SUPPORTING PERSONAL MOBILITY FOR NOMADIC COMPUTING OVER THE INTERNET

ABSTRACT — This paper presents a new paradigm for nomadic computing over the Internet called universal personal computing (UPC), where mobile users can access computing resources, network services, and personalized computing environments anywhere using any available terminals. The concept of UPC and system design issues are discussed, and the required system architecture capable of managing different mobile objects, i.e., users and terminals, in the UPC environment is presented. Modifications of connection setup procedures between user application programs to enable addressing based on a global user identity are considered.

I. INTRODUCTION

In recent years, portable computers, ranging from laptop computers, to notebook computers, to PDAs, and so on, are becoming increasingly compact and powerful. At the same time, connections of computers to the global networks have grown exponentially, while rapid advancement of wireless communications technologies is making it possible for mobile users with portable terminals to access information anywhere and at any time. The combination of mobile computers and wireless communications is promoting the evolution of information technologies to enable a computing environment that is often called nomadic computing in the literature [1, 2]. Nomadicty refers to the system support needed to provide a rich set of computing and communications capabilities and services to mobile users with portable terminals to access information anywhere and at any time. The desirable characteristics for nomadicty include independence of location, motion, computing platform, communication device, and communication bandwidth, and the widespread availability of access to remote files, systems and services.

The Internet is today’s most successful global network for data communications, providing the means to interconnect a large number of heterogeneous computer networks. A large group of applications such as e-mail, Telnet, FTP, Gopher, World-Wide Web (WWW), etc., have been developed to take advantage of Internet communications, and their increasing popularity has led to exponential growth in the number of hosts and users connected to the Internet. The future version of the Internet protocol (IP) will support a substantial increase in the number of available host addresses, as well as quality of service management for real-time traffic, flexible congestion control schemes, and security features [3]. Due to its growing popularity and continuous evolution, the Internet is expected to support nomadic computing in the future by incorporating suitable upgrades in the Internet protocol suite.

Mobility support is the fundamental requirement in this Internet protocol enhancement. Research activities to enable nomadic computing are currently centered around the support of terminal mobility. The protocol for IP mobility support, or mobile-IP has recently been standardized by IETF as an RFC [4]. Mobile-IP enables a mobile terminal (MT) to retain the home IP address as its network level identification, and to employ a second IP address (commonly referred as the care-of address) associated with the current location of the MT for routing datagrams addressed to the MT via the MT’s home network by means of tunneling. The association between mobile user and mobile terminal is not addresses in the mobile-IP scheme, and this association may be assumed fixed between the terminal and its owner. However, expansion of nomadic computing in the future will require an additional degree of mobility to be supported over terminal mobility, namely personal mobility, which enables a mobile user to access a user-defined set of subscribed services from any currently available networked terminal, be it fixed or mobile, irrespective of geographical location, limited only by the terminal’s and network’s capabilities and any restrictions imposed by the network service provider.

The concept of personal mobility itself is not new. A global standard for such services, Universal Personal Telecommunication (UPT), is being studied by CCITT[5]. UPT’s network architecture, functional model, and call setup procedure have been discussed extensively in the literature [5–9]. But the implementations of UPT services are based on the Intelligent Network (IN) and focused on extending point-to-point connection-oriented service provided by the public switched telephone network to mobile users. Recently, the Telecommunications Information Networking Architecture (TINA) Consortium [10] is defining and validating an open architecture for telecommunications systems in the broadband, multi-media information era. The architecture is based on distributed computing, object orientation, and other concepts and standards from the telecommunications and computing industries. The final TINA’s architecture will provide personal mobil-
ity functions [11]. Although the principles of TINA’s flexible software architecture can be mapped to Internet application design, TINA is mainly developed to interwork with INs and B-ISDNs. However, parallel developments in extending location independent network computing services over the Internet to mobile users have been lacking.

In this paper, we introduce a new paradigm for location independent network computing over the Internet, called universal personal computing (UPC). It refers to a computing environment which enables mobile users to access computing resources, network services, and personal applications, data files, and environmental configurations, through any available terminal (stationary or mobile) anywhere on the Internet. Support of this extra degree of freedom in personal mobility in nomadic computing over the Internet requires the development of new or enhanced architectures and protocols beyond what is currently being considered for terminal mobility support. These developments should be evolutionary in nature so that they are backward compatible with the substantial infrastructure invested in the current Internet, and with the emerging IP mobility support protocol [4].

In the rest of the paper, Section II introduces the concept of UPC, identifies the differences between terminal mobility and personal mobility, and discusses some system requirements and design issues related to UPC. To manage globally roaming mobile users and terminals, logical identifications of users and terminals are discussed in Section III. A network architecture with the necessary mobile object control entities is also introduced, and the functions of these components are described. Section IV gives the procedures for registrations, location management, and authentication for mobile users and terminals. To enable the establishment of TCP connections between users employing global logical identifiers, Section V examines three possible methods to upgrade the current TCP connection setup protocol. Section VI concludes the paper.

II. THE CONCEPT OF UNIVERSAL PERSONAL COMPUTING

A. Terminal Mobility and Personal Mobility over Internet

The Internet technology provides a fundamental suite of communication protocols to foster communications of packets between host computers with diverse hardware architectures and operating systems, over interconnected heterogeneous computer networks. It is assumed that hosts remain static through their lifetime. A host’s name is identical with its network address. Any host movement to another subnet involves manual network reconfiguration procedures for name and address changes before the host is connected to the new subnet.

Extension of Internet connectivity automatically to hosts visiting foreign subnets requires host or terminal mobility support. Several versions of host mobility protocol have been proposed [12, 13], and efforts in IETF have led to the recent mobile-IP standard [4]. Mobile-IP retains the home IP address of a mobile host or MT for use in identifying it at the network level, but also associates a second IP address (commonly referred as the care-of address) with the MT to indicate its current location. Incoming datagrams are first routed to the MT’s home network, where a home agent redirects the datagrams to a foreign agent at the visited network by tunneling to the care-of address, and the foreign agent in turn delivers the datagrams to the MT.

With host mobility support as in mobile-IP, a mobile user can only access network services through a MT that is from the same home network as the user, since the MT is still logically attached to the home network while roaming. Only users authenticated by a MT’s home domain can login through the MT. In most cases, each user has her own MT, in which her installs enough applications and personal files as needed while traveling away from her home network. Therefore, the associations between users and MTs are basically fixed. However, as the concept of nomadic computing expands to encompass ubiquitous location independent computing, and networked terminals become increasingly available in public places such as airports, hotels, shopping malls, rental cars, etc., there are many situations in which the support of terminal mobility only is insufficient, and the capability of mobile users to access locally available networked terminals is desired or required:

• In real life, not all computer users own portable computers, while owners of portable computers may not find it convenient to carry them all the time. When traveling away from home or office, these users become disconnected unless locally available networked terminals provides them with a “virtual presence” at their home networks.

• In addition to the traditional Internet services, many new information services targeted towards mobile users are emerging. Locally available networked terminals provides a ready means for travellers to access local information such as the route to a destination, local weather forecast, reservations for parking space, restaurant, cinema, theatre, etc.

• Furthermore, locally available networked terminals provide a direct means for users to access local network resources such as printers, fax modems, etc. In combination with capabilities for mobile users to access data, applications, and customized environmental settings at their home network, these terminals can provide a complete “virtual office” solution to
The above discussions suggest that another degree of mobility, i.e., personal mobility (PM), should be introduced in nomadic computing. We name this new paradigm of network computing over the Internet that provides PM support as Universal Personal Computing (UPC). In this context, PM support entails system capabilities to enable a mobile user to access a user-defined set of subscribed services, to access local and remote computing resources, and to initiate and receive any type of communications on the basis of a logical user identifier at any terminal, fixed or mobile, irrespective of the user’s geographical location, and limited only by capabilities and restrictions imposed by the network provider and the accessed terminal.

B. UPC System Design Issues

In order to design a system architecture and protocol enhancements over TCP/IP and mobile-IP that enables the main features of UPC, it is necessary to establish some boundary conditions and identify the major system requirements and design issues.

We consider only regular users of the Internet. Thus each mobile user is assumed to belong to a certain home network, an administrative domain where the user is registered on a long-term basis. Assuming adequate data security is provided by the network, the home network is responsible for authenticating the identity of a roaming mobile user, and may also vouch for the mobile user and accepting charges when the user wishes to purchase service from a visited network.

Each mobile user has a service profile at her home network which specifies services the user may access through the home network while the user is at home or roaming, as well as default parameters for these services and for the mobile user’s computing environment in general. Special services to support roaming, e.g., email filtering or digesting, may also be specified.

Since users may access network services from any terminals, user and terminal control functions have to be logically separated. The combination of these control functions constitutes personal mobility control. However, in the case of a user accessing a fixed terminal, terminal mobility control functions are not invoked.

Each user and terminal should be globally identified by a logical user identifier (LUI) and a logical terminal identifier (LTI), respectively, which should be independent of their current locations, and a user’s LUI should also be independent of the LTI of the user’s current terminal. Network services and communications received by a mobile user should be transparent with respect to the logical associations or bindings between user, terminal, and location, managed relative to the mobility of the user and the terminal.

Location information management of mobile objects is a key issue in UPC. The algorithms for searching and updating locations of mobile users and terminals should not adversely burden the Internet in terms of traffic overhead and protocol processing. Backward compatibility with the existing Internet naming and addressing methods and protocols should be maintained.

Services provided to mobile users should be transparent to user and terminal movements. When wireless access is employed, handoffs between radio cell should not disrupt service access or communications in such a way that is noticeable by the user.

Facilities are required to manage a mobile user’s local network resources and personal resources at her home network, and to transparently provide a personalized computing environment to the user, so that the mobile user can access services in an environment that she is accustomed, as if she was home.

Adaptation capabilities should be provided to harmonize the differences in operating environments, input, output, display, and storage formats, etc.

Certain intelligent agents may be incorporated to optimize the UPC operations through optimal functional divisions between terminals and networks.

III. SYSTEM ORGANIZATION

A. Address Binding in UPC System

To enable personal mobility, a Logical User Identifier or LUI is needed to uniquely and directly identify a user irrespective of the terminal used. The LUI is used as the basis for sending and receiving messages and for charging a user for services. A mobile user could access network computing and communication services using a fixed or mobile terminal attached to a UPC service supporting network by specifying her LUI and providing additional authentication information. Each terminal is identified globally by a Logical Terminal Identifier (LTI) regardless of whether it is fixed or mobile. Fig. 1 illustrates the dynamic associations among mobile objects, fixed objects, and networks. A MT employing wireless access could handoff to a neighboring base.
LUI: logical user identifier
LTI: logical terminal identifier
BS: base station
FT: fixed terminal
R: router
TM: terminal mobility
PM: personal mobility

Figure 1. Dynamic associations of mobile objects station within the same network, or handoff to a base station that belongs to another network.

Although a LUI could be in many forms such as a personal number or even the photo of a user, a user’s LUI should be a unique name on the global network, independent of the current location, consistent with the current naming method in Internet applications, and provide a ready association with the user’s home network. Table 1 lists a few examples of naming a person or a server in Internet applications. To facilitate implementation of and experimentation with UPC in the near term, we propose that the LUI be simply composed of the user ID of a user at her home network concatenated with the user’s home domain address, such as user@dept.univ.edu. This obviates the need for global user-name servers and is compatible with the current Internet architecture.

Table 1. Examples of addresses used in different Internet applications

<table>
<thead>
<tr>
<th>Applications</th>
<th>Server or personal addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teleconference</td>
<td><a href="mailto:user@dept.univ.edu">user@dept.univ.edu</a></td>
</tr>
<tr>
<td>e-mail</td>
<td><a href="mailto:user@dept.univ.edu">user@dept.univ.edu</a></td>
</tr>
<tr>
<td>www</td>
<td><a href="http://www.dept.univ.edu/~user">http://www.dept.univ.edu/~user</a></td>
</tr>
<tr>
<td>ftp</td>
<td>dept.univ.edu</td>
</tr>
</tbody>
</table>

Since IP was designed before TM was entertained, an IP address both identifies a host and specifies its location for the purpose of packet routing. In mobile-IP [4], a host’s home IP address is used as its LTI, and its physical location while roaming is given by a forwarding (care-of) address. Tunneling is employed to redirect packets addressed to a LTI to the terminal’s current location. Thus TM is transparent to the transport layer and the protocol extension is backward compatible with the existing Internet protocol suite. UPC should further extend these methods of terminal and location identification to maintain backward compatibility.

Figure 2. Address binding for personal mobility

From the above, a mobile user’s address binding can be composed of the user’s LUI, and the terminal’s LTI. This address binding is kept at the mobile user’s home network. For a fixed terminal, the LTI and its IP address are consistent. For a mobile terminal, datagrams addressed to the LTI can still be routed to the MT’s location by means of mobile-IP protocol. In order to provide route optimization in UPC, the MT’s address binding which enables TM support should be transferred to overall address binding supporting PM as shown in Fig. 2 during user registration and location updating procedures. The actual algorithm will be discussed in a subsequent section.

B. Network Infrastructure

The major difference between UPC and mobile-IP is the addition of mobility management for mobile users which is handled separately from that for MTs. Therefore a User’s Home Agent (UHA), a Terminal’s Home Agent (THA) and a Foreign Agent (FA) are configured in each self-administrative domain of the conceptual multi-network Internet architecture to support personal and terminal mobility in UPC as shown in Fig. 3. This enables the separation of mobile object control functions including user and terminal profile management, registration, authentication, location searching and updating, datagram routing, and handoff processing. The following defines each component in the proposed network architecture and describes their basic operations.

1. User’s Home Agent (UHA)

Each mobile user has a home network. The UHA in each network maintains a list of users associated with this network as their home domain. The UHA includes a user-database that records the LUIs of all users calling the network home, and the pertinent information for
Table 2. Types of mobile user information

<table>
<thead>
<tr>
<th>Service Profile Information</th>
<th>Location Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authentication information</td>
<td>• Location binding</td>
</tr>
<tr>
<td>• Service access information</td>
<td>• Type of terminal</td>
</tr>
<tr>
<td>• Special treatments while roaming</td>
<td>• Type of services</td>
</tr>
<tr>
<td>• Access domain information</td>
<td></td>
</tr>
<tr>
<td>• Usage accounting and billing information</td>
<td></td>
</tr>
</tbody>
</table>

Each user, including the service profile and location information. Table 2 lists the possible items in a user’s home database entry. In particular, the service profile contains the user’s authentication information, defines the entitlement of the user to access services and resources, and includes the user’s service preferences and environmental defaults. This database information is accessed whenever the user roams into a new network, registers on a new terminal, and accesses services and resources. Database management operations on a user’s service profile can be performed only by authorized network administrators or by the user herself. The location information provides the mobility binding between the LUI, the LTI of the terminal the user currently uses, and possibly the location of the terminal (e.g., in the form of a care-of IP address) in case the terminal is mobile. This information is updated whenever the user moves or changes her association with a terminal. The terminal’s configuration should also be copied to the user’s database in order to evaluate the possible services the home network may provide the user, as service availability may be limited by the terminal’s capability.

2. **Terminal’s Home Agent (THA)**

Each network has a THA which maintains a home list or database identifying all MTs that call the network home. A MT is a normal terminal with additional software that allows it to move through the Internet in a manner transparent to software above the network layer within the host. Terminal-related information such as terminal identity (LTI), terminal profile, terminal authentication key, and current terminal location (care-of address) are stored in the THA database. The terminal profile identifies the terminal’s capabilities such as resident operating system, GUI, file format, display mode and resolution, etc., so that the serving network can coordinate with the terminal’s software to create the computing environment required by the user, or a close approximation of such an environment.

3. **Foreign Agent (FA)**

As mobile users and terminals migrate over the Internet, they need to access network computing resources and services from different networks connected to the Internet. To enable service access, the mobile user and the terminal must first establish temporary residence in the visited foreign domain. Each network serving mobile users and mobile terminals has a foreign agent (FA) which enables visiting users and terminals to be temporarily associated with the network. Each foreign agent maintains two lists, one for visiting users, and the other one for the visiting terminals. The entry for each mobile user mirrors the user’s mobility binding stored in the user’s UHA. For a visiting MT’s user, the FA may serve as a default router terminating tunnels [13] extended from UHAs or THAs to enable packet redirection to the MT. To provide more efficient service to a mobile user, the FA may cache pertinent parts of the terminal profile and the user’s service profile.

**C. Relationship between PM and TM**

To understand the relationship between PM and TM services, Fig. 4 presents the different service areas of a fixed network, and the TM and PM protocols. It can be seen that mobile-IP, which enables TM control, is a special case of PM control in a UPC system, where both the mobile user and her MT have the same home network and are permanently bound. In general, UPC covers all possible combinations of user-terminal associations. Therefore, new extensions and enhancements of the Internet protocol suite, that are compatible with the existing protocols and mobile-IP, need to be developed to address the different combinations.

**IV. MOBILITY CONTROL SCHEMES**

**A. Registrations**

Registration is usually divided into terminal registration and user registration procedures for personal mobility control [14]. In a UPC system, the combination of these two kinds of registrations is used for different combinations of user-terminal associations and at different communication stages as illustrated in Fig. 5. If a user is accessing a fixed terminal at her home or a foreign network, only user registration is needed. If a
From the users’ viewpoint, mobile users’ and terminals’ name-to-address bindings should be stored in a global database and updated in real-time. However, experience in Personal Communications Services (PCS) [15] reveals that the HLR (Home Location Register) experiences a high update rate. Also, as indicated in [12], Internet’s domain name system (DNS) was designed to optimize the access cost, not the update cost. So a distributed directory service based solution for address updating in mobile location management is too expensive, and so is the corresponding need to change existing host software around the global Internet to access this directory service.

In the proposed UPC system, we consider placing MT and user address information at their respective home networks. The essential location information for any user in the UHA is her associated terminal’s LTI. For a fixed terminal, its LTI is also its routing IP address. For a MT, mobile-IP may be employed to route packets to its current location. However, in order to realize route optimization, the MT’s care-of address should be registered simultaneously at the user’s UHA and the MT’s THA during the initial registrations, and updated at the UHA and the THA during inter-network handoffs.

In the current mobile-IP, every time a MT crosses the border of a cell served by different FAs will initiate a location updating at its home agent [13]. Considering that intra-network handoffs will happen more frequently than inter-network handoffs, and personal mobility will require care-of address updating at both UHA and THA, location updating of intra-network handoffs should be handled within the visited network to reduce the signaling across the networks (see Fig. 7). This consideration suggests the use of a single FA per network, in which case only handoffs between different networks would require updating of care-of addresses at the UHAs and THAs.
Assuming that a mobile user only knows her LUI, the UPC protocol should discover IP address of her UHA by sending a broadcast message to her home network, using the service of the DNS. Alternately, the UHA could be set up to intercept all packets addressed to the user’s home domain, while the user is roaming, i.e., there is a current entry in the UHA for this user, following the same approach for home agent operation in mobile-IP.

C. Authentication

User authentication and terminal authentication are two independent functions during registration procedures between a user and her UHA, and between a terminal and its THA, respectively.

Terminal authentication is used to guard against possible attacks on packet routing to MTs, including the interception or redirection of arbitrary packets within the network [13]. User authentication is required to protect user’s privacy, personal resources and illegal use of computing resources by unauthorized users. An authenticated user not only has access to her personal resources and network resources at her home network, but also has the right to use the visited network’s resources once her identity and ability to pay is vouched by her home network. So the local network security is maintained, and the charges for the use of local network resources by a visiting user is reported and billed to the user’s home network. Administration of a shared secret between a mobile user and her UHA does not require any network key management infrastructure, since the user and her UHA belong to the same administrative domain. The shared secret could be set manually when the user is at home.

While it does not appear that a basic implementation of UPC through UHAs, THAs and FAs introduces any more security risk than what exists in the current Internet, the cost to the users could be much higher in a UPC system if security is breached, as a malicious user could then obtain service anywhere over the Internet. It is expected that as Internet evolves, additional security measures will be incorporated to minimize this risk, e.g., by encrypting the messages exchanged between MTs, FAs, UHAs and THAs.

V. TCP CONNECTION MANAGEMENT

To reliably communicate with each other, two application programs on different hosts have to set up a virtual circuit connection at the transport layer using TCP, which requires knowledge of the host addresses at the two endpoints. Since UPC users communicate with each other using LUIs without necessarily knowing the other user’s current location or host address, the existing TCP protocol is unable to directly set up a connection to the other user’s MT. Therefore, the TCP connection establishment method needs to be enhanced to utilize the dynamic binding between the LUI, LTI and care-of address. Fig. 8 presents the protocol stack of the UPC system where address binding between LUI and LTI is performed by the enhanced TCP, and the binding of LTI and care-of address is carried on by mobile-IP.

Before considering this enhancement, a brief review of the TCP connection setup procedure is necessary. TCP uses the connection as its fundamental abstraction. A connection is identified by a pair of endpoints. TCP defines an endpoint to be a pair of integers (host, port), where host is the IP address of a host and port is a TCP port in that host. For convenience in the following discussion, the port numbers in the endpoint identities are ignored because port numbers will be kept unchanged in the enhanced protocol. Thus a connection from machine 192.60.36 to machine 119.20.2.3, for example, may be defined by the endpoints (192.60.36, 119.20.2.3).

To establish a connection, TCP uses a three-way handshake [16]. In the simplest case, the handshake proceeds as shown in Fig. 9. The three-way handshake guarantees that both sides are ready to transfer data, and it allows both sides to agree on the initial sequence numbers. The TCP software at each endpoint uses a finite state machine to trace the state of a connection. It starts from the CLOSED state and return to the same state after the connection is closed.

To establish a connection between two mobile users in the UPC system, three alternative methods are possible.
A. The Transparent Solution

As mentioned before, a source communicates with a UPC user by her LUI such as user@dept.univ.edu. The name server may translate this name into the IP address of the UHA at her home network domain. Whether the other user is at home or not, the only choice at the source is to set up a connection with the other user’s UHA. If the user is not at home, and she is registered on a terminal at a remote network, the UHA can set up a separate TCP connection with the user’s current host since the UHA knows the user’s current LTI. The UHA plays the role of a gateway that conveys network messages between the source and mobile user. Fig. 10 illustrates the sequence of messages in the two separate TCP connections. Two finite state machines are used in the UHA to record the connections at each side. If the user is using a MT, the TCP connection between the UHA and MT is supported by mobile-IP. As the MT’s care-of address is updated at the UHA whenever the user and MT move to a new location, the UHA can always tunnel packets directly to the MT’s care-of address. Thus triangular routing from the UHA to the MT’s THA then to the MT’s care-of address can be avoided.

![Figure 10. The two separate TCP connections between source and mobile user](image)

This method does not require any protocol changes at the calling host, so it is completely transparent to the calling host. But it prevents the calling host from communicating directly with the mobile user. Every packet must pass through the UHA. Thus it has the same triangular routing problem as mobile-IP and caching technology cannot be used to provide an optimized routing since the source and the destination transmit all the packets to the mobile user’s UHA address as shown in Fig. 11.

![Figure 11. Transparent solution’s inefficient routing](image)

B. The TCP Layer Solution

The second method needs a slight modification of the TCP layer at the source. As shown in Fig. 12, the source requests to set up a connection with a mobile user by sending message 1 (m1) to the UHA using IP address D-IP. The UHA transfers the message to the user’s MT by substituting the endpoint IP address with the MT’s IP address, and the massage is tunneled to the MT’s care-of address. Upon receipt of this message, the MT will acknowledge the setup request directly to the source by message 2 (m2). The MT’s care-of address is also included in the m2’s piggyback field to enable the source to tunnel future messages directly to the mobile user. The TCP layer at the source is modified to recognize that this message acknowledges the original request message 1. After the source replies to the MT with message 3 (m3), the TCP connection is successfully set up between the source and the MT.

![Figure 12. The modified handshake sequence](image)

The advantage of this method is that, by means of mobile-IP, the source can communicate directly with the mobile user. Route optimization employing cache agents is applicable. The problem is that personal mobility is no longer transparent to the TCP layer. Should universal personal computing become an important feature of the Internet in the future, this modification at the TCP layer should be considered in future TCP/IP standard activities.

C. The Middleware Layer Solution

Besides personal mobility, future nomadic computing systems should support a variety of other features and capabilities. It has recently been suggested [2] that these functions are best incorporated in the middleware level of the commonly accepted layered protocol architecture. This motivates us to consider a solution to support per-
personal mobility at the middleware layer. By means of an appropriate directory service, the middleware protocol of the source could check the IP address of the mobile user’s MT at the UHA (see Fig. 13) before setting up a connection with the user’s MT. When the UHA returns the MT’s IP address to the source, the MT’s care-of address could be piggybacked on the message, so that the source could tunnel packets directly to the MT.

This method employs middleware layer capabilities to manage mobility so that the TCP layer needs not be modified. Of course, this method is not transparent to the source in the sense that the source needs to engage a UPC compatible middleware. Nevertheless, it presents a clean solution with a clear layered architecture in alignment with OSI principles.

In summary, the purpose of all three methods is to enable the source to learn the host address (LTI) currently associated with the destination party. The piggybacked care-of address is just a by-product of the protocol to avoid triangular routing from the source to the MT’s THA and then to the MT’s current location. After the connection is set up, future updating of care-of address due to the MT changing location will be carried out by mobile-IP with route optimization. The UPC system provides PM functionality on top of TM functions provided by mobile-IP. Handoff processing will not disrupt the existing connections because the logical addresses at the connection end-points have not changed, and the connection state information is kept at the end terminals. The transparent solution gives the simplest but least efficient method. The TCP layer solution is efficient, but not backward compatible with the present network. The middleware layer solution seems the best candidate since it offers the flexibility to incorporate a rich set of UPC functions and is backward compatible. However, given the very large number of hosts already deployed within the Internet, it seems quite likely that some will not be upgraded to support PM for some time. To provide a scalable transformation, the transparent solution may be provided to the conventional hosts before they are upgraded.

The middleware layer solution gives a unique chance to provide intelligent services in a UPC system. A mobile user can define a number of selections to deal with different situations when she is not at home. These selections can be presented back to the source user when the source attempts to set up a connection with a roaming user. It is then up to the source user to decide the next action. For example, if the source hopes to hold a teleconference with a mobile user who is not at home but has left some choices in methods to contact her, the source could send an e-mail to the mobile user instead, or go forward to set up a conference connection with the user’s MT for emergency contact, even though such a connection may be expensive.

If the source does not have the right to make selection, a mobile user’s UHA could make choices according the user’s preference indicated in the service profile. For instance, the UHA can transfer e-mails to the mobile user’s current location based on the sender’s name, mail topics, private or business messages, degree of emergency, and the time of the day, but leave the other e-mails at the user’s home mail box.

VI. CONCLUDING REMARKS

We have proposed a new paradigm for future mobile and nomadic computing over the Internet, called universal personal computing, which allows the mobile users total freedom to access network computing services, resources and personalized computing environments from any available fixed or mobile terminals. In order to support an extra degree of personal mobility over terminal mobility, a new system architecture for UPC and enhanced protocol suite are proposed in the paper. Components to manage mobile users and terminals separately are arranged in each administrative domain because users and terminals are independent objects in the UPC system. These lead the separations of mobile object control functions including user and terminal profile management, registration, authentication, location searching and updating, datagram routing and handoff processing. Communications with a mobile user is performed by indicating the user’s logical identifier. The algorithm to route messages and set up connections with the user’s current terminal should be carried out transparently between end users. The TCP/IP suite does not currently support these functions. Therefore we propose a few alternatives to upgrade connection management over Internet. Most of the proposed mechanisms are backward compatible with the Internet and mobile IP protocol suites.

There are many issues related to the upper layer structure to offer service mobility to mobile users. We are defining now an agent-based personal computing architecture to meet the UPC requirements at the upper layer. Because user-related information is initially unavailable at an arbitrary MT in the UPC system, users will depend
heavily on network connectivity to access these information at their home networks. Although a user may access different terminals, she would prefer to operate in a familiar computing environment and delegate the tasks of managing this environment to the system. The model will be based on object oriented and distributed computing technologies to create a roaming personal agent (PA) for each user in order to perform multiple functions for the user [2, 11, 17–19]. The PA follows the user’s movement to provide local access to the user’s service profile and the terminal’s capability profile to enable fast service access and harmonize functional differences between heterogeneous systems. The PA may allow a mobile user to access network services and resources by means of a resource discovery facility (RDF) provided at the visited network. The PA may also help to manage the user’s personal resources at the home network in a transparent way. Movements of mobile users will cause the migration of their PAs to new locations. The PA not only can bring the user’s computing environment to the new network, but also keep the connections with the rest of the world.

Universal personal computing is a powerful concept. The full UPC implementation is ambitious, and will likely require collaborations between researchers internationally. Our analysis of the system architecture and protocols necessary to support the basic features of UPC show that it is a logical extension of the ideas of terminal mobility support in mobile-IP to the more general case of personal mobility support. As the Internet protocols have evolved to encompass terminal mobility support, we submit that the next step in evolving the Internet towards global support of nomadic computing is to take into account of personal mobility support by incorporating some of the ideas presented in this paper in future enhancements of Internet architecture and protocols.

REFERENCES


