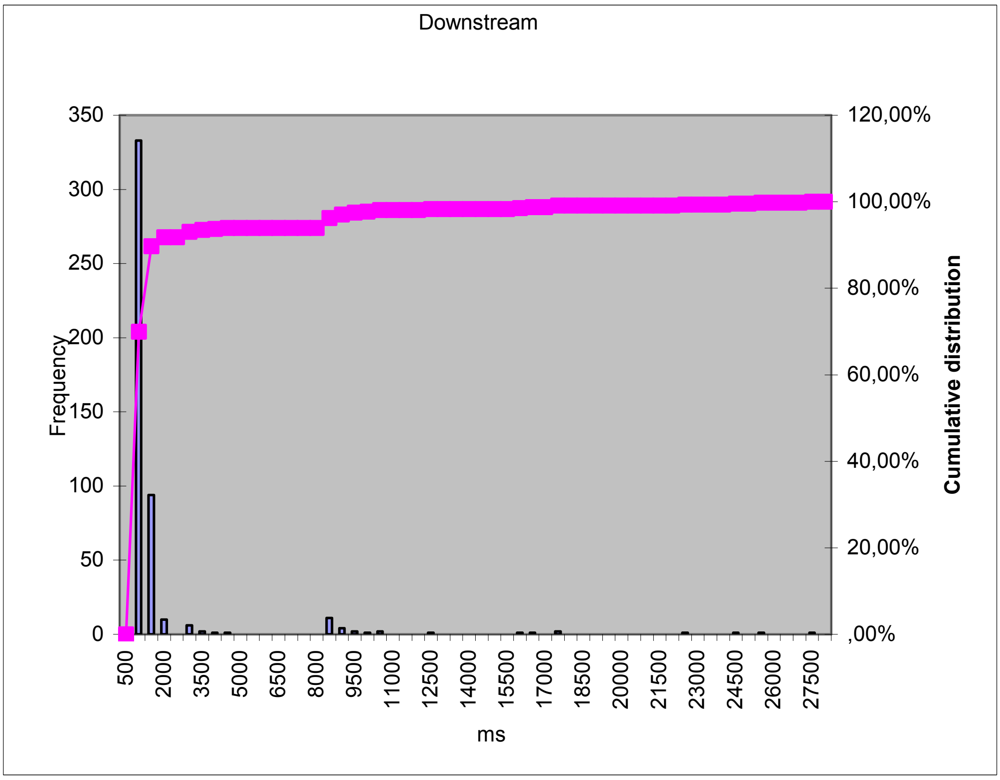


Figure 7.1.1.8 Downstream delay distribution for Comviq, no movement

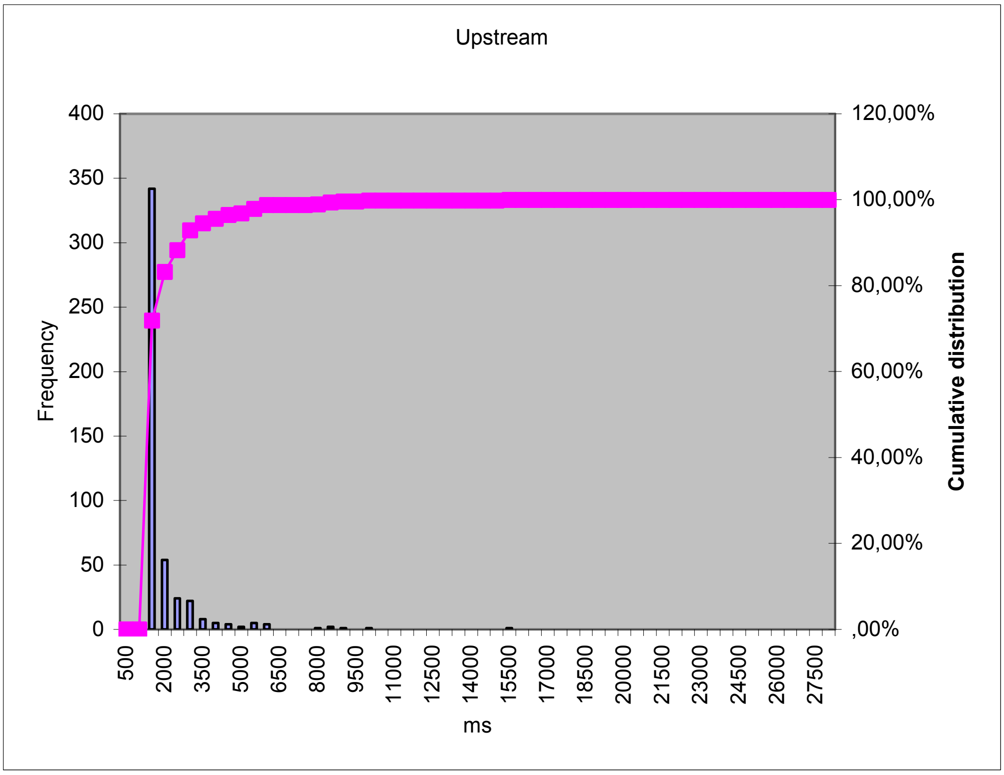


Figure 7.1.1.9 Upstream delay distribution for Comviq, no movement

7.1.2 PDP Context Activation Delay

This delay is of importance for the scalability of the Location aware communication service. Since the operators do not have enough IPv4 addresses to have one for every vehicle in use in Sweden (let alone more populous countries). If the user could have PDP context activated but return the IP address after each use, more users could exploit the small set of IP addresses. The user could send their position along with a request "is there any info for me at this location?" and then deactivate the IP address if there was no info.

In the Ethereal-log all Ethernet traffic to and from the GPRS module can be seen. When activating the GPRS module, the IP address is not assigned immediately. First the GPRS module must send and receive some authentication- and configuration information. This is done via the PPP Link Control Protocol and PPP IP Control Protocol, which are directly on top of the MAC (medium access control) layer.

In Microsoft windows operating system a NDIS WAN miniport [42] is used to communicate over PPP, see Figure 7.1.2.1. NDISWAN converts send packets, passed to it by protocols, from LAN to PPP format. It performs the reverse conversion for received packets passed to it by WAN miniport drivers. The NDISWAN maps WAN packets into Ethernet packets, as it binds to the TCP/IP protocol stack as an 802.3 adapter. This can be seen when the GPRS link is established in the Ethereal log file. Two Ethernet addresses are showed in the log; hence GPRS uses two channels for its connection establishment.

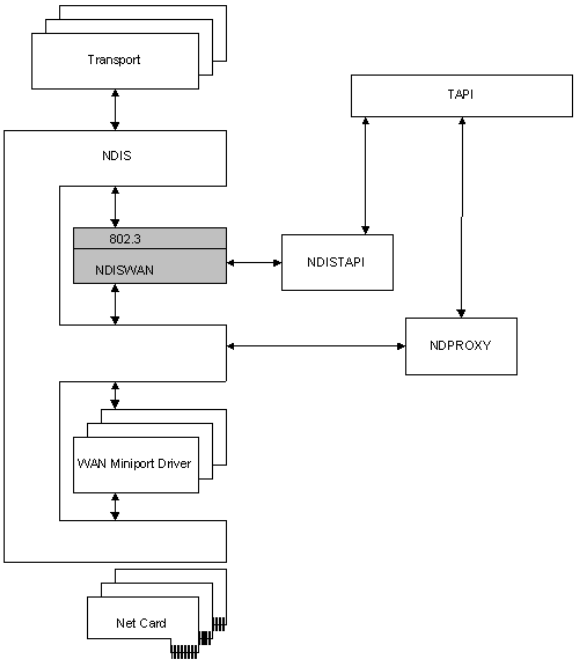


Figure 7.1.2.1 The Microsoft Windows conversion from PPP to Ethernet packets (the 'Transport' in the figure corresponds to PPP)

The delay can be measured because the first packet is sent from the mobile node only after the GPRS module receives an IP address. The delay I could measure was unfortunately only the compound delay of the PDP context activation delay and the IP address assignment delay. I did not find a way to separate these two delays. The PDP context activation delay is thus lower than the one registered. The results are showed in Table 7.1.2.1 below. The delay implies that the smallest interval of sending positioning data upstream must be around 10 seconds.

Operator	Telia	Comviq
Compound delay of PDP Context activation- and IP address assignment delay	1-2 s	3-4 s

Table 7.1.2.1 Result of the PDP context activation and address assignment delay

7.1.3 IP Addresses, use of Network Address Translator

To see what kind of IP address were assigned by the operators one must look at the log files at the web server. By comparing the IP address at the mobile node and server one can see if they are public or private, dynamic or static, and if the operator uses a NAT.

Telia

One can see that Telia uses a NAT as they said in former interviews [33]. Thus the IP address is a private dynamic address as can also be seen at the mobile node where you get an IP address from the 10.x.x.x address space. This shows also up as the IP address at the mobile node being different from the one at the web server. Telia said also that the IP address in the NAT should change after six minutes if one did not use the GPRS link. My tests have not shown this. Once you have a connection you keep the same private IP address in the NAT even if you have not sending any packets over a period longer than six minutes, I waited up to 25 min.

Comviq

Comviq assigns dynamic public IP addresses; the IP addresses are the same at both nodes. During periods of inactivity the IP address does not change, I waited up to 40 minutes of inactivity. One cannot see any trace of a NAT.

One conclusion is that Comviq provides easier access to their customer by other interested parties compared to Telia. On the other hand Telia's GPRS network is safer from an integrity point of view.

The use of NAT combined with port mapping (NAPT) could improve the scalability by a factor of ~64K, but then you can't run other applications from your mobile at the same time because they too would need to have a distinct port number in order to demultiplex. The operator could use private address (perhaps from the 10.x.x.x space), but now each information provider would have to have a server inside this private address space - or the operator would need to provide a proxy inside this space, which encapsulated the traffic inside a tunnel to send it to the information provider's service.

7.1.4 Connection Breakdowns

Three types of errors were experienced when running the application;

- Application cannot establish a connection with the server but re-establishment can be done automatically.
- Operation times out (the application has a timeout of 30 seconds).
- Connection completely breaks and a new PPP session must be initiated.

When the two first errors occur the same IP address is kept. These errors are probably due to delays in the network and packet losses, which can occur when the signal quality is poor, or cell re-selections due to the cell update procedure. These temporary breaks can last for a few minutes.

The last error is fiercer, without any warning the connection completely dies. In the Ethereal log a PPP termination request is sent from the same Ethernet address as when the PPP was initiated. A new PPP session must be initiated, a PDP context activation will be performed, and a new IP address will be assigned. From [43]: "Termination-Request and Termination-Ack are used to tear down a link in a graceful manner, they allow individual network protocols to be shut down to conserve resources or for security reasons". One possible cause is thus network resources could be low and since GSM voice traffic has higher priority than GPRS the link is terminated.

The termination request message is normally sent from the mobile node when you are doing a voluntary deactivation of the GPRS link.

A countermeasure would be if the application could detect the error and establish a new connection automatically.

The possible causes and my investigation of them is summarized in table 7.1.5.1 below.

Possible causes	**Possible countermeasure**	**Result**
Disturbance in the network	Not able to control	-
Bugs in the Nokia D211 Manager	Download the latest version of the software	No Result
Problems in the Nokia D211 hardware	Search the Nokia FAQ support site	No Result
Handovers in network while changing Routing area	Drive in the same area several times and see if the error repeats when entering and/or exiting the same area.	Shows no systematic errors, The errors are not bond to a location/area.
Intra-zone handovers	Not able to control	-
Sudden signal quality degradation	Not able to control	-

Table 7.1.5.1 Possible connection breakdown causes

7.1.5 Network Bottlenecks

These tests were made with the MS DOS tracert (traceroute) command. The tracert command is used to estimate the path that packets will take to a given destination and the number of hops required for those packets to get to this destination. The test where made from the mobile node running the command tracert to my test web server with IP address 195.17.228.20.

Telia

When running traceroute with the Telia SIM card the request timed out. The reason is probably the NAT and other safety precautions in the network not allowing ICMP packets. The request timed out and did not give any clue about the route after passing node 10.144.0.1, which probably is the default gateway, see Figure 7.1.5.1. 18 hops were required to reach the web server. I also tried with SNMP to get information about neighboring and intermediate routers but that gave no result since there was no response.

```
C:\>tracert 195.17.228.20

Tracing route to 195.17.228.20 over a maximum of 30 hops

  1  1402 ms   862 ms   861 ms  host-144.0.1.private.mobileonline.telia.com [10.
144.0.1]
  2   891 ms   852 ms   861 ms  host-144.0.1.private.mobileonline.telia.com [10.
144.0.1]
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18  1342 ms   861 ms   861 ms  195.17.228.20
```

Figure 7.1.5.1 Example of traceroute for Telia GPRS network

Comviq

Here you can see the nodes between the mobile node and the web server. There are no particular nodes that are distinguished by extreme delays. The delays are around 700 ms at each node. 10 hops were required to reach the web server, see Figure 7.1.5.1.

```
C:\>tracert 195.17.228.20

Tracing route to 195.17.228.20 over a maximum of 30 hops

  1   731 ms   691 ms   671 ms  m213-101-158-1.swipnet.se [213.101.158.1]
  2   721 ms   691 ms   691 ms  gprs1-gw.fasteth4-0s2.swip.net [130.244.228.25]

  3   721 ms   691 ms   691 ms  stbf2.ve.swip.net [130.244.187.254]
  4   701 ms   691 ms   691 ms  stb1-core.gigabiteth1-0.swip.net [130.244.194.14
5]
  5   721 ms   701 ms   681 ms  stb2-core.srp6-0.swip.net [130.244.198.21]
  6   721 ms   671 ms   681 ms  v10-bar-sto-pos0-1-0.global-ip.net [130.244.193.
54]
  7   721 ms   671 ms   681 ms  v16-car-sto-fe0-0.global-ip.net [194.52.1.53]
  8   721 ms   681 ms   711 ms  mobileinnovation-cpr-sto.global-ip.net [194.52.3
.10]
  9   721 ms   721 ms   731 ms  195.17.228.65
 10   701 ms   671 ms   701 ms  195.17.228.20
```

Figure 7.1.5.1 Example of traceroute for Comviq GPRS network

7.1.6 POI Information Downloading

The presentation of information of POI when entering a POI area worked well. The simultaneous request from other external web server did not interfere with the reporting of position. Slightly higher delays were however experienced when reporting the position. From the Ethereal log time-sequence graphs were made to illustrate the communications, see Figure 7.1.6.1. Plot (a) and (c) shows positioning reporting and plot (b) and (d) shows the POI information downloading. See [49] for explanation of the plots. No extraordinary events are observed during the downloading of POI-information in the time sequence plot. The round trip times, RTT's were also plotted, here one can see that the RTT for the position reporting increases when the POI information download begins.

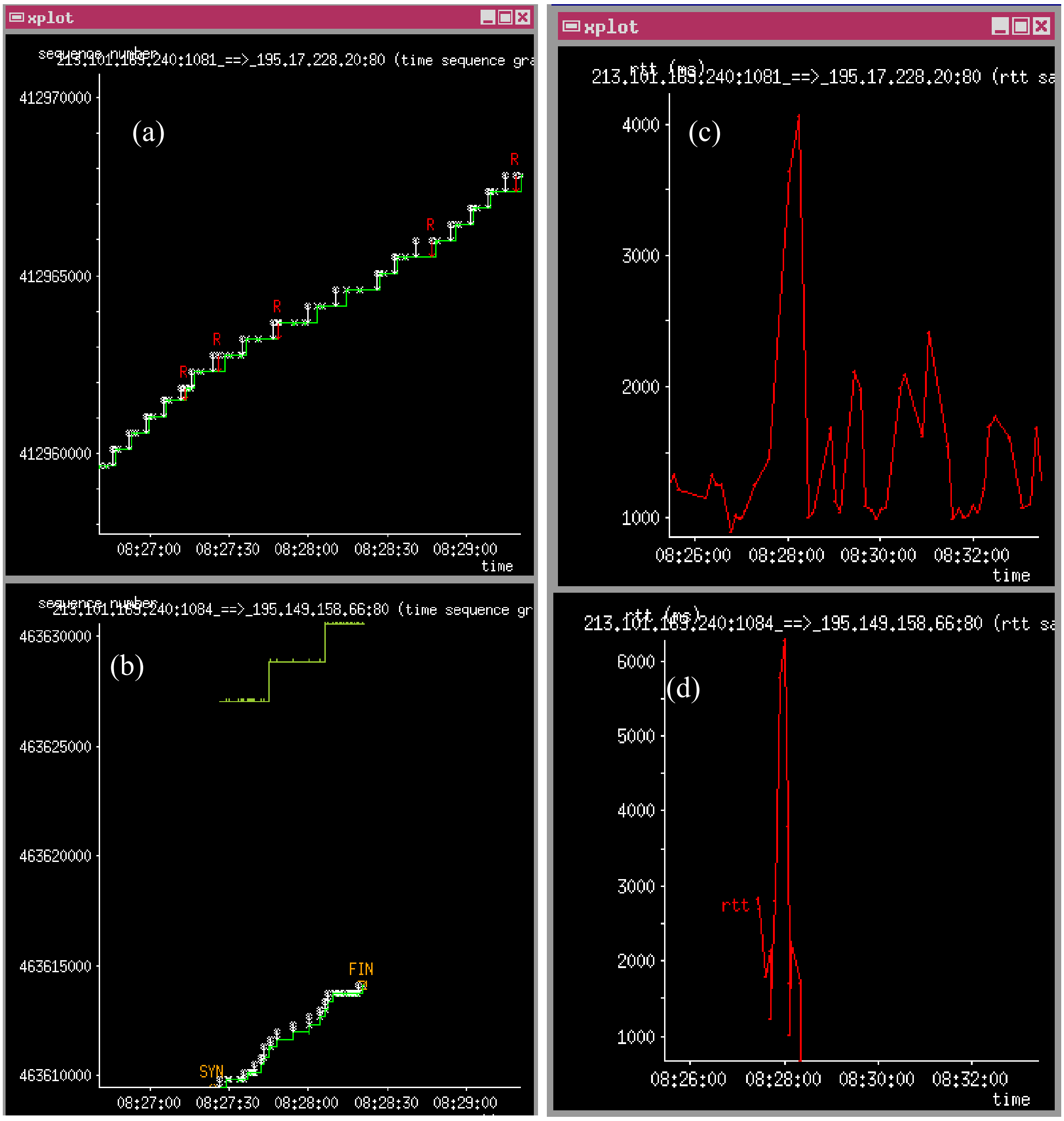


Figure 7.1.6.1 Time-sequence and RTT graphs. Plot (a) and (c) shows the position reporting. Plot (b) and (d) shows the POI information download.

The overall experience when testing this feature was that as long as you had a connection when entering a POI area the information showed up before leaving the area, which was a basic condition. However many times the connection was down when entering the area and nothing showed up. The POI position was determined with GPS, an area (approximately 150 x 150 m) around the POI position was stored in a database along with the POIID and POIINFO.

8 Conclusions

The goal with this master's thesis was to find out whether GPRS is a suitable carrier for location-based services. Several tests were made with a built application that sent coordinates to a web server with a database. When entering some special Point of Interest areas, whose position are stored in the database, information about the POI was sent back to the mobile node. Some of the tests succeeded and some failed. Taken as a whole the test and analysis gave a good picture of the GPRS ability to work as bearer of location-based services.

The conclusion is that GPRS works, but errors occur and the transmission time of information in the network is quite long compared to store locally information in the handset/ car-system. The advantage of having all the information centrally in a server is that the service can provide dynamic information. However, GPRS, with the quality of today, works for only certain types of services that are not that dependent on time or require that the connection never fail. Improvement for future technologies should be faster transmission times in the network so the user feels convenient with the service and does not have to wait long for the requested information, thus that the reported position is current, and more reliable acquisition of the communication service requires fewer breakdowns.

The use of HTTP over TCP for the communication was not that well suited for these kind of small data transfer due to the high overhead (60 percent upstream and 30 percent downstream) for the position reporting. Unfortunately no tests with UDP could be made due to the server's firewall.

The scalability problem is an important issue where the operators must have capacity for up to 10 million users to be of commercial interest. Ways to scale up could be solved by combining NAT with port mapping to scale up the service by 64K unfortunately with the drawback of difficulty in demultiplexing other services. Private IP address assignment is another approach, but then each external information provider would have problems to get access to the users.

9 The Future

With the introduction of 3G cellular system and built in assisted GPS in the handset the location based service industry will grow. The 3G operators could have the positioning reporting in a special signal channel, the integrity of the user must however be protected (see section 3 about Privacy).

Faster download of web content over GPRS can be achieved with the use of a proxy server. Work about this has already been done and could be of interest to investigate in conjunction with location based services. See for example GPRSweb by Rajiv Chakravorty, Andrew Clark, and Ian Pratt [46].

Interaction with Control Area Network (CAN) or Onboard Diagnostics (OBD-2) busses
For remote surveillance and diagnostics of the vehicle The CAN bus or OBD-2 can be integrated with the application. The data bus has connections to all the many sensors that modern cars have. Here you can extract speed, temperature, fuel injection statistics, airbag activation, seat belt stretcher, and service online. Many services can benefit these available data. Work has been done in this area, for example Onstar, Volvo Oncall systems, and the exjobb by Mikael Gunnarsson, "Truck-Trailer Wireless Connections" [47]. However, all the available data from the CAN bus has not been exploited in these systems.

The scalability problem must be investigated and solved. Which solution works best with the existing network and location-based services, with respect to minimal changes and cost needs to be determined.

References

[1] ATX Technologies. Available from: http://www.atxtechnologies.com
Date of access 2002-06-20

[2] S. Fischmeister, G. Menkhaus,. *The Dilemma of Cell-Based Proactive Location aware Services.* Available from: http://www.softwareresearch.net/reports/C42.pdf. 2002.
Date of access 2002-06-13

[3] *Global System for Mobile Communication*, The International Engineering Consortium. Available from: http://www.iec.org/online/tutorials/gsm.
Date of access 2002-06-10

[5] *GPRS, white paper.* Usha Communications Technology.
Available from: http://www.mobilein.com/GPRS.pdf. 2000.
Date of access 2002-06-10

[6] *GSM 02.60 V8.1.0 (1999-07) Technical Specification Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description, Stage 1.*
Available from: http://www.3gpp.org/.
Date of access 2002-06-12

[7] *GSM 03.60 V7.8.0 (2002-01) Technical Specification Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2*
Available from: http://www.3gpp.org/.
Date of access 2002-06-10

[9] J. Hjelm. *Creating Location Services for the Wireless Web: professional developer's guide.* ISBN 0-471-40261-3. Wiley & Sons. 2002.

[11] Mobilecomms Technology *IMT-2000 Global Standard,International.*
Available from:
http://www.mobilecomms-technology.com/projects/imt2000/index.html#imt20003.
Date of access 2002-05-13

[12] WLANA. *Introduction to Wireless LANs.*
Available from: http://www.wlana.com/learn/educate1.htm#over. 2001.
Date of access 2002-06-14

[13] I. Koeppel, *GIS and Location Services on the Web - An ESRI White Paper.*
Available from:
http://www.esricanada.com/english/engine/prod_detail.asp?productid=30&version=2#.
Date of access 2002-06-11

[14] B. Ludden, Vodafone. *Location technology*. Power point presentation from the Location Interoperability Forum.
Available from: http://www.locationforum.org/Home.htm. 2000. Date of access 2002-05-28

[15] NIRA dynamics. Available from: http://www.niradynamics.se/
Date of access 2002-06-27

[16] *Overview of The Universal Mobile Telecommunication System***.** Umtsworld.com
Available from: http://www.umtsworld.com/technology/overview.htm. 2000.
Date of access 2002-06-20

[17] D. Rae, *WLAN hotspots to melt 3G profits.*
Available from: http://www.networknews.co.uk/News/1130955. 2002.
Date of access 2002-06-12

[19] R. Skewes, *Mapblast a location service.*
Available from: http://www.geocities.com/madpup8ca/. Date of access 2002-06-18

[20] *SS7,* Available from: http://www.mobilein.com/ss7.htm
Date of access 2002-06-15

[21] J. Tisal, *The GSM Network, GPRS Evolution: One Step Towards UMTS* ISBN 0-471-49816-5 Wiley & Sons. 2001
[22] Mobitex, a wireless network. http://www.mobitex.org/. Date of access 2002-07-28
[23] The OnStar website. http://www.onstar.com/. Date of access 2002-08-06
[24] Volvo OnCall. Information about the system. http://vcc.volvocars.se/voc/voc.asp. Date of access 2002-08-06
[25] Wismo (Wireless Standard Module) http://www.wavecom.com/about/what_is_wismo.php. Date of access 2002-08-06
[26] Bosch's CAN (Controller Area Network) bus. www.can.bosch.com. Date of access 2002-08-07
[27] Guide project, a tourist information system. http://www.guide.lancs.ac.uk/. Date of access 2002-08-07
[28] Telia *"väder nära dig"- service.* Weather service http://www.teliamobile.se/picpath/pdf/Vader_nara.qxd.pdf. Date of access 2002-08-10
[29] Gula Sidorna. Yellow pages proximity search, http://mobile.gulasidorna.se/mobpos.html. Date of access 2002-08-10
[30] Telia, *GPRS- en introduktion*, documentation made by Telia Research AB, 1997-10-08.
[31] U. Karlsson, *Electronic payment and control functions in the BESTYR project*, M.Sc. Thesis, Royal Institute of Technology, Teleinformatics, April 2000.
[32] Northwestern University Information Technology, *WLAN information*, http://www.tss.northwestern.edu/wireless/faq_wir.html
[33] E-Mail correspondence with Stefan Svärd at Telia mobile. 2002-08-21
[34] SiRF website, information about SiRF GPS receivers. www.SiRF.com
[35] Tre, 3G operator, www.tre.se.
[36] Ethereal traffic analyzer tool, www.ethereal.com.
[37] Microsoft WinHTTP, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winhttp/http/winhttp_versions.asp
[38] TARDIS, Software for synchronization. http://www.kaska.demon.co.uk
[39] Network Time Protocol http://www.ntp.org/
[40] Nokia D211 Manager, http://www.nokia.com/cda1/0,4267,1449,00.html
[41] Make WinPcap use on dial-up links, http://winpcap.polito.it/misc/dialup.htm, Date of access 2003-04-10.
[42] NDIS WAN miniport an overview, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/network/hh/network/208mwan_18br.asp
[43] J. Carlson, *PPP Design and Debugging* ISBN 0-201-18539-3, Addison- Wesley
[44] The NMEA 0183 Protocol for GPS, www.nmea.org
[45] Information about the RS232 interface, http://www.camiresearch.com/Data_Com_Basics/RS232_standard.html
[46] R. Chakravorty, A. Clark and I. Pratt, *GPRSWeb: Optimizing the Web for GPRS Links,* 2003 May. http://www.cl.cam.ac.uk/~rc277/GPRSWEb_html/paper.html
[48] M. Gunnarsson, *Truck Trailer wireless connections.* M.Sc. Thesis, Royal Institute of Technology, Teleinformatics, December 2001
[48] P. Lindström and P. Velenik, *Evaluation of Architectures for the Development of Secure Mobile Applications,* M.Sc. Thesis, Royal Institute of Technology, Teleinformatics, February 2003
[49] TCPTRACE, interpreting time sequence plots and RTT plots, available from http://www.tcptrace.com/manual/graphing.html. Date of access 2003-06-29