The GSM cellular telephony system, and the Personal Mobile Telecommunications option of the Japanese cellular telephony system (PDC) support personal mobility within their respective networks by separating the subscriber's identity from the device he uses. However, it is unlikely that people will use only one type of network in the future. Therefore, these systems cannot provide the full personal mobility support that MPA aims to provide.

Mobile IP [Per96] enables a mobile host to be addressed by a well-known, static IP address and to receive communication regardless of its current point of attachment to the Internet. However, it provides only host mobility and only within the Internet.

Iceberg [JBK98] aims at integrating cellular telephony networks with the Internet. It shares with MPA the view that people will continue to use multiple devices for communication. However, Iceberg approaches the problem primarily at the network layer, rather than the people layer. Moreover, it does not provide location privacy. We believe location privacy is a key goal when supporting personal mobility.

A related project is NINJA [GWBC99], which focuses on providing an infrastructure for the construction of flexible and adaptable services in a clustered environment. This infrastructure could provide a solid foundation for new, pluggable Application Drivers in our Personal Proxy.

The Presence Information Protocol [ADM98] (PIP) and the IDentity Infrastructure Protocol [FM98] (IDIP) provide some support for personal online identities and tracking of people. Both allow people to advertise dynamic information about their online presence and to exchange instant messages with each other. IDIP goes a step further, by permitting more specific negotiation of multimedia communication formats. Neither of the two approaches addresses location privacy.

VII. Conclusions

People-centric communication is the next big step for mobile computing. Whereas existing mechanisms have addressed mobility in the network, none has fully addressed the issue of providing mobility support to *people*, who are the ultimate and most important endpoints of communication.

We propose an architecture called the Mobile People Architecture (MPA), which provides support for instant and convenient communication between people, as they move from place to place and make use of multiple heterogeneous communication devices, including laptops, PDAs, or cellular phones. MPA makes it possible for people to protect their location privacy and for application designers to facilitate the deployment of their applications within this framework. We identify the key components within this architecture and their corresponding functionalities. Finally, we illustrate a potential prototype design of the system.

People cannot be the outsiders in the communication landscape any longer. We firmly believe that with the help of the mobile computing research community, this challenge will be met.

VIII. Persistent Mobile Data

A. Design Issues

While MPA mainly focuses on delivering messages, it is important to consider what happens to a message once it arrives at the recipient's device. Most people do not simply throw messages away after reading or hearing them; some people diligently categorize and archive all their messages, while others just let them pile up in an "inbox." Email and voicemail systems currently fulfill this need by allowing users to manage archives of their messages. However, they don't allow users to keep one consistent message archive that may be distributed among multiple devices. Instead, they force users to act as the consistency mechanism between multiple message archives.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

We propose a personal distributed file system (DFS) that allows people to locate, access and manage their personal data—including message archives—regardless of where they are or what devices they use.

Multi-user constraints of earlier DFS systems (see Section VI) are relaxed in the personal DFS case. This is because one person is unlikely to be modifying two copies of a file at the exact same time, or at least by nature, avoids doing so.

In a personal DFS, users will have data and files spread over several devices, and should be able to control which subsets are propagated where. Some devices are more resource-poor than others. For example, a palmtop device is unlikely to have the same amount of computational power and storage as a laptop. Therefore, users will want to store or view only a subset of all their personal data on each device.

A persistent mobile data mechanism could be used to synchronize a user's message store, as well as his or her files.

While the personal DFS does not have the multi-user constraints of previous systems, it does present other challenges, because:

- not all hosts are up and running and connected.
- not all devices run on the same platform or share the same principal file system.
- there may be no general mechanism to guide the data traversal from device to device. Sometimes we will need application-specific mechanisms to do this.

A.0.a Rumor. Rumor[GRR+98], from UCLA's File Mobility Group, is a software package that allows users to keep multiple copies of their files synchronized on different machines automatically. For example, Rumor would allows a user to keep one copy of her files on her desktop machine at work, a second copy on a portable machine, and a third copy on a machine at home. Rumor could also be used at different sites to share files, with each site storing its own local copy. It detects changes made to any files under its control and propagates the changes made at any replica to all other replicas. Rumor permits users to update any of their replicas freely, while guaranteeing that the updates will be properly propagated to all replicas.

A.0.b Distributed File Systems. Existing distributed file system protocols (e.g. NFS, AFS, SMB, Coda) have unnecessarily strict consistency requirements, and treat disconnected operation as a special case. They also force a distinction between clients and servers.

Coda at least allows replication of data among several servers. Coda has the best support for disconnected operation: clients record a log of all file system calls while disconnected, which is then replayed upon reconnection.

Some of the key differences in motivation between traditional distributed file systems and our work can be found in the Coda paper: "Servers are like public utilities...they are carefully monitored and administered by professional staff." "Disconnected operation...represents a temporary deviation from normal operation." We expect that neither of these assertions will hold true in the future.

IX. Acknowledgements

We would like to thank Ichiro Okajima, of NTT DoCoMo, for providing us with valuable questions and suggestions during our MPA discussions, Trevor Holt of Nortel Networks for bringing to our attention related work on PIP and IDIP, and Armando Fox for his encouragement.

This research has been supported by a gift from NTT Mobile Communications Network, Inc. (NTT DoCoMo), a grant from the Keio Research Institute at SFC, Keio University and the Information-technology Promotion Agency in Japan, and a grant from the Okawa Foundation.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

REFERENCES

[ADM98] S. Aggarwal, M. Day, and G. Mohr. Presence Information Protocol Requirements, August 1998. http://search.ietf.org/internet-drafts/draft-aggarwal-pip-reqts-00.txt.

[Ame] America Online, Inc. AOL Instant Messenger. http://www.aol.com/aim/.

[ATT] AT&T Easy Reach^{SM} 500 Service. http://www.att.com/easyreach500/.

[FM98] S. Fujimoto and D. Marvit. The IDentity Infrastructure Protocol, August 1998. http://search.ietf.org/internet-drafts/draft-fujimoto-idip-00.txt.

[GRR+98] Richard Guy, Peter Reicher, David Ratner, Michial Gunter, Wilkie Ma, and Gerald Popek. Rumor: Mobile Data Access Through Optimistic Peer-to-peer Replication. In *Proceedings: ER'98 Workshop on Mobile Data Access*, 1998.

[GWBC99] S. D. Gribble, M. Welsh, E. A. Brewer, and D. Culler. The MultiSpace: an Evolutionary Platform for Infrastructure Services. In *Proceedings of the Usenix Annual Technical Conference*, June 1999.

[ICQ] ICQ, Inc. How to Use ICQ. http://www.icq.com/icqtour/quicktour.html.

[JBK98] A. D. Joseph, B. R. Badrinath, and R. H. Katz. The Case for Services over Cascaded Networks. In *Proceedings of WOMMOM '98*, October 1998.

[Per96] Charles Perkins. IP Mobility Support - RFC2000, 1996.

[WKH97] M. Wahl, S. Kille, and T. Howes. Lightweight Directory Access Protocol (v3) - RFC 2251, 1997.

$Id: TechReport.tex,v 1.9 1999/03/14 00:35:57 laik Exp $

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

draft-rosenberg-sip-pip-00.txt
Internet Engineering Task Force pipr
WG
Internet Draft
J.Rosenberg,H.Schulzrinne
draft-rosenberg-sip-pip-00.txt Bell Laboratories,Columbia
U.
November 13, 1998
Expires: May 1999

SIP For Presence

STATUS OF THIS MEMO

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress''.

To learn the current status of any Internet-Draft, please check the ``lid-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this document is unlimited.

ABSTRACT

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

We describe an extension to SIP for subscription, notification, fetching, and indication of presence events. The extensions consist of two new methods, SUBSCRIBE and NOTIFY.

1 Introduction

An event notification service allows a user (called the subscriber) to subscribe to some entity. Associated with the entity is some state. The subscription is a request to be informed about changes to the state. When state changes occur, a notification is delivered asynchronously to the subscriber. The applicability of the service is extremely broad; events could include things like network management events, presence information, device status, system failures, etc. Subscriptions can be as simple as "notify me when person X logs in"

or as complicated as "notify me when event X in state machine Y occurs if the day is Tuesday and the temperature in Zimbabwe is 85 degrees fahrenheit".

Furthermore, different events and subscriptions will vary in their requirements for reliability, scalability (in terms of number of subscribers for some event), timeliness (in terms of the latency between an event and delivery of the notification to the subscribers), and control (in terms of the complexity of the description of events which may be subscribed to). For example, subscribing to a service which notifies you when concert tickets become available requires a supporting protocol to be scalable, and may mandate multicast. However, reliability is not a concern. On the

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.