A Hybrid P2P/Infrastructure Platform for Personal and Social Internet Services

Dimitris N. Kalofonos and Zoe Antoniou
Nokia Research Center Cambridge
3 Cambridge Center, Cambridge, MA 02142, USA
{dimitris.kalofonos, zoe.antoniou}@nokia.com

***Abstract*—While pure web-based services and P2P technologies are popular for personal and social networking, they both have inherent limitations. A hybrid P2P/Infrastrucutre approach could leverage strengths and address limitations of both paradigms. In this paper we propose such a platform based on MyNet, our P2P personal and social networking system. The new hybrid architecture enhances the properties of pervasive access, security and ease of use found in MyNet through the introduction of infrastructure-hosted MyNet Virtual Devices (MVD). MVDs act as users' personal devices, but also host MyNet-aware Internet Services (MaIS), proxies for 3rd party Internet services. A proof-of-concept prototype and user results are presented to showcase key system features.**

I. INTRODUCTION

The proliferation of digital personal devices, such as mobile phones, cameras, laptops, portable music players, and game consoles, which are able to produce and/or consume digital content and distributed services, has led to a sharp increase in the demand for Internet consumer services. Examples include online music, video rentals, photo printing, and gaming, as well as new forms of services such as personal networking (e.g. online storage-backup, remote connectivity) and, most notably, social networking and online communities. The dominant paradigm currently addressing this demand is that of centralized web-based user interaction: a user registers for a service and gains access to the service provider's infrastructure over the web, where he/she uploads, downloads, and streams all related content and accesses services for personal consumption or sharing.

The web-based paradigm has certain limitations. For example, users have to sign-up to tens of different web-sites to be able to manage their daily digital lives, each with different tools and user interaction models. Also, this paradigm requires users to take several extra steps, adding delays and/or expenses, just to be able to access and share personal content and services already available in their network-enabled personal devices. Migrating personal content while changing service providers can be frustrating. Finally, this paradigm makes it cumbersome or impossible to access and share dynamic personal content and distributed services hosted on the users' own devices.

Recently, a number of technologies in peer-to-peer (P2P) networking have been developed (e.g. [1], [2]), which address universal connectivity issues without requiring centralized infrastructure support. Building on top of such technologies, an alternative decentralized P2P paradigm for personal and social networking services becomes possible, e.g. as proposed in MyNet [3]. MyNet users are able to easily organize their personal resources (devices, services, content, social contacts) to form personal networks, and use these to interact and share securely with other people's personal networks. In contrast to the centralized web-based paradigm, there is no need for a central repository or infrastructure support to expose the resources of each user; instead, content and services are exposed directly by the users' own devices, often in real-time as they are created.

This pure P2P personal and social networking paradigm, however, has its own limitations. For example, P2P networks without any infrastructure support offer no connectivity guaranties. Furthermore, the availability of content and services hosted on personal devices is intermittent, as these devices may be frequently turned off or disconnected from the network. Finally, the lack of integration with Internet services limits the possibilities available to the users.

To leverage the strengths and address the limitations inherent in both the pure P2P and web-based paradigms, in this paper we propose a new hybrid P2P/Infrastructure platform based on MyNet that offers personal and social networking Internet services. Our proposal complements seamlessly the unique features of pervasive access, security and ease-of-use found in the P2P MyNet [3], with an optional infrastructure component and support for Internet services. We introduce MyNet Virtual Devices (MVD), which, depending on the implementation, are hosted servers, virtual machines, or just processes with a P2P MyNet component, which act as any other personal devices. MVDs expose the exact same UI model when accessing and sharing personal services-content and Internet services-content. This is achieved via special MyNet-aware services on MVDs, called MyNet-aware Internet services, that act as proxies on behalf of one or (a composition of) more Internet services offered by 3rd-party providers. Finally, an infrastructure element, called MyNet Broker, is used to establish trust when face-to-face introductions are not possible.

The rest of this paper is organized as follows: Sections II and III provide related work and our motivation; Section IV describes in detail the proposed system; Section V provides our experience with a prototype and real users; finally, Section VI gives our conclusions and future directions.

II. Related Work

Most of the popular Personal and Social Networking systems today rely on web-based centralized interfaces (e.g. Facebook [4], Myspace [5], and Flickr [6]). While these systems allow users to easily describe social links, unlike MyNet, they do not extend to the user's devices or services running on those devices, and they require a centralized infrastructure. Sites such as Amazon have aggregated 3rd party services and offer a seamless experience, but mainly serve a focused type of interaction, e.g. online shopping.

There exist a number of pure peer-to-peer data-sharing systems (e.g. Turtle [7], SPROUT [8], F2F [9], Tribler [10]). The hybrid MyNet architecture extends the capabilities offered by such systems to include connectivity guarantees, easy-to-use security and support for sharing general services.

The proposed service architecture has similarities with hybrid systems [11], [12]. However, these systems use infrastructure-hosted nodes to guarantee connectivity and focus on select Internet services (e.g. VoIP, content sharing). They do not aim to integrate P2P systems with general Internet services. Furthermore, infrastructure-nodes are not perceived and used by the users as personal devices.

Several papers propose proxy-based architectures that implement new services. IBM's WBI project [13] and TranSend [14] use web proxies to adapt web content to varying client bandwidths. iMobile [15] is a proxy-based platform allowing mobile clients to access internet services and to control network devices. It also uses device and user profiles for personalization and transcoding. UC-Berkley's ICEBERG [16] shares the same goals as iMobile, but focuses on voice rather than data services. [17] describes a composable proxy infrastructure that enables dynamic use of proxy filters through detachable Java I/O streams. Furthermore, Amazon [18] and Google [19] recently made it possible for developers to develop and host services on their infrastructure. The above platforms, however, focus mainly on service adaptation for mobiles or on web-based services and do not explore how Internet services can be seamlessly added in the context of P2P personal and social networks.

III. Motivating Use Cases

James has a PDC with three devices: a mobile phone, a PC and a DVR. Using his PC, James signs up for a MyNet Virtual Device (MVD), which provides him with free backup storage and a number of optional services. James clicks on the MyNet music service which automatically launches the installation wizard. The music service is installed with a GUI customisation for the PC device. James can now build his playlist, both from songs he has stored on his DVR and from songs he purchases online through the music service. Next, James switches to his mobile phone and clicks on the MVD music service, which launches the installation wizard with a customised GUI for the phone display. The songs on the playlist he built on his PC are now available to all his PDC devices, including his mobile phone. The music service allows James to give a limited number of streaming Passlets for songs he has already purchased. A streaming Passlet allows the recipient to stream the song free of charge on one instance. Using his phone, James gives a streaming Passlet to his friend Peter for the latest hit "Crazy" he recently bought. Peter does not have an MVD in his PDC but he is still able to use the Passlet to listen to the song.

James wants to add his friend Andrew, who lives overseas, as a MyNet contact. Using MyNet on his PDA, James sends an invitation to Andrew via e-mail before he switches off his device for the day. Andrew sees the invitation in his Inbox and clicks on the invitation link provided in the e-mail. The introduction process completes in the background and seconds later, James appears in his list of contacts. The next morning, James starts MyNet on his laptop and sees Andrew in his list of contacts as well.

IV. System Description

A. P2P MyNet Background

First, we give a brief background on P2P MyNet (see [3] for more details), the basis of the proposed hybrid system.

MyNet is a P2P system enabling non-expert users to easily access and share their resources within their social neighborhood (Figure 1). A wizard-like interface, part of a MyNet UI tool called MyNetBook, first guides the user to imprint his/her identity on a new device. Devices of the same owner are joined to create a Personal Device Cluster (PDC) using the *MyNet Introductions* process. PDCs can be linked to create Social Networks. Users can share access to the resources they own through *Passlets*, real-world metaphors resembling "passes" or "tickets". The security framework permits unlimited access to the PDC owner. Social contacts, however, can only access resources they have been granted rights to. Global connectivity and social network navigation become as simple as selecting another icon on the screen, while complex configuration for service discovery, network access, and security remain hidden from the end-user.

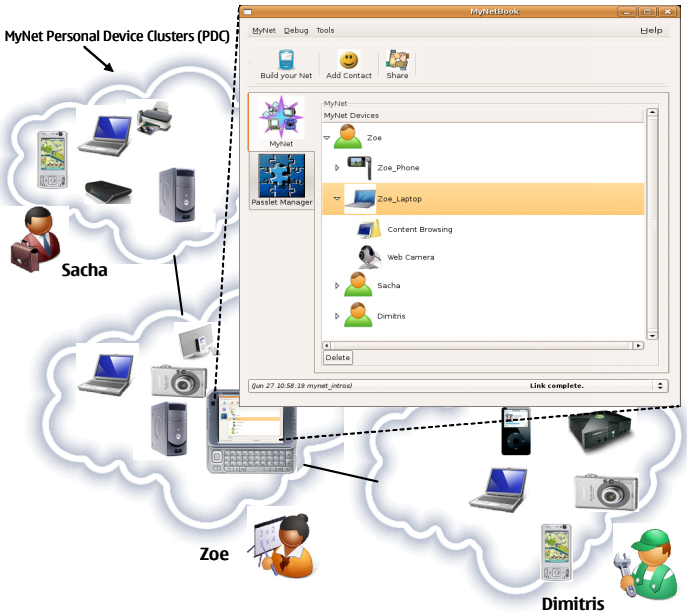

Figure 1: An example P2P MyNet network.

MyNet relies on the UIA P2P overlay [1] for connectivity and distributed group management, although other overlays [2] could be used. UIA bootstraps trust and connectivity by exchanging information among devices locally. Then, its P2P routing layer leverages social relationships to securely route traffic globally over regular IPv4 networks. As a pure P2P system, however, UIA does not guarantee connectivity.

B. *Hybrid MyNet Architecture*

In this paper, we propose a hybrid P2P/Infrastructure system that complements the P2P aspects of MyNet with a centralized infrastructure component provided by a MyNet Service Provider (MSP). The goal is two-fold: (a) add infrastructure support to provide connectivity and service availability guarantees, and (b) offer seamless integration with Internet consumer services without modifying the intuitive MyNet user experience [20]. It is important to note that our approach does not make infrastructure support mandatory: MyNet users who do not wish to use the MSP service can continue interacting in a pure P2P fashion.

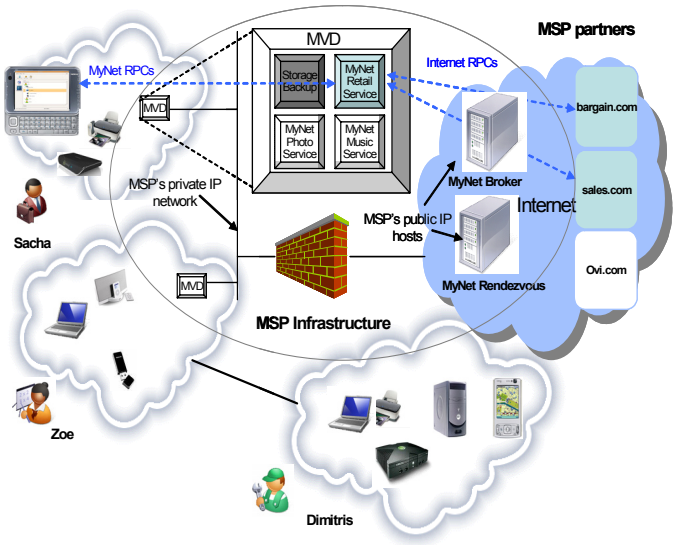

Figure 2: Proposed hybrid P2P/Infrastructure architecture.

A depiction of the proposed system architecture is shown in Figure 2. The MSP maintains an infrastructure which includes one or more private IPv4 networks of servers that host a number of MVDs. MVDs, depending on the implementation, are servers, virtual machines, or just processes with a P2P MyNet component that allows them to route traffic over the P2P overlay. MVDs become part of a user's PDC via the new *Remote MyNet Introduction process*, with the help of one or more (for load balancing) publicly routable IPv4 hosts, called *MyNet Brokers*, whose public DNS name is known to the MyNet middleware.

MyNet Brokers (Figure 2) mediate, authenticate, and authorize remote MyNet operations, in effect replacing the user interaction when introducing MyNet devices remotely. MVDs maintain a mutually trusted relationship with the MyNet Broker, i.e. both sides can authenticate each other as such. Regular MyNet devices also authenticate the Broker. Authentication is done via X.509 certificates trusted by the MyNet middleware and issued by the MSP to the Broker and the MVDs. Regular MyNet devices continue to use UIA self-signed certificates [1], [3]. All communications to the Broker are initiated by MyNet devices (regular and MVDs) and take place over secure IPv4 SSL connections. The use of MyNet Brokers is transparent to the end-users.

Finally, the MSP infrastructure includes one or more (for load balancing) hosts called *MyNet Rendezvous (MRV)*. The role of these hosts is to run an instance of the UIA P2P routing layer on a publicly routable IPv4 host. This guarantees connectivity to the MVDs over the P2P overlay and, consequently, to all other devices in the MVDs' PDCs.

C. *MyNet Virtual Devices*

The main integration point between the P2P MyNet system and the MSP Infrastructure is the MVD. MVDs are a type of MyNet devices that are hosted on the MSP infrastructure. As a result, an MVD is available and reachable over the P2P overlay 24/7 and can guarantee connectivity among all devices in its PDC and linked PDCs.

MVDs run a modified version of the P2P MyNet middleware that has no UI components and where P2P MyNet Introductions are assisted by an RPC exchange with the MyNet Broker. Running an instance of the MyNet middleware allows MVDs to behave like all other MyNet devices, i.e. route traffic over the P2P MyNet overlay, become members of a user's PDC, run distributed applications, host personal content, and share their resources via Passlets issued by PDC devices. Once a user decides to make an MVD part of his/her PDC via the Remote MyNet Introduction process, the MVD appears and behaves exactly the same as any of his/her other MyNet personal devices.

D. *Remote Introductions*

P2P MyNet enables the user to bring a new device in physical or local network proximity with any of his already bootstrapped MyNet devices and manually performing what is called the P2P MyNet Introduction process. This process is based on exchanging peer discovery records containing security credentials and connectivity information. The user/owner of the existing PDC manually authorizes via this process the new device to join his/her PDC. From that moment on, the new device has full connectivity and secure access to the user's PDC resources. Furthermore, the user can use a similar P2P MyNet Introduction process to initiate the creation of a social link from his/her PDC to another user's PDC. After this process is complete, traffic can be exchanged among devices of the two PDCs, depending on user's authorization enforced by the MyNet security.

To allow users to add MVDs and social contacts remotely, we propose to complement the P2P introduction process with a new Remote MyNet Introduction process. This is implemented by additional MyNet middleware components on all MyNet devices (regular and MVDs), which allow them to exchange RPC messages with the MyNet Broker.

Remote MyNet Introduction of MVDs. After a new MVD is instantiated, it registers with the MyNet Broker and sends it its peer discovery record, which is the same as in the P2P MyNet Introduction process. The Broker replies with the overlay routing information of the MyNet Rendezvous (MRV). The MVD's P2P overlay router uses this information to add an overlay route to the MRV. This ensures that P2P overlay traffic destined to the MVD can be later routed by the MRV, even though the MVD may be behind the MSP's NAT/Firewall.

When a user decides to use one of his/her devices to register for an MVD, a request is sent by that device to the Broker. Security information about the user's device is stored by the Broker at this time that will allow it to authenticate it later. In response, the user's device receives from the Broker a modified version of the MVD's peer discovery record, in which the Broker has replaced the overlay routing information produced by the MVD with that of the MRV. This will allow the rest of the P2P MyNet Introduction messages to be routed through the MRV. The user's device then proceeds to merge with the MVD over the overlay according to the P2P MyNet Introduction process, with the difference that, before consenting to join the user's PDC, the MVD requests authorization from the MyNet Broker. The Broker checks if the user has registered and the device authorization information matches the one stored earlier and, if yes, authorizes the merging to complete. From that point on, the MVD becomes part of the user's PDC.

Remote MyNet Introduction of social contacts. To add a social contact remotely, the process has similarities to the case of adding an MVD. We will describe it assuming that User A wishes to add a social link to User B. We also assume that User A has already an MVD in his PDC.

When User A decides to invite User B to create a social link between their PDCs, he uses any of his PDC devices (e.g. D1) to contact the MyNet Broker and request for a remote invitation to be sent. The user may specify an out-of-band method on how to notify User B, e.g. an email address or an SMS number. The Broker authenticates D1 as being a device in the same PDC with a registered MVD and, if yes, it creates a large random number (large enough that the probability of guessing it is almost zero, e.g. 128-bit), which is called the Random Invitation Number (RIN), and sends it back to D1. If an out-of-band notification method was specified by D1, the Broker also sends the RIN to User B. Otherwise, User A can just call B and tell him the RIN. At this point the Broker adds an entry that corresponds to the RIN in its internal invitations database. This invitation has a default expiration period (e.g. 7 days), which can be modified by the user, up to a global system maximum (e.g. 1 month). User A can revoke the invitation at any time.

When (and if) User B decides to accept User A's invitation, she uses any of her PDC devices (e.g. D2) to notify the MyNet Broker that she desires to respond to an invitation identified by a certain RIN. If the MyNet Broker finds in its invitations database an entry that corresponds to this RIN, it responds with a modified version of User A's MVD peer discovery record, where it has again replaced the overlay routing information with that of the MRV. The rest of the P2P MyNet Introduction process proceeds as usual, with the difference that, before consenting to create a social link to device D2, the MVD requests authorization from the MyNet Broker. If successful, the process completes and Users A and B have linked their PDCs.

E. MyNet-aware Internet Services

In order to seamlessly integrate Internet consumer services with the P2P MyNet system, we propose special MyNet-aware applications that use the MyNet API, called *MyNet-aware Internet Services (MaIS)*, which run on MVDs and act as MyNet-aware proxies of existing Internet services. MaIS are MyNet-aware distributed applications which, on one side (the Internet-side), use whatever distributed interface these Internet Services expose over the Internet (e.g. Web Services via SOAP, XML-RPC, HTTP), and on the other side (the P2P MyNet-side), translate these interfaces to appropriate MyNet RPCs, which are invoked by the user's MyNet-aware clients over the MyNet P2P network (Figure 2).

MaIS appear to the user as any regular MyNet distributed applications running on his/her other PDC personal devices (Figure 3). Because they are MyNet-aware, MaIS can take full advantage of MyNet's unique features, such as the MyNet service management, security, and intuitive UI frameworks [3]. Because they are running on an MVD, i.e. on a device in the user's PDC, MaIS have seamless and secure access to all of the user's personal devices, content and distributed applications, wherever they may reside, as soon as they are created. The user can share selective MaIS functionality with any of his/her social contacts using Passlets, in the same way as he/she shares any of his other personal resources.

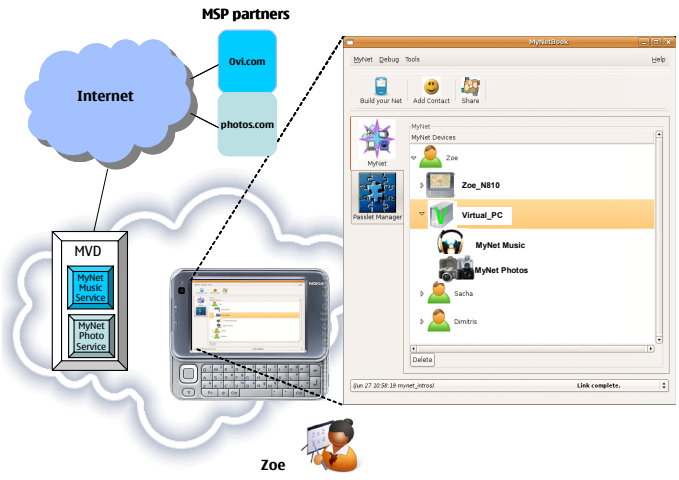

Figure 3: User view of MyNet-aware Internet services.

The MyNet service management framework installs the server-side and client-side components of the MaIS by default or on user's demand. The MSP can customize the

user experience for a particular service by customizing the client-side application. For instance, the front-end GUI for a mobile phone will be designed differently than the front-end GUI for a laptop for the same MaIS service.

Finally, MaIS may be composite services that combine functionality from more than one Internet services. For example, a MaIS may offer a service that ships photos from a Photo Printing online service on frames selected from another online retailer, while the user interacts with only one service. In addition, MaIS composite services may include components from personal distributed applications running on the users' own PDC devices. For example, the above MyNet Photo Printing service could include a component that allows the user to print snapshots captured from live video in his/her Wi-Fi home camera.

V. IMPLEMENTATION

A. Prototype

The hybrid MyNet platform was prototyped for PCs and laptops running Ubuntu Linux, using C, C++, shell scripts and Python. It has also been ported to the Nokia N800 (Linux OS), and MacOS X. MVDs were prototyped using VMWare Workstation 6.0.1 Virtual Machines (VM) running on an Ubuntu Dell XPS 410. Each VM was assigned 384 MB of RAM and 10 GB of disk for OS and personal data storage. These low requirements allow support for 8-10 MVDs even on a regular PC with an unoptimized VM setup. Figure 4 shows MyNet on the current experimental setup.

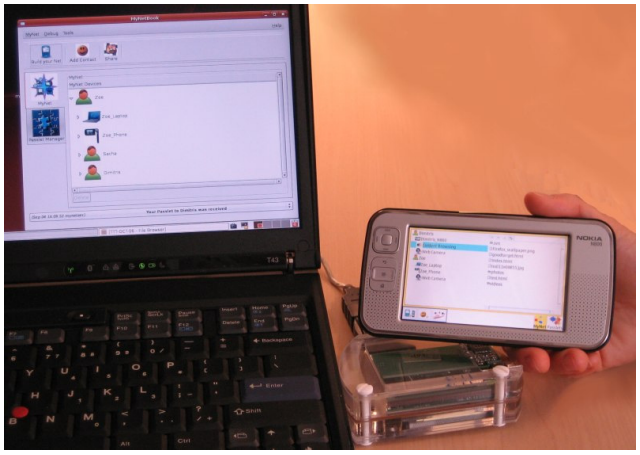

Figure 4: MyNet experimental prototype.

The MyNet user experience was a fundamental system design goal. Therefore, special effort has been made to reflect it in the experimental prototype. In this section we focus our presentation on functionality related to MVDs and remote introductions. The reader is referred to [3], [20] for more on the P2P aspects of the MyNet implementation.

Figure 5 demonstrates the user experience of adding an MVD. Under the "Add Personal Device" toolbar option, the user selects "Add Virtual Device". An optional registration window prompts the user to enter the displayed number; this step aims to avoid spam registrations by software entities. This completes the process and the newly added MVD appears as one of the personal devices. The user can simply click on the MVD icon in order to access its services.

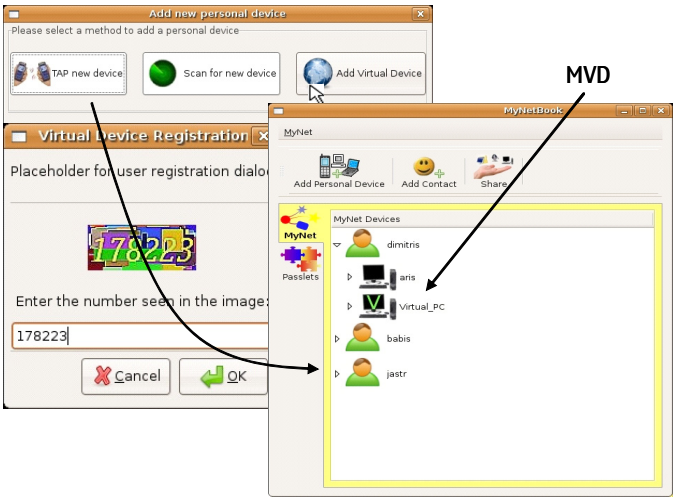

Figure 5:Prototype: adding an MVD.

The Remote MyNet Introduction process is depicted in Figure 6. Under the "Add Contact" toolbar option, Dimitris selects "Send Invitation" and chooses to enter Zoe's email. After receiving Dimitris' email with the RIN, Zoe selects "Accept Invitation". This completes the Remote Introduction process. From this moment on, both Zoe and Dimitris see each other in their Contacts and can start sharing any of their resources, including those offered by Dimitris' MVD.

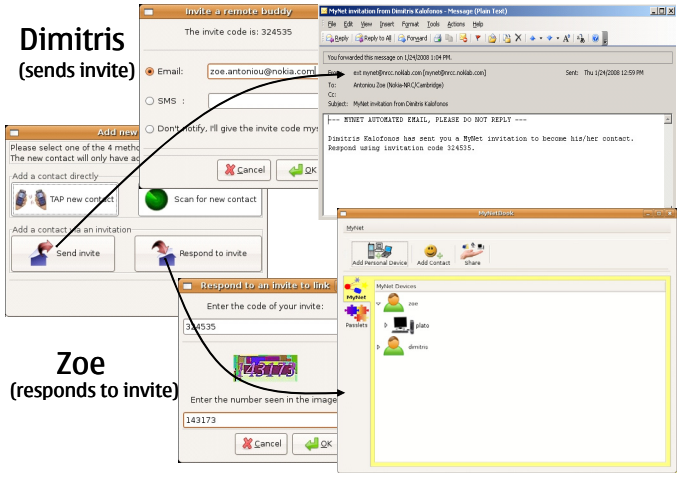

Figure 6:Prototype: adding a "buddy" remotely.

B. User Evaluation

This section presents results from a user evaluation of MyNet, which included, among others, the concepts of sharing, Passlets, MVDs and MaIS. The study was conducted in November 2007 and included 50 participants, ages 15-55+, with a diverse educational background and no formal technical training. TABLE 1 summarizes the most relevant results. Though security and privacy concerns were raised by the users, overall, Passlets were rated as a useful sharing mechanism by 96% of the participants, while 86% agreed that it was an easy to understand security concept.

Remote introductions were rated as useful by 98% of the participants. After using the prototype, 83% of the users agreed that they would try MyNet in conjunction with or as an alternative to current sharing technologies.

With respect to MaIS, 62% of the participants indicated that they would sign up for a free (ad-sponsored) MVD, while 18% were opposed due to privacy/security concerns. MyNet-aware Internet Services were rated useful in the context of personal networks (90%), professional networks (83%) and social networks (69%).

TABLE 1: SELECT USABILITY STUDY RESULTS.

ISSUE	YES	NO	Neutral
MyNet sharing, security & remote introduction:			
Users rated Passlets concept easy to understand as a security mechanism after using it once.	86%	8%	6%
Users rated Passlets useful as sharing mechanism	96%	2%	2%
Users rated remote introductions useful	98%	2%	0%
Users trust MyNet enough to use it in conjunction with or as an alternative to current sharing technologies	83%	2%	15%
MyNet-aware Internet Services:			
Users would sign up for a free (ad-sponsored) MVD	62%	18%	20%
Users would use MaIS for Personal Networking	90%	3%	7%
Users would use MaIS for Social Networking	69%	8%	23%
Users would use MaIS for Professional Networking	83%	5%	12%

Finally, Figure 7 looks more closely at the users' main concerns with respect to MaIS services. Using services through an MVD in their PDC raised strong privacy and security concerns for their personal data. The second most important issue was ease-of-use of MVD services. Although, clearly, an MSP would need to put special effort into gaining users' trust, we believe that these are encouraging results.

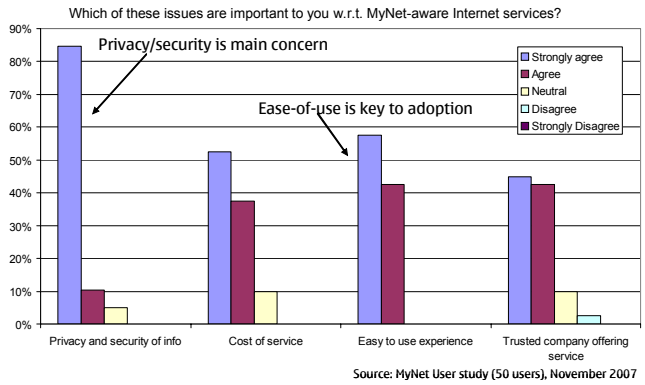

Figure 7: Key issues for MyNet-aware Internet Services.

VI. Conclusions and Future Directions

This paper extends MyNet [3], our P2P personal and social networking platform, by incorporating a centralized component based on the concept of MVDs. Infrastructure support guarantees connectivity and offers seamless integration with Internet consumer services. The key to the success of such as a system is reassuring users about the security and privacy of their data, as well as ease-of-use.

The proposed hybrid architecture enables the creation of a wide range of MaIS that can be easily customized. Users can install MaIS to consume new Internet services or to access services they have already signed up for (e.g. [4], [5], [6]).

In addition to prototyping example MaIS, we are currently working on examining the issue of MVD scalability. Our goal is to bring the cost of hosting MVDs to the same level as commercial storage and application hosting Internet services (e.g. [18]). We are considering two alternatives: (a) reducing the footprint of VMs used for MVDs and taking advantage of recent advances in virtualization technologies, (b) extending the MyNet/UIA middleware to implement MVDs as different user accounts and not VMs, each with its own EID and overlay network interface, as suggested in [1].

References

[1] B. Ford et al, "Persistent Personal Names for Globally Connected Mobile Devices". In Proc of 7th USENIX Symp. on OS Design and Implementation (OSDI'06), Seattle, WA, Nov 2006.

[2] JXTA Community Projects, https://jxta.dev.java.net/

[3] D.N. Kalofonos, Z. Antoniou, F. Reynolds, M. Van-Kleek, J. Strauss, and P. Wisner, "MyNet: a Platform for Secure P2P Personal and Social Networking Services". In Proc. 6th IEEE Intl. Conf. on Pervasive Comp. and Comm. (PerCom'08), Hong-Kong, March 2008.

[4] "Facebook", http://www.facebook.com/.

[5] "Myspace", http://www.myspace.com/.

[6] "Flickr", http://www.flickr.com/

[7] B. Popescu et al., "Safe and private data sharing with Turtle: Friends Team-Up and Beat the System," in *Proc. 12th SPW*, 2004.

[8] S. Marti, P. Ganesan, and H. Garcia-Molina, "SPROUT: P2P routing with social networks," in *P2P&DB*, 2004.

[9] J. Li and F. Dabek, "F2F: Reliable storage in open networks," in *5th IPTPS*, Santa Barbara, CA, Feb. 2006.

[10] J. Pouwelse *et al*., "Tribler: A social-based peer-to-peer system," in *5th IPTPS*, Feb. 2006.

[11] S.A. Baset and H. Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol",http://arxiv.org/abs/cs.NI/0412017

[12] J. Liu and J. Callan, "Content-based Retrieval in Hybrid Peer-to-Peer Networks", Proceedings of CIKM'03, November 2003.

[13] R. Barrett and P.P. Manglio, "Intermediaries: New Places for Producing and Manipulating Web Content", Proc. of 7th International WWW Conference, 1998.

[14] A. Fox et al. "Adapting to Network and Client Variation Using Active Proxies: Lessons and Perspectives", IEEE Personal Communications, Vol. 5, No. 4, Aug. 1998.

[15] C.H. Rao et al., "iMobile: A Proxy-based Platform for Mobile Services", ACM Proc. 1st Work. on Wireless Mobile Internet, 2001.

[16] Wang et al., "ICEBERG: An Internet-core Network Architecture for Integrated Communications", IEEE Personal Communications Special Issue on IP-Mobile Telecommunication Networks, 2000.

[17] P.K. McKinley et al. "Composable Proxy Services to Support Collaboration on the Mobile Internet", IEEE Transactions on Computers, Vol. 52, No. 6, 2003.

[18] Amazon Web Services, http://www.amazon.com/aws

[19] Google App Engine, http://code.google.com/appengine/

[20] Z. Antoniou and D.N. Kalofonos, "User-Centered Design of a Secure P2P Personal and Social Networking Platform". In Proc. 3rd IASTED Intl Conf on Human-Computer Interaction, Austria, March 2008.