Proposal for a Mobile Service Control Protocol

Jens Kammann
Institute for Communications and Navigation
German Aerospace Center (DLR)
P.O. Box 11 16, D-82230 Wessling, Germany
Fax: +49 8153 28 1442
email: jens.kammann@dlr.de

ABSTRACT
This paper introduces an access network independent mobile service control protocol. After providing a brief overview of the current Internet access techniques, it summarizes the most common application protocols of the Internet based on TCP. Therefore, these application protocols get differentiated in protocols with and without state and the possibilities of proxies for them is evaluated. Based on the results thereof and a scenario of a mobile user accessing Internet services using Bluetooth equipped handheld devices, a new protocol is introduced which allows mobility, supports devices with limited resources, such as smart phones and PDAs and keeps the existing TCP/UDP socket interface to avoid modifications of client side applications.

KEYWORDS
Wireless Networks and Mobile Computing, Network Protocols

1. Introduction

Speaking of Internet access we usually think of browsing the World Wide Web, reading and writing E-Mails and transferring files. Although the Internet has lead to a wealth of protocols, only a few are widely spread: HTTP for retrieving web pages, FTP for file transfer and POP3/IMAP4 for E-Mail service - all of them using the Transport Control Protocol (TCP).

Solutions for the mobile Internet usually try to copy the framework of the stationary Internet access but face problems due to limited device capabilities. Smaller screens of cellular phones or PDAs can be accommodated by new Mark-up languages like cHTML or WML, although different versions and very limited fault tolerance of today's mobile browsers prohibits seamless portability of services.

What is more, mobile devices usually emulate a full network protocol stack even if device resources would not allow for a full featured stack. This, coupled with the inherent problems of TCP with unstable or changing network conditions [1] with respect to connectivity and throughput necessitates a more flexible solution that does not only provide a foundation for information exchange in a heterogeneous network environment, but also puts a focus on how to provide network independent services to the user.

2. Methods to support user mobility

User mobility is typically provided on the network or on the session layer (see figure 2). Network layer mobility can be achieved with Mobile IP [2] by assigning two IP addresses to the client. One is the fixed home address and the second is a care-of-address, which changes at each new location. In contrast, session layer mobility does not try to keep TCP sessions open, but utilizes the ”session resume” function of WTLS. Or, in the case of a Virtual Private Network (VPN), the client is assigned a second IP address which remains the same even if the primary one changes due to link re-establishment. All three methods allow ongoing TCP connection while the physical link changes. However, if e.g. a handover between networks takes too long, TCP timeouts may occur which in most cases results in error messages passed on to the user.

3. Scenario

Figure 1 shows a scenario of a mobile user connecting to different access points via short range communication such as Bluetooth or Wireless LAN. Since these access points will be able to to provide services based on local or remote resources beyond basic IP access, we call them service points (SP). We make further distinction between service points which are located in the proximity of the user, which we call Local Service Points (LSP). To enlarge coverage outside of the range of LSPs, public mobile networks such as GSM, GPRS or in future UMTS will be used to reach so-called Global Service Points. For simplicity reasons we assume for this scenario that all SPs shall be linked together via fixed high speed links. The capability of SPs depends on availability of local memory, storage and backbone connectivity. In this scenario, the mobile user could request a certain service, say a web-based travel information service while being connected to LSP A. The response from the service might reach the user through LSP B. Finally, the mobile user might continue the service using a

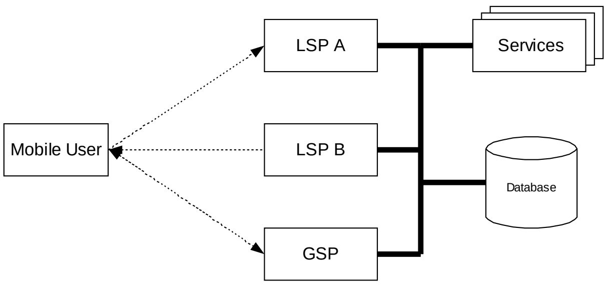

Figure 1. Mobile User Scenario.

GSP.

3.1 Services and Applications

Internet Applications can be classified into transaction based and stream based. Transaction based applications include the Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP) for sending electronic messages and POP3/IMAP4 for retrieving E-Mail. Stream based services are not the main focus of this paper; [3] has a proposal for an access network independent service control system for stream based services. Services can be ad-hoc or session based. Ad-Hoc service means the service is provided immediately by the SP or - in case of a fixed backbone connection - by a server on the network.

Session based services means, the application protocol used by the services need to keep a state in contrast to stateless protocols where every request is followed by an immediate response.

HTTP: Specified in [4], the HTTP protocol is used for accessing WWW content. It is a stateless command-response protocol, i.e. each command (GET, POST, PUT, DELETE) plus applicable headers are followed by a usually immediate response such as content headers, a HTML file, a binary file or an error message. Therefore, it can easily be handled by proxies. This includes distributed proxies where request and response are directed to different entities as described later in this paper.

FTP: Although HTTP supports binary file transfer as well, FTP is still popular for transferring files. See [5] for full specification of the FTP protocol. The protocol has several states (login, changing and listing of directories, setting file transfer options and transferring files) and separates command and data transfer by different connections. However, most actions (e.g. requesting or uploading a single file) do not require an alternating dialogue and therefore can be handled by proxies.

SMTP: Used for sending electronic mail was first specified in 1982 by [6]. Although several commands of the SMTP are intended for an interactive dialogue with the user, E-mails are typically send from programs which use only a subset of the capabilities of SMTP. The protocol can be handled by proxies, but strictly spoken, SMTP proxies should be called SMTP relays.

POP3: The counterpart for retrieving E-Mail form a remote service is POP3, specified in [7]. It is widely used, especially for E-Mail accounts hosted at Internet Service Provides (ISPs). After downloading new mail, it usually gets stored within the user's mail application and deleted from the server. The protocol defines states (Authorization, Transaction and Update) and therefore is less suited for use with a proxy.

IMAP4: Specified in [8], IMAP is a protocol to retrieve mail from a server, too. Unlike POP3, subfolders are supported and mail is kept on the server, allowing access to E-mail from several applications and locations with consistent folder content. The protocol defines several commands and states, rendering it difficult to be handled by proxies.

3.2 Access Networks and Data Link Protocols

3.2.1 Physical

Bluetooth: Bluetooth is a new standard for wireless short range communication. A growing number of portable devices such as PDAs and smart phones support this technology which allows piconets of up to eight simultaneous active connections with data rates of up to 723 kbit/s. For networking purpose, the Bluetooth specification [9] defines the ”LAN Profile” and the ”Dial-up Networking Profile”. Both profiles use a link based on RFCOMM which provides an error corrected and optionally encrypted serial data stream. The serialization of the IP traffic is done by using the Point-to-Point Protocol (PPP). Additionally, Bluetooth supports also a ”Serial Port Profile” which allows a transparent serial data stream between two devices.

Modem, ISDN or DSL Access: These PSTN access techniques provide usually a reliable encoded, but not encrypted link. In case of a modem the link quality may vary over time. The link parameters of a DSL link are adjustable over a wide range and although ISDN connections would allow for setup parameters, typically standard serial links using the X.75 or V.120 protocol are established. Usually PPP is used, although ISDN also allows raw-IP over HDLC. Instead of using PPP, DSL is sometimes configured as frame relay.

Cable Modems and Broadband Wireless Access: Most implementations of cable modems and their wireless counterparts use a DOCSIS compatible framing which is similar to Ethernet frames. Hence there is no need for a PPP protocol, although a derivation of it, the Point to Point Protocol over Ethernet (PPPoE) is sometimes used for user authentication and accounting purpose.

PLMN - circuit switched (e.g. GSM, HSCSD): Line switched GSM data connections have optional Radio Link

Network		Link setup [s]	PPP setup [s]
ISDN	HDLC	1,50	-
	PPP	1,50	0,50
Modem	V.90	28,00	1,00
GSM	V.32	14,00	4,75
	V.110	6,50	5,25
HSCSD	V.32	18,20	6,60
	V.110	9,80	4,50
Bluetooth	DUN	0,60	5,50

Table 1. Average duration of link and PPP setup

Protocol (RLP) error correction and rely on the encryption provided by the system. PPP is also used in resource limited devices such as cell phones with WAP browser.

PLMN - packet switched (e.g. GPRS, UMTS): Although IP is transferred over the GPRS network transparently, current implementations often use PPP for the communication between the TE (Terminal Equipment) and MT (Mobile Terminal)

3.2.2 Radio Link and Point to Point Protocol

As seen above, although the physical medium differs, most access methods rely on PPP to handle authentication, error correction and optional compression and encryption [10].

Table 1 shows link and PPP setup times for different access networks. Times have been averaged over several connections to the same access router and do not include the time for registering with the network itself (e.g. network search in GSM or service discovery in Bluetooth). Since the PPP negotiates several parameters until the link is up, the round trip delay of a link mainly determines the duration of the PPP setup. As long the link is established only once in a session, these times up to 30 seconds are not critical. However, in the given scenario of a user connecting to several short range entities, current setup takes too long, as the user may have already moved out of a small cell before the link has been successfully established.

Also after the link is up, both the RLP in wirless networks and the PPP affects upper layer performance. In case of TCP, [1] provides a thorough overview.

The following chapter introduces a new protocol, which does not require, but will support PPP and TCP for selected services.

4. Mobile Service Control Protocol Outline

4.1 Protocol Stack Classification

Figure 2 shows how the Mobile Service Control Protocol (MSCP) fits into the protocol stack compared to other methods of providing mobility like Mobile IP and WTLS. If a TCP/IP stack is available, the MSCP acts as proxy on the client side and forwards data to the server. On resource limited devices such as smart phones running a JAVA MIDP, the MSCP client can accept connections without supporting TCP. As the server side should always support full TCP/IP, this allows Internet applications to run on the client without TCP/IP stack on the device.

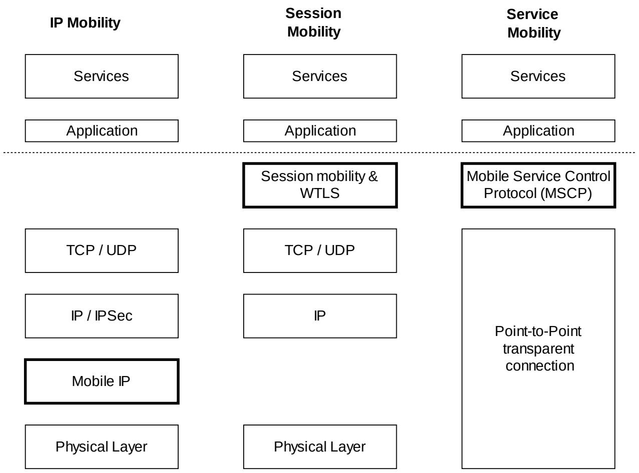

Figure 2. Protocol stack comparison.

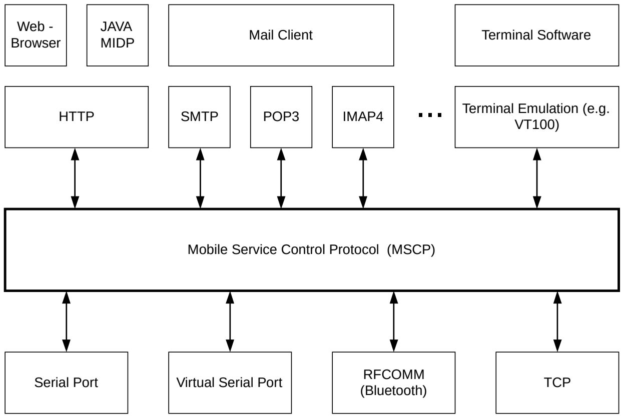

Figure 3. MSCP connections.

4.2 Requirements

As the MSCP is located at the upper layers of the protocol stack, it shall not be dependent on special physical layer or link layer requirements. As a minimum, the following requirements do exist:

- An error corrected, transparent point-to-point link, as provided e.g. by the RLP in public mobile networks or RFCOMM in Bluetooth.

- An application that either handles sockets in an TCP/IP environment

- or -

- An application that can communicate with a serial port or an emulation thereof in case of the device lacks a TCP/IP stack

In the latter case, it depends on the number of available simultaneous emulated serial ports, whether multiple applications or instances thereof will be supported. However, this case usually applies only to resource limited devices, where simulataneous access is either unlikly due to the design (e.g. small screen not allowing multiple windows of a browser window to display) or is avoided by queueing.

4.3 Benefits

Introducing a new communication protocol requires changes on all devices involved in the data transfer. Therefore convincing benefits over existing protocols must exist in order to reach acceptance:

- Compatibility: The MSCP protocol can co-exist with the standard PPP, as an access server e.g. can switch to PPP once it detects Link Control Packets (LCP)

- Adaptive to a wide range of clients: The approach of implementing proxies on the application layer avoids system dependent network drivers and implementation can be fully JAVA based.

- Distributed proxies whcih handle the data traffic, no single aggreation point. The central database is only required to provide handover (session tracking and caching)

- No TCP/IP required (but supported) on the client side

- Seamless handover both intranetwork and internetwork possible, even if the access network itself does not support it

- New application protocols will be supported. This includes a plain-text mode, where e.g. XML-files can be exchanged between client and server without using HTTP.

4.4 Modes of Operation

4.4.1 Tunnel Mode

In the tunnel mode (see figure 4), data is tunneled from the MSCP client to the Service Point (SP) running a MSCP server. The functionality of MSCP depends on the resources available on the client side. Three submodes can be defined:

- Full TCP/IP support: If there is a socket interface between a service interface (e.g. towards a TCP entity) and a user interface (usually towards the application) on both sides, MSCP client and server can carry TCP streams across the wireless link similar to the Remote Socket Architecture described in [11].

- Limited TCP/IP support: This mode supports Internet applications on devices which have no full TCP/IP stack implemented. This is useful on smart phones with JAVA MIDP [12] support, which currently specifies only data exchange using HTTP, but does not provide access to TCP/UDP sockets.

- No TCP/IP support: In this case, the client may just offer a terminal application using a terminal emulation (e.g. VT-220 or ANSI). Internet applications run on the MSCP server and the wireless link carries only keystrokes from the user and display information.

In any case, the application server (e.g. a telnet daemon) sees only the IP address of the SP, so a TCP session will not time out or break in case of delays or a transitory failure of the wireless link, e.g. caused by a handover. If no TCP/IP support is available, the MSCP server acts as a shell which can run Internet applications (e.g. a WWW-Browser or an E-Mail client). This mode supports encrypted links from the SP to the application server (e.g. HTTPS) and relies on the Link-Layer level encryption of the wireless link between the SP and the mobile user.

If the user roams during a connection (e.g. a POP3 or IMAP4 session) between two SPs, the SP from which the session originated becomes the session master. The MSCP will handle the data forward between the service points. This allows interactive sessions (e.g. shell access via telnet) to be continued after a handover.

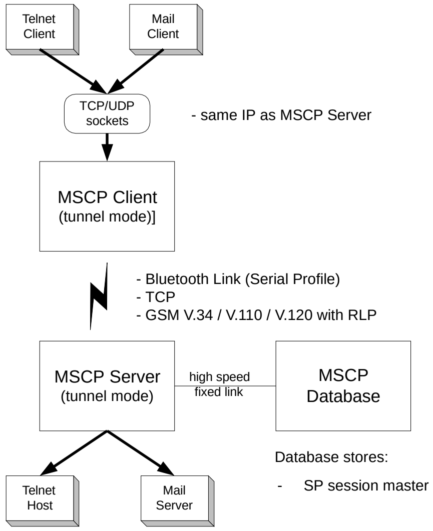

Figure 4. Tunnel Mode.

4.4.2 Proxy Mode

The proxy mode (see figure 5) can be used for any stateless text based application protocol that uses TCP. It works without modifications with HTTP and HTTPS and non-interactive FTP sessions.

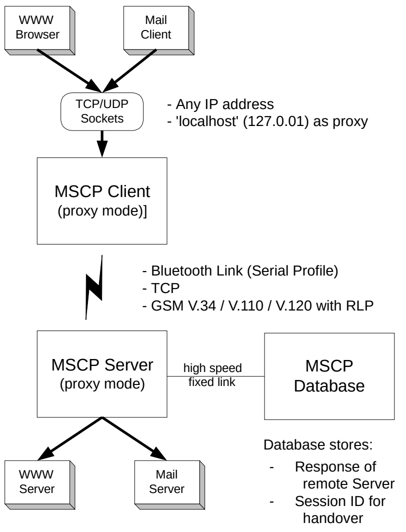
WWW Browser
Mail Client
TCP/UDP Sockets
- Any IP address
- 'localhost' (127.0.01) as proxy
MSCP Client (proxy mode)]
- Bluetooth Link (Serial Profile)
- TCP
- GSM V.34 / V.110 / V.120 with RLP
MSCP Server (proxy mode)
high speed fixed link
MSCP Database
WWW Server
Mail Server
Database stores:
- Response of remote Server
- Session ID for handover

Figure 5. Proxy Mode.

5. Data Flow Examples

The following describes the data flow for the given scenario: The user is with his Bluetooth-equipped PDA close to two Service Points and wants to retrieve a web page or a file from a remote host. While within range of SP A he submits the URL request. Before he receives the server's response, he leaves the coverage area of SP A and moves into the range of SP B. This example shall further assume that the wireless Link is established using the Bluetooth Dial-up profile, i.e. IP traffic is encapsulated in PPP packets. Since HTTP is not a session based protocol, the proxy mode of MSCP can be used as shown in figure 6.
The next example assumes the same scenario as described above, but this time the user wants to access his electronic mail using the IMAP4 protocol. Since this protocol is session based, the tunnel mode of MSCP will be applied. See illustration 7 for the communication sequence.
More examples, including sample implementations that avoid PPP altogether can be found at [13].

6. Conclusion and future work

This paper advocates keeping TCP/UDP sockets on mobile terminals where they have been implemented so far, but replacing PPP with a lightweight protocol which is better adopted to the wireless link. Where possible, distributed

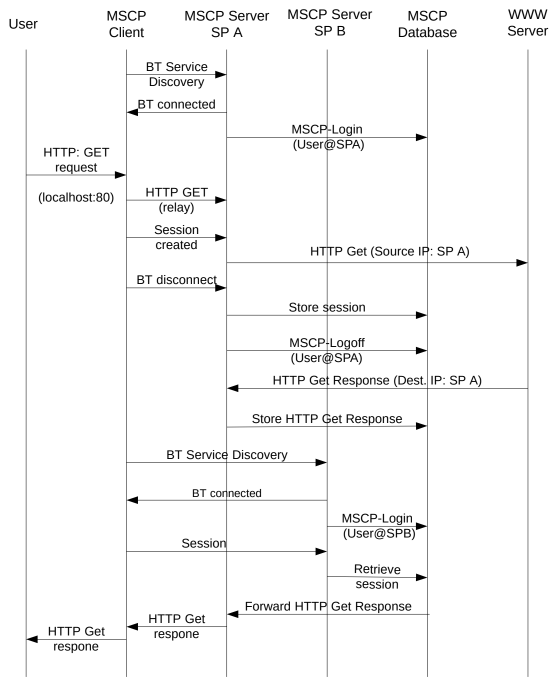

Figure 6. Communication sequence with user roaming (Proxy mode for HTTP).

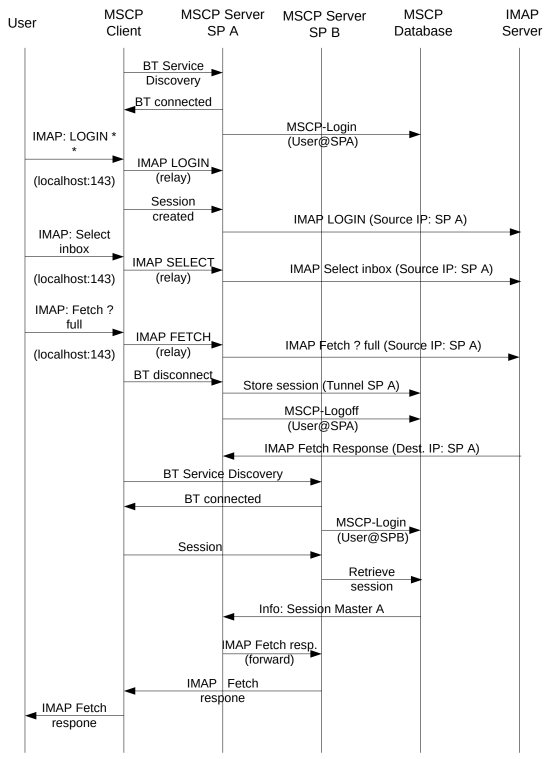

Figure 7. Communication sequence with user roaming (Tunnel mode for IMAP).

proxies for stateless TCP applications are used to provide access network independent roaming and avoiding TCP on the wireless link. Otherwise, TCP connections are tunneled between service points to allow a transparent and continuous transmission of data. This ongoing work is part of the ”Heywow” framework [14], a new platform for mobile distributed services in a heterogeneous network environment. More information about the current work and sample implementations of the MSCP can be found at [13]. Future work includes compatibility evaluation with Peer-to-Peer networks, especially the just recently released JXTA [15] project.

References

[1] G. Xylomenos, G. Polyzos, P. Mähönen, M. Saaranen, “Tcp performance issues over wireless links,” *IEEE Communications Magazine, Vol. 39 No. 4*, 2001.

[2] C. Perkins, “Ip mobility support,” *RFC 2002*, October 1996.

[3] J. H. R. Lehtonen, “Access network independent service control system for stream based services,” in *Proc. EUNICE 2000*, (Enschede, Netherlands), September 13-15 2000.

[4] R. Fielding, “Hypertext transfer protocol – http/1.1,” *RFC 2616*, June 1999.

[5] J. Postel, “Simple mail transfer protocol,” *RFC 959*, October 1985.

[6] J. Postel, “Simple mail transfer protocol,” *RFC 821*, August 1982.

[7] J. Myers, “Post office protocol - version 3,” *RFC 1939*, May 1996.

[8] M. Crispin, “Internet message access protocol - version 4,” *RFC 1730*, December 1994.

[9] Bluetooth Specification (Bluetooth SIG). http://www.bluetooth.com.

[10] J. Carlson, *PPP Design and Debugging*. Addison Wesley, 1998.

[11] M. Schager, B. Rathke, S. Bodenstein, and A. Wolisz, “Advocating a remote socket architecture for internet access using wireless lans,” *MONET, Special Issue on Wireless Internet and Intranet Access*, 2000.

[12] JAVA MIDP Specification (Sun Microsystems Inc.). http://java.sun.com/products/midp.

[13] MSCP Specification and Sample Implementation. http://www.heywow.com/mscp.

[14] Michael Angermann, Patrick Robertson, Alexander Steingass, “Integration of navigation and communication services for personal travel assistance using an java and jini based architecture,” in *Proc. GNSS1999*, (Genua, Italy), 1999.

[15] Li Gong, “Project jxta: A technology overview,” *http://www.jxta.org*.