Use of Peer-to-Peer Technology in Ambient Intelligence

Cornelia Kappler and Frank-Uwe Andersen, Siemens Information & Communication, 13627 Berlin, Germany; *{cornelia.kappler / frank-uwe.andersen}@siemens.com*
Kurt Tutschku, Lehrstuhl für verteilte Systeme, Institut für Informatik, Universität Würzburg, Am Hubland, 97074 Würzburg, Germany; *tutschku@informatik.uni-wuerzburg.de*

Abstract

In the Ambient Intelligence environment of the future, we expect intelligent, embedded devices need to flexibly respond to input they receive, and hence they need to continuously update their information. In this paper, we investigate the feasibility of using Peer-to-Peer technology for realising distribution of these information updates. We illustrate our ideas by two scenarios, discuss the technical problems that arise and finally analyse to what extent technology available today can address these problems.

1 Motivation

In the Ambient Intelligence environment of the future, intelligent, embedded devices presumably need to flexibly respond to input they receive. Hence they need to continuously update the information about their surroundings. In this paper, we investigate the feasibility of using Peer-to-Peer technology for realising distribution of *information updates*, e.g. user profiles, device configuration or software, in an AmI environment.
This article is organized as follows: We give an overview of Ambient Intelligence (AmI) and Peer-to-Peer (P2P) technology, and introduce the basic idea of how P2P technology could be used in AmI. We illustrate our ideas in two scenarios, describe problems that need to be addressed, and finally analyse applicability of technology available today for realizing these ideas. In the last sections we present related work and draw conclusions.

2 Introduction

2.1 Ambient Intelligence

Ambient Intelligence (AmI) is a new concept foreseen to be supported by the 4th generation of mobile networks. It stands for an environment of a multitude of embedded intelligent devices (AmI Devices) that respond to the presence of users in a seamless, unobtrusive and often invisible way [1]. Examples are the proverbial milk-ordering fridge, or, as illustrated in Sec. 3, an airport dealing with immigration automatically by wireless interaction with an electronic representatives of the traveller.
AmI Devices can be sensors and actuators, intelligent appliances or other intelligent electronic devices. They typically communicate wirelessly, either among themselves or with centralized control equipment.

The AmI vision entails AmI Devices are not programmed once-and-for-all. Rather, they must be easily re-programmable after deployment, and must be able to retrieve up-to-date information, e.g. user-specific information, to process an event. Moreover, AmI Devices presumably have intelligence to recognise when they need information updates, and to act autonomously to obtain this knowledge.

2.2 Peer-to-Peer Technology

P2P technology [2] provides a simple and therefore low-cost while efficient mechanism to pool and share exchangeable resources like disk space, files – e.g. MP3 files - , state information or CPU cycles. P2P-based sharing and distribution of resources is an alternative to centralized client-server based systems which today are preferred by operators.
P2P technology is based on the interaction of equal partners called “peers”. Each peer in principle has identical capabilities and responsibilities – although in some P2P networks, some peers are “more equal” and assume more or specialized tasks, in order to improve scalability. P2P networks typically form and operate in a self-organised fashion, i.e. there is no central entity managing the process. Peers are autonomous and may leave or join a P2P network arbitrarily without impacting the overall operation. Popular examples of services building on P2P technology are file-sharing services such as KaZaa [3] and eDonkey [4], or P2P voice-over-IP such as Skype [5]. JXTA [6] and FreeNet [7] offer frameworks for deploying P2P services.
In general, applications based on P2P technology need to support two fundamental coordination and control functions: a) *resource mediation mechanisms*, i.e. functions to locate resources or entities, and b) *resource access mechanisms*, i.e., functions to permit, prioritize, and schedule the access to resources. *Pure P2P* architectures, such as Gnutella [8], are imple-

menting the fundamental control function in a fully decentralized manner [9]. *Hybrid P2P* systems may perform one of these functions in a more centralized mode.

2.3 Peer-to-Peer Technology in Ambient Intelligence

Applying P2P technologies for updating AmI Devices is interesting for several reasons:

- The autonomy of AmI Devices maps onto the autonomy of peers.
- Decentralizing the process of distributing information updates among AmI Devices improves some aspects of scalability because information update requests do not need to be processed by a single server.
- P2P technology per-se has no notion of geographic location. However, typically, information updates are of local interest (e.g. a moving user). Thus P2P data sharing keeps traffic local, reducing wide area data traffic.
- Users of P2P services, e.g. file sharing services, usually form loose groups with common interests that search and exchange resources. These communities typically are defined only on a semantic level, i.e. by what they search. We expect similar behaviour of AmI Devices that can be exploited to increase efficiency.

3 Scenarios

3.1 Business Traveller

In the first ISTAG AmI Scenario [1], the business woman Maria travels abroad. Assisted by a personalized communication device on her wrist, the P-Com, interacting with local AmI Devices, she walks through immigration and enters the car she rented without visible administrative interaction. Her hotel room is personalized by AmI Devices interacting with the P-Com as she enters, e.g. by adjusting temperature, music and video choices. The computer files she needs are transferred to a local laptop.

While each AmI Device is performing a different task, it typically needs the identical basic information ("user profile"), e.g. for authentication. It makes sense to retrieve this information from a local, trusted, AmI peer device rather than multiple times from Maria's home network. Information exchange is kept local, speeding up the process and saving overall bandwidth. Local bandwidth usage would however be slightly increased due to the higher communication needs of a distributed P2P service. Furthermore, Maria does not need to authenticate with each AmI Device. Rather her user profile is propagated peer-by-peer as she moves along, saving her time. Processing overhead due to authentication with each AmI Device is thus reduced at the cost of user profile distribution overhead. Storage of user profiles would be soft-state in order to prevent misuse and state overflow.

Basic information in the user profile includes authentication and authorization information, other security settings such as where the user profile is allowed to propagate, charging information etc.

3.2 Temporary Extension of a Mobile Access Network

In the following scenario we slightly extend the scope by illustrating the updating of intelligent devices is not restricted to AmI environments.

With mobile communication becoming an ubiquitous commodity, it will become increasingly important for operators to easily extend their access network infrastructure to accommodate shifting user concentrations. For example, a major sports event such as the Olympics or the soccer world championship call for temporarily increased mobile access capacities. Other mass-events such as major rock concerts raise the same problem – and business opportunity.

The mobile access infrastructure is extended by installation of new antennas and control nodes, e.g. Node Bs and RNCs for UMTS. These nodes need to be configured in order to attach them properly to the existing core network. Manual configuration is time consuming and expensive. Hence an automated process would be desirable, in which the necessary information is fed into the new infrastructure only once, and then it distributes and installs itself automatically. P2P technology is one possible choice for supporting this process.

Similar to the Business Traveller Scenario above, information updates in this scenario are shared locally in a peer group of common interest, e.g. among Node Bs or RNCs only. The members of this group need to have a trust relationship in order to prevent rogue nodes from distributing malicious information. Furthermore, group members need to have an idea of the kind of information update they are interested in.

4 Problem Analysis

While it is clear how the above scenario can be realised in principle, a number of problems and issues arise when looking at it in more detail.

- Bootstrapping

A common P2P base protocol seems essential for performing AmI "bootstrapping", e.g. neighbour discovery and related tasks. Other tasks however can be performed using application-specific protocols. Usage of common protocols that must be known by all AmI Devices should be reduced to a minimum.

- Group Formation

Group formation is expected to be a key function in AmI systems. Group structures reduce the effort for locating information since fewer entities have to be

checked. Furthermore, some information updates, e.g. user profile information, are sensitive information that should only be shared with and received from suitably authorised AmI Devices. Therefore AmI Devices need to form groups in which members have a trust relationship, and in which all members are authorised to the same level of information – e.g. some groups share just basic authentication information, whereas other groups are authorised to also handle banking information.

Group formation can be enforced on a case-by-case basis by the administrator, or, more conveniently, each device joins groups based on preconfigured profiles. It is interesting to consider how this self-configuration would work if the set of existing (or to be founded) groups is not known in advance. In this case a list of existing groups must be openly accessible. If the name space of groups is not standardized, a group's purpose or the nature of information updates shared within a group would need to be described in a meta-language. A new device entering a network would need "a high level view of what its purpose is" in order to be able to join or found the right groups. Related ideas are described in more detail in [10] as "A Knowledge Plane for the Internet".

The same AmI Device may belong to multiple groups. Groups can be organised hierarchically, e.g. regarding authorisation rights or relating to company organisation. The P2P technology as a means for AmI hence needs to support hierarchical group management, and only peers in the same group are allowed to share particular information updates. Group formation can be an ad-hoc process based on preconfigured profiles, or it can be enforced by the administrator.

- Choice of suitable information update

How do AmI devices know what information update are of interest to them? In today's P2P file sharing applications the user makes a guess at a suitable string in the file name. This method clearly is not applicable here. Possibilities are that an AmI device always synchronizes its information with that of other peers in its group(s). It may also make a more educated choice based on rules or, again, based on "a high level view of what its purpose is". As with group names, the naming of information updates either needs to be standardized, or meta-information needs to be provided describing the content of each information update.

- Security and Trust

Many interesting security aspects need to be considered, in addition to those already mentioned.

It must be ensured that sensitive user information cannot be corrupted or eavesdropped, particularly on the wireless links between AmI Devices, due to the broadcast nature of wireless transmissions. AmI Devices of one group can be assumed trustworthy, however, we need to protect against man-in-the-middle attacks by encrypting and integrity protecting data. A detailed security analysis also needs to consider other threats, such as Denial-of-Service attacks by a malicious device, e.g. flooding an AmI Device with bogus user profiles that subsequently propagate to all neighbouring AmI Devices.

- Mobile wireless P2P technology

Today's P2P technology is typically used in wired environments. Hence, it is not adapted to the special restrictions found for wireless mobile devices. These comprise limited and possibly expensive bandwidth on an air interface, highly dynamic error rates, potentially high delay times (in the case of 2G/3G networks) and delay variations, some probability for interruption of connectivity or limited online-time, and scarce resources on peers, including battery-lifetime. P2P technology hence needs to be adapted to handle wireless peers.

- Interaction with the network topology

When AmI devices are communicating via a centralized access point, P2P-based applications form an overlay network that is rather independent of the network topology. However when the AmI devices form an ad-hoc network, the ad-hoc routing protocol should be coordinated with the P2P resource mediation mechanism as described in [11] in order to maintain meaningful routes only.

- Comparison with centralized approaches

P2P-based distribution of information updates for AmI devices is just one way to solve the problem. Another possibility is the classic client-server based approach, where AmI devices draw information updates from one centralized server. A P2P-based solution must be compared to client-server based solution. It is expected that client-server based solutions are more efficient since there is less signalling overhead due to self-organization. However, P2P-based solutions typically are more robust, and moreover they are self-organized and hence require less manual configuration. It is an open problem how to provide "carrier-grade P2P services" that guarantee timely delivery of information updates.

5 Realization Paths

In this section we analyse to what extent information updates of AmI Devices using P2P technologies is already possible with today's technologies. Technologies of interest include wireless transmission technology P2P technology and security support.

4.1 Wireless Transmission Technology

AmI Devices need secured wireless communication among themselves. Ideally, they form a multi-node multi-hop ad-hoc network. Interaction with user devices adds another hop. At this point, however, only simple single-hop ad-hoc networks are commercially available. Alternatively, all AmI devices communicate via networked access points. Possible technologies for AmI communications include (ordered ac-

cording to increasing range) Bluetooth [12], IEEE802.15.4 and the related ZigBee [13], the IEEE 802.11x [14] family of wireless LAN, and 2.5/3G networks [15].

Bluetooth (BT) allows ad-hoc secure short-range peer-to-peer communication, optionally supported by an access point. In particular, two BT nodes can engage in a trusted relationship by a so-called "pairing process", by exchanging authorization profiles. A generalization of this pairing process would allow for secured group formation as described above. A BT piconet is a group of up to eight devices actively connected to one master device. Many more devices can be connected in a "parked", inactive state. The latest BT protocol version (1.2) supports overload management for operation in environments with many wireless participants as well as a "scatternet" mode. A scatternet is a group of piconets which are connected because some participants are a member of several piconets. It is however not possible for two piconets to communicate unless they are in broadcast range of each other.

IEEE 802.15.4 and the ZigBee alliance protocol layers on top of it enable wireless personal area networks (WPAN). Running the TCP/IP protocol suite on top of IEEE 802.15.4 layers is also possible instead of ZigBee. Star and P2P (Mesh-) topologies are defined, the former requiring a traversal of a centralized "PAN coordinator", the latter supporting direct device-to-device communication paths. Additionally, ZigBee provides a toolbox for security key dissemination.

Applications in ZigBee and BT use profiles to describe the interaction they expect from other devices. E.g. a certain application could declare it resides on a headset and is only interested in audio files. While the number of ZigBee profiles currently is limited, and profile definitions in ZigBee and BT are not interoperable, in principle profiles could support group formation of AmI devices.

The 802.11x protocol family allows two modes of operation: In infrastructure mode, devices are attached to an access router. All communication between devices is via the access router. Access routers can also be networked among themselves. In ad-hoc mode, single-hop ad-hoc communication between pairs of devices is supported. While the original – and today commonplace - 802.11b specification has limited security, with the new 802.11g plus 802.11i, security management has become more attack-resistant and is currently being developed further.

2.5G and 3G Networks at this point do not allow peer-to-peer communication, but all communication is tree-like via the network infrastructure. Security is high, albeit not suited for distributed applications and group formation [16]. The (U)SIM card on the mobile device offers a trusted environment in which security-relevant data is stored safely, and 2.5/3G networks offer security infrastructure for processing this information. 2.5/3G networks have good coverage, mation. 2.5/3G networks have good coverage, whereas range of 802.11x networks and particularly BT is more limited. At the same time, usage of 2.5/3G networks typically is license-bound and charged, whereas usage of BT and 802.11x is free and uses license-free spectrum.

Since some data needs to be retrieved non-locally, an architecture lends itself in which all or some devices support all three technologies and seamlessly switch between them. Such seamless inter-technology handover presumably will only be common in 4G networks. 3G/WLAN interworking in fact is currently being standardized, albeit at this point with limited functionality [17]. In [18], a secure multi-radio architecture is proposed based on the SIM / USIM that additionally integrates BT and other wireless technologies.

4.2 P2P Architecture

An initial step in the design of a P2P architecture for AmI support is to find out what is the appropriate architecture, particularly how the two fundamental control functions for P2P networks, *resource mediation* and *resource access* defined in Sec. 2.2 are realized. In P2P-supported AmI, these control functions have to be implemented in very reliable, e.g. highly available, strongly secure, e.g. highly trusted, and especially efficient way, i.e. fast and with little overhead.

Figure 1 provides a two-dimensional cartography, in which the two control functions form the axes. Both control functions can be realized in a centralized or decentralized fashion. The degree of decentralization is the range of the axes. The cartography maps the architectural choices for realizing control: a domain of *device-centric* P2P architectures, which expose a strongly decentralized control whereas the domain of *infrastructure-oriented* P2P architectures is characterized by a strong centralization of control.

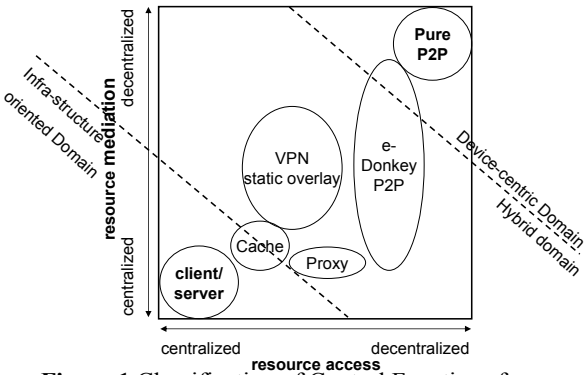

Figure 1 Classification of Control Functions for P2P Architectures

A *cache* temporarily stores popular information updates and peers draw them from the cache instead of from other peers. Such an approach could be suitable when AmI devices are communicating via a central-

ized access point anyways. The cache could be located with the access point. In principle caching is an opposite concept to P2P, as it transfers access control away from the peers.

Proxies can support at central locations the communication between peers, e.g. for locating mediation entities in an infrastructure-oriented P2P architecture.

Hybrid P2P architectures, such as the eDonkey File-sharing network [4], which utilize multiple servers for fast resource mediation, support group formation. *Virtual Private Networks (VPNs)* are able to support a variety of centralized and decentralized architectural choices. They can support secure group formation of AmI devices. A drawback are their static nature and the reduced adaptivity of VPNs, e.g. VPNs still need high configuration efforts and are inherently not sensitive on the underlying physical network topology..

Currently, decentralized resource mediation control based on *Distributed Hash Tables (DHTs),* such as Chord [19] or Content Addressable Networks (CAN) [20] is discussed as a very promising techniques. DTHs provide resource mediation based on hashing functions which assigns unique hash keys to resources. Each peer is responsible for a certain range of the hashing function and maintains links to peers holding neighboring hash value ranges. Thus resources can be located in a small number of hops. Reliability and minimal latency, however, are a challenge for DHTs. The peers which hold the information may be far away in the network, might have an unstable on-line behaviour, or may experience varying degree of congestion and packet loss. Recent analyses have shown that these characteristics can be handled, or are not as severe as expected if DHTs are appropriately designed [21,22].

Resource access control in P2P applications has to maintain the autonomy of the entities, i.e., peers retain the ability to decide what resources are shared and how this is accomplished. Popular P2P file sharing application have proven that mechanism like *swarming,* i.e. a resource /file can be obtained/downloaded from several different peers at once, or *hording,* i.e. peers cooperate in resource access, can be implemented in a highly decentralized way.

4.3 Peer-to-Peer Frameworks

JXTA offers a framework for deploying P2P services. It includes protocols for bootstrapping and support for group management, including hierarchical groups and peers being members of multiple groups. “JXTA for J2ME” (JXME) [23] is an extension for supporting resource-limited mobile peers. These peers only assume limited functionality and are supported by a fixed proxy infrastructure. This solution however is not adequate for the problem at hand since the mobile peers, i.e. AmI Devices, need to be able to function autonomously without infrastructure support. Whether this is technically feasible needs to be explored in future work.

The Freenet P2P framework has been designed with security and especially privacy in mind, offering a fully anonymised and distributed file system. It is possible to build services on top of Freenet, such as anonymous chat forums, news and mail servers. However Freenet offers neither group formation nor mobility support.

4.4 Trust and Reputation

Different trust and reputation mechanisms are currently studied for ad-hoc networks, e-commerce systems, or P2P services [24-26]. *Trust* is a peer’s believe in another peer’s capabilities, honesty, and reliability based on his its own experience, whereas *reputation* is a peer’s belief based on recommendations received from other peers [26].

Reputation can easily be implemented in centralized architectures by using trusted entities. This feature suggests the application of reputation mechanisms in infrastructure-oriented P2P architectures. However, the reputation mechanisms inherit the disadvantages of limited scalability of centralized architectures. Trust mechanisms, therefore, appear better suited for device-centric P2P architectures. However, the scalability and performance of these mechanisms with respect to mobility and different type of on-line behaviour has to be investigated.

5 Related Work

The traditional means for sharing information updates are directory services, i.e. a centrally managed, centralized repository exists either with the actual data, or with links to this data. The drawbacks of this approach are management overhead, single points of failure, processing bottleneck, and routing overhead.

In [27], an “Ambient DB” is described, providing relational database functionality, while most data is stored in a distributed fashion on AmI Devices, and only integrated at query time. This approach is particularly suitable for decentralised management of persistent structured data, e.g. a family music collection. In this paper however we aim at the efficient distribution of information updates that are either short-lived (e.g. information related to user presence) or immediately consumed (e.g. software updates).

The MIGRA system [28] builds on JXTA and JXME to support the migration of a user’s context information across “smart spaces” (a concept similar to AmI) in order to support ubiquitous services available at any point in the network. As a result, users are able to move and to suspend a computing task in one environment and resume it in another. In this paper, we generalize this idea towards the exchange of any information update. Information updates not necessarily triggered by human users, but also by machines.

In the case of software being the information update distributed in the P2P enhanced AmI environment, the step towards mobile agent technology seems rather small. Agent technology knows and uses the concepts of self-replication and travelling code, i.e. executable code that serializes (i.e. packs) itself and sends itself to other entities in the network that will execute the new instance of the code.

6 Conclusion

In this paper we discussed the feasibility of using P2P technology for realising distribution of information updates in AmI devices. We conclude that using P2P technology is a viable option, however its performance compared to other approaches, notably traditional client-server technology needs to be investigated. Furthermore we showed that while important technology support for realizing P2P supported information updates of AmI Devices already exist, some ingredients are still missing, most notably ad-hoc networking, seamless, integrated multi-radio transport, support for secured group formation, and adaptation of P2P technology to mobile peers.

7 Literature

[1] K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten and J-C. Burgelman (Eds), IST Advisory Group of the European Commision Community Research, „Scenarios for Ambient Intelligence in 2010", Feb. 2001.

[2] R. Steinmetz and K. Wehrle,"Peer-to-Peer-Networking & -Computing", Informatik Spektrum, Band 27.1, Feb. 2004.

[3] N. Leibowitz, M. Ripeanu, and A. Wierzbicki, "Deconstructing the Kazaa Network", WIAPP'03, San Jose, CA., June 2003.

[4] MetaMachine Inc., www.edonkey2000.com.

[5] http://www.skype.com .

[6] http://www.jxta.org.

[7] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A Distributed Anonymous Information Storage and Retrieval System",, ICSI Workshop on Design Issues in Anonymity and Unobservability, July 2000.

[8] The Gnutella Protocol Specification v0.4, available at http://dss.clip2.com, 2001.

[9] D. Barkai: "Peer-to-Peer Computing", Intel Press, Hillsborow, OR, 2001.

[10] D. Clark, C. Partridge, Ch. Ramming, and J. Wroclawski, "A Knowledge Plane for the Internet", ACM Sigcomm 2003, Karlsruhe, Germany, Aug. 2003.

[11] R. Schollmeier, I. Gruber and F. Niethammer, „Protocol for Peer-to-Peer Networking in Mobile Environments", Proc. ICCCN'03, Dallas, USA, Oct. 2003.

[12] Bluetooth Special Interest Group (SIG): "Core spec.", http://www.bluetooth.org .

[13] http://ieee802.org/15/pub/TG4.html, http://www.zigbee.org.

[14] IEEE 802.11x, http://standards.ieee.org/getieee802/802.11.html.

[15] www.3gpp.org.

[16] 3GPP TS 33.102 "Security Architecture", v6.0.0, Sept. 2003.

[17] 3GPP TS 23.234 "3GPP system to Wireles Local Area Network (WLAN) interworking; System description", v2.4.0 January 2004.

[18] M. Danzeisen, T. Braun, D. Rodellar and S. Winiker, "Heterogeneous Networking Establishment Assisted by Cellular Operators", MWCN 2003, Oct. 2003, Singapore.

[19] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan: "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," ACM SIGCOMM`01, San Diego, Sept. 2001.

[20] S. Ratnasami, A Scalable Content-Addressable Network, PhD Thesis, UC Berkeley, October 2002.

[21] F. Dabek, J. Li, E. Sit, J. Robertson, M. F. Kasshoek, R. Morris: „Designing a DHT for Low Latency and High Throughput", Proc. ACM/USENIX Symposium on Networked Systems Design and Implementation, March 2004.

[22] A. Binzenhöfer, P. Tran-Gia: "Delay Analysis of a Chord-based Peer-to-Peer file-sharing System", Technical Report No. 332, Institute of Computer Science, University of Würzburg, May 2004.

[23] http://jxme.jxta.org/.

[24] S. Capkun, L. Buttyan, J.-P. Hubaux: "Self-Organized Public Management for Mobile Ad-Hoc Networks", IEEE Trans. Mobile Computing, Vol. 2, No. 1, January-March 2003.

[25] B.J. Schaefer, A. Konstan, J. Riedl: „Recommender Systems in E-Commerce", ACM Conference on Electronic commerce (EC-99), Denver, CO, Nov. 1999.

[26] Y. Wang, J. Vassileva: "Trust and Reputation model in Peer-to-Peer Networks", P2P'03, Linköping, Sweden, Sept. 2003.

[27] W. Fontijn and P. Boncz, "AmbientDB: P2P Data Management Middleware Ambient Intelligence", PERWARE 2004, Orlando, Florida, March 2004.

[28] "JXTA, In support of the Migration of Users Across Smart Spaces", M. Commins, MSc. Thesis, Trinity College Dublin, Ireland, 2002.