HELSINKI UNIVERSITY OF TECHNOLOGY
Department of Electrical and Communications Engineering

Juho Heikki Pekka Seppänen

Prospects of Peer-to-Peer SIP for Mobile Operators

Thesis submitted in partial fulfilment of the requirements for the degree of Master of Science in Engineering

Espoo, 25 July, 2007

Supervisor	Jörg Ott
Instructor	Jouni Korhonen

HELSINKI UNIVERSITY OF TECHNOLOGY **ABSTRACT OF THE MASTER'S THESIS**

Author:	Juho Heikki Pekka Seppänen	
Name of the Thesis:	Prospects of Peer-to-Peer SIP for Mobile Operators	
Date:	25.07.2007	Number of pages: 8+114
Department:	Department of Electrical and Communications Engineering	
Professorship:	Networking Technology	Code: S-38
Supervisor:	Professor Jörg Ott	
Instructor:	Jouni Korhonen, M.Sc	

The purpose of this thesis is to present the Peer-to-Peer Session Initiation Protocol (P2PSIP) being developed. In addition, the purpose of this thesis is to evaluate the impacts and prospects of P2PSIP to mobile operators, to whom it can be regarded as a threat. In P2PSIP, users can independently and easily establish voice and other multimedia connections using peer-to-peer (P2P) networking. However, P2PSIP is not meant to replace the existing telephony networks of the operators.

We start by introducing the principles of SIP and P2P networking that the P2PSIP is intended to use. SIP enables to establish, terminate and modify multimedia sessions, but its versatile exploitation requires using centralized servers. By using P2P networking, users can decentralize the functions of centralized servers by performing them among themselves. This enables to maintain large and robust networks without maintenance costs resulted of running such centralized servers.

Telecommunications market is transforming to a more open environment, where mobile operators and other service providers are challenged to adapt to the upcoming changes. Subscribers have easier access to rivalling Internet-services (such as Skype) and in future they can form their own communication communities by using P2PSIP.

The results show that despite of these threats, telecom operators can find potential from P2PSIP in concurrence in adaptation to the challenges of the rapidly changing telecom environment. These potential roles include optimization of the network of the operator, but as well roles to provide alternative and more versatile services to their subscribers at low cost. However, the usage of P2PSIP should not conflict with the other services of the operator. Also, as P2PSIP is still under development, its final nature and features may change its impacts and prospects.

Keywords: Peer-to-peer, SIP, mobile operator, Skype

TEKNILLINEN KORKEAKOULU **DIPLOMITYÖN TIIVISTELMÄ**

Tekijä:	Juho Heikki Pekka Seppänen	
Työn nimi:	Peer-to-peer SIP-protokollan näkymät ja mahdollisuudet mobiilioperaattoreille	
Päivämäärä:	25.07.2007	**Sivumäärä**: 8 + 114
Osasto:	Sähkö- ja tietoliikennetekniikan osasto	
Professuuri:	Tietoverkkotekniikka	**Koodi:** S-38
Työn valvoja:	Professori Jörg Ott	
Työn ohjaaja:	Diplomi-insinööri Jouni Korhonen	

Tämän diplomityön tarkoituksena on esitellä kehitteillä oleva Peer-to-Peer Session Initiation Protocol (P2PSIP), jonka avulla käyttäjät voivat itsenäisesti ja helposti luoda keskenään puhe- ja muita multimediayhteyksiä vertaisverkko-tekniikan avulla. Lisäksi tarkoituksena on arvioida P2PSIP protokollan vaikutuksia ja mahdollisuuksia mobiilioperaattoreille, joille sitä voidaan pitää uhkana. Tästä huolimatta, P2PSIP:n ei ole kuitenkaan tarkoitus korvata nykyisiä puhelinverkkoja.

Työn alussa esittelemme SIP:n ja vertaisverkkojen (Peer-to-Peer) periaatteet, joihin P2PSIP-protokollan on suunniteltu perustuvan. SIP mahdollistaa multimedia-istuntojen luomisen, sulkemisen ja muokkaamisen verkossa, mutta sen monipuolinen käyttö vaatii keskitettyjen palvelimien käyttöä. Vertaisverkon avulla käyttäjät voivat suorittaa keskitettyjen palvelimien tehtävät keskenään hajautetusti. Tällöin voidaan ylläpitää laajojakin verkkoja tehokkaasti ilman palvelimista aiheutuvia ylläpito-kustannuksia.

Mobiilioperaattorit ovat haasteellisen tilanteen edessä, koska teleliikennemaailma on muuttumassa yhä avoimemmaksi. Tällöin operaattoreiden asiakkaille aukeaa mahdollisuuksia käyttää kilpailevia Internet-palveluja (kuten Skype) helpommin ja tulevaisuudessa myös itse muodostamaan kommunikointiverkkoja P2PSIP:n avulla.

Tutkimukset osoittavat, että näistä uhista huolimatta myös operaattorit pystyvät näkemään P2PSIP:n mahdollisuutena mukautumisessa nopeasti muuttuvan teleliikennemaailman haasteisiin. Nämä mahdollisuudet sisältävät operaattorin oman verkon optimoinnin lisäksi vaihtoehtoisten ja monipuolisempien palveluiden tarjoamisen asiakkailleen edullisesti. Täytyy kuitenkin muistaa, että näiden mahdollisuuksien toteuttamisten vaikutusten ei tulisi olla ristiriidassa operaattorin muiden palveluiden kanssa. Lisäksi tulisi muistaa, että tällä hetkellä keskeneräisen P2PSIP-standardin lopullinen luonne ja ominaisuudet voivat muuttaa sen vaikutuksia.

Avainsanat: Vertaisverkot, SIP, mobiilioperaattori, Skype

Preface

This thesis has been written during my employment at the department of Research & Development of Mobility Services of TeliaSonera Finland. I highly appreciate my supervisors Mika Raitola and Juha-Matti Järviranta for giving me this opportunity to carry out this thesis.

I would like to thank my instructor Jouni Korhonen, my supervisor Jörg Ott and colleagues for their indispensable guidance and comments.

Especially I would like to express my sincere gratitude to my family for their support throughout my studies.

Helsinki July 25, 2007

Juho Seppänen

Table of Contents

List of Figures

List of Tables

Acronyms

3GPP	The 3rd Generation Partnership Project
CAPEX	Capital expenditures
CS	Circuit Switched
CSCF	Call/Session Control Function
DHT	Distributed Hash Table
DNS	Domain Name System
DoS	Denial of Service
ENUM	tElephone NUmber Mapping
FQDN	Fully Qualified Domain Name
GRX	GPRS Roaming eXchange
GSM	Global System for Mobile Communications
GSMA	The GSM Association
GTP	GPRS Tunnelling Protocol
HTTP	Hyper Text Transfer Protocol
ICE	The Interactive Connectivity Establishment
I-CSCF	Interrogating-CSCF
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
LI	Lawful Interception
MNO	Mobile Network Operator
MO	Mobile Operator
MSO	Mobile Service Operator
MVNO	Mobile Virtual Network Operator

NAT	Network Address Translation
NGN	Next Generation Network
OPEX	Operating expenditures
P2P	Peer-to-Peer
P2PSIP	Peer-to-Peer Session Initiation Protocol
P-CSCF	Proxy-CSCF
PBX	Private Branch eXchange
PLMN	Public Land Mobile Network
PS	Packet Switched
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SBC	Session Border Controller
S-CSCF	Serving-CSCF
SDP	Session Description Protocol
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SOSIMPLE	Self-Organizing SIMPLE
SIP	Session Initiation Protocol
SHA-1	Secure Hash Algorithm
TDM	Time Division Multiplexing
TISPAN	Telecoms&Internet converged Services&Protocols for Advanced Network
UA	User Agent
UAC	User Agent Client
UE	User Equipment
URI	Uniform Resource Identifier
VoIP	Voice over IP
WG	Working Group
WLAN	Wireless Local Area Network

1 Introduction

For a long time now, the Internet has been using mainly client-server networking, where centralized servers serve the masses of users. Today, peer-to-peer (P2P) networking has become a notable alternative for this traditional client-server approach. Napster, Kazaa, and other (e.g. BitTorrent later on) file sharing networks have shown the potential of P2P networking to build large and globally spread P2P overlay networks to establish communities for file sharing. This is possible through the exploitation of participating nodes (i.e. peers) to build the overlay network and to perform the functions otherwise performed by the centralized servers. Therefore, P2P networks can operate without any server infrastructure, even though some P2P networks use some servers to enhance their functionality. P2P traffic has dominated Internet traffic during the recent years, with a few dominant P2P file sharing networks alone accounting for the bulk of it. P2P cannot replace every client-server system, but it is a reasonable alternative at least for a subset of applications that are run in a client-server environment. P2P networking opens up possibilities for other purposes than file sharing as well, of which an example is the world-wide P2P Voice over IP (VoIP) network Skype. Skype has become a rival for traditional telecom operators, and it has shown that P2P networking enables the operation of large-scale telecom business models without the need for large dedicated centralized systems.

Using the P2P approach, Skype exploits users' computer resources to maintain the overlay structure and to route calls in the Skype network. This cost-effective P2P approach has been an important factor facilitating the profitable provision of free Skype-to-Skype Internet calls and messaging, but also a rich variety of other communication services to millions of customers. Making this kind of global system profitable without P2P networking would be very challenging, because running such a system only with servers would incur much more expenses than could be covered with the current earning principles of Skype. In addition to Skype, there are many other similar proprietary networks, but they are not mutually interoperable.

While the P2P environment in the Internet has evolved, so has the ordinary operator-based telecommunication environment. Traditional unintelligent mobile and landline phone usage has changed over to using more intelligent end-points also for purposes other than regular phone calls. Intelligent end-points include devices such as

smartphones (i.e. a full-featured mobile phone with personal computer-like functionality), VoIP phones and softphones (i.e. computer phone programs). Furthermore, the evolution of voice trunking is moving increasingly from traditional circuit-switched networks to digital packet-switched networks and the number of IP-based telephony networks (that use packet switching) is growing [Mohanty05]. Thus, e.g. the dominance of the traditional land-line telephony technology in operator networks is diminishing. The intelligence of the end-points can be exploited to push the intelligence from the network to the terminals. This supports the convergence of telecom operated personal communication environment with the Internet environment, where the intelligence lies mainly at the end-points. Skype and other Internet-based telecom services are widely used in PCs and currently they are also barging into mobile devices. The current smartphones are quite intelligent and they have many capabilities that are actually closer to those of PCs. Smartphones are already capable enough e.g. to access the open Internet and to process operations required to access Skype and other such networks.

SIP (Session Initiation Protocol) is a standardized protocol for multimedia communications, such as VoIP, and it has been widely used for a long time. However, SIP is based on using servers as central points and therefore requires an infrastructure of SIP servers to implement VoIP networks. The P2P approach is now also being applied to SIP in order to have an open and standardized protocol to the communication environment dominated by Skype and others in the Internet. This system being developed is called Peer-to-Peer SIP (P2PSIP). Because it is a standardized and open protocol, it will allow a more versatile range of services to emerge. Experience has shown that standardized and open technologies and protocols (such as IP used as the main protocol in the Internet) enable better and faster development of services.

1.1 Problem Statement

The preconditions for using P2P for personal communications more generally are already in place. Recent mobile phones are becoming more advanced and the applicability of P2P for even more sophisticated personal communication needs is evolving. The general nature of user communication is person-to-person, so leveraging P2P networking for personal communication appears to be a very logical approach.

As P2PSIP-based networks (both commercial and private) are likely to emerge in forthcoming years, their existence might also be regarded as a threat to traditional telecom operators. P2PSIP and other services available in the Internet challenge the existing earning principles of telecom operators. Telecom operators are challenged to adapt to the upcoming changes and add more value to their service portfolio in order to preserve their revenues. The role of network intelligence is diminishing, as smartphones are able to use multiple access technologies (e.g. Wi-Fi in addition to 2G/3G) and run third party communication clients. Terminal providers have a big role in driving the evolution from closed mobile telecom environments to more open environments by providing smartphones that are less dependent on telecom operators. P2PSIP makes it potentially even more challenging for telecom operators to preserve their earnings from traditional billing of voice communications in the future. Operators may try to hinder the evolution, as has been claimed that Orange and Vodafone are doing, when they disabled Internet VoIP of the Nokia N95 phone they sell to their customers [ITWeek]. This, however, is not the only way to react to new technologies that may threaten operators business.

P2PSIP is being developed for general benefit and not primarily for commercial purposes. Therefore, its applicability for telecom operators is not a concern for the developers. However, instead of merely providing the data pipe (or impeding P2PSIP traffic), telecom operators (and especially mobile operators) could potentially benefit from P2PSIP in many ways, possibly even by using it in their own network infrastructure. Nonetheless, P2PSIP is not intended to be a replacement for existing infrastructural telephony systems. In any case, the operators should decide how to react to P2PSIP and what is the business rationale behind their reaction, even if they should choose to ignore it. It is not obvious what the right strategy is for any given operator, as P2PSIP poses at the same time both a potential external threat as well as an opportunity for them. Furthermore, the exploitation of P2PSIP in providing operator services may present challenges. There are potential conflicts with existing services and network infrastructures that must be avoided.

The characteristics of P2PSIP must be understood not only in order to be able to identify the prospects for a mobile telecom operator, but also to evaluate the systems' impacts and potential threats it presents. The adoption and the extent of P2PSIP usage depend on many aspects, such as how well the P2PSIP will function and what is the status quo of

telecom services when the P2PSIP standard has been developed. For example, Skype, operator-run IMS and other systems may have gained such a dominant position that using another similar new technology (e.g. P2PSIP) can no longer be justified. However, even in that case, P2PSIP would be desirable e.g. for networks without outside involvement, including company networks.

1.2 Objectives and Scope of the Thesis

In this thesis, we try to understand the potential of the forthcoming P2PSIP by describing its characteristics and identifying how it could fit into the service portfolio of a traditional mobile operator. While traditional national telecom operators have become mobile operators, they still carry the baggage of heavy infrastructure. Therefore, the impact of P2PSIP on them would be more severe than for a more modern virtual operator (possibly with no own infrastructure). In addition to mobile operators, telecom operators in general are also considered. Background information related to P2PSIP will be covered by introducing primarily the components of P2PSIP (P2P networking and SIP), but also other matters related to P2PSIP. The actual P2PSIP is presented mainly with a relatively general focus, but some specific draft details are also used in order to better demonstrate the general functioning of P2PSIP.

Interworking of P2PSIP with the conventional SIP is of general importance, and it will be examined using the current P2PSIP interworking drafts. Also interworking between heterogeneous P2PSIP overlays is discussed. However, for telecom operator purposes, other interworking cases that are not included in the drafts are also important. These cases include interworking with the operator-run networks, such as the networks used for land-line and mobile telephones, but also the IP Multimedia Subsystem (IMS). These cases are identified, and even though they are not covered in the current P2PSIP drafts, they are feasible (due to the open and standard nature of P2PSIP).

Possible roles to play for mobile operators are presented mainly by identifying and analyzing preliminarily the possible roles that mobile operators may consider in P2PSIP networking. In addition, impacts of P2PSIP for operators will be included to some extent, as the type of a telecom operator significantly affects the extent to which P2PSIP solutions would be applicable to them.

1.3 Means and Methodology

Because the area of research is relatively new and no standards exist (and therefore no standard implementations are available) of the P2PSIP to be examined, this thesis consists of a literature study and theoretical analysis. The literature study is based on Internet Engineering Task Force (IETF) Drafts, RFCs, Internet publications and conference articles. Drafts are mainly used to describe the technical details of the P2PSIP protocol. As many incomplete standards (i.e. drafts) are used, changes are possible as the work continues. Therefore, minor details are avoided as far as possible, as they are less stable during the development than the general details. Theoretical analysis is used to explore the prospects and benefits of the P2PSIP protocol for mobile operator environment.

1.4 Outline of the Thesis

The thesis is organized as follows. In Chapter 2 we give a technical background related to P2PSIP. This helps the reader to understand the elements of the P2PSIP protocol, namely the P2P concept and the SIP standard, and their current applications. Systems such as IP Multimedia Subsystem (IMS) are also introduced in Chapter 2, mainly for interworking purposes with P2PSIP. In addition, related networks and forms of real-time communication are presented shortly.

In Chapter 3 we describe the actual P2PSIP protocol. We present the P2PSIP architecture and its functionality, but also other matters, such as NAT traversal and security issues. Possible use cases for P2PSIP are also identified.

In Chapter 4 we discuss interworking cases that are included in P2PSIP: interworking with conventional SIP networks as well as other interworking cases for P2PSIP that could be implemented, but are not included (at least initially) in P2PSIP. One such case is interworking with IMS networks.

In Chapter 5 we move to mobile operator-specific aspects of P2PSIP. We identify the prospects of P2PSIP mainly for a mobile operator environment and what could be the possible roles of a mobile operator in P2PSIP networking.

Finally, in Chapter 6 we conclude with the main findings of the thesis.

2 Technical Background

In this chapter we go through the concepts and protocols that are essential background information to comprehend the concept of Peer-to-Peer SIP (P2PSIP). Most weight will be on the SIP protocol and on the concept of peer-to-peer networking. Other related concepts (e.g. IMS) are also presented. IMS is presented before the P2P and SIP concepts in order to better understand the comparison that is made between IMS and SIP.

2.1 IP Multimedia Subsystem (IMS)

The IP Multimedia Subsystem (IMS) has been developed for telecom operators to provide mobile and fixed multimedia services within the same network. The main purpose of IMS is to merge the Internet and the cellular world together (i.e. to provide ubiquitous 3G cellular access to all the Internet services). However, for telecom operators the big benefit of IMS is to have control over users and make charging easier. Telecom operators and vendors have put much effort into developing IMS and therefore they are eager to implement it, but the current business cases do not appear to imply there being big financial benefits in implementing the IMS.

According to [Camarillo04], the motivation (for operators) to use IMS is threefold: QoS (Quality of Service), charging and the integration of different services. Internet services are also accessible through the 3G packet-switched (PS) domain (for data, but without QoS). Thereby, the quality of a connection may vary dramatically during e.g. a VoIP call. IMS provides an adequate level of QoS for real time multimedia sessions. As regards charging, the advantage is the feasibility to charge the users according to the type of session. Thereby, e.g. web surfing can be charged differently from a video session, which usually generates much larger amounts of data traffic than regular web surfing. Integration of different services enables the operators to take the advantage of having multi-vendor service creation industry. The standard interfaces (not introduced, but can be found in the 3GPP specification [TS23.002]) of the IMS allows for a wider variety of interoperable services to be provided, as already existing services can be provided with third-party developed new services. Also, IMS uses Internet protocols, which makes the IMS interoperable with many systems, most importantly the Internet. Interworking and roaming between two IMS of different telecom operators is also possible (this will be discussed in Section 2.1.4). This is not the case with current 3G PS domain, which is a closed system with its own protocols. The decision to use SIP in the IMS is based mostly

on the fact that SIP makes it easy to create new services. However, signalling in IMS does not consist only of SIP signalling, but also of e.g. DIAMETER (for authentication etc.) and H.248 (for controlling between MGW and MGCF). Nonetheless, SIP is the major protocol used in IMS and IMS uses the 3GPP version of SIP (3GPP SIP will be described in Section 2.2.2). [Camarillo04]

IMS was intended to be the first step to transfer voice over IP. However, 2G/3G networks today can carry voice over IP (without IMS). In general, carrying voice over IP in the network would be more cost effective for telecom operators, as the network traffic can be multiplexed to a shared link. Carrying voice over IP does not require fixed amount of bandwidth (and other network resources) to be allocated for every call (as is the case in a circuit-switched network).

2.1.1 Basic Entities in IMS

This section defines the basic entities in IMS as per [Camarillo04].

Usually the SIP servers in IMS are stateful in order to achieve the control and billing of the sessions. Here we present the most essential entities used in the IMS. Actually, the entities are called functions, as these functions are not node-dependent. There are many other functions, and each connection between the functions has a dedicated interface. The following functions are also shown in Figure 1, when the IMS architecture is discussed.

The **CSCF** (Call/Session Control Function) is a SIP server and it is an essential node in IMS. There are three different CSCFs that all have their specific functionality.

The **P-CSCF** (Proxy-CSCF) is an inbound/outbound SIP proxy server for an IMS terminal. For an IMS terminal, it is the first point of contact to the IMS network. The P-CSCF authenticates the IMS terminal, so that the IMS terminal does not need to authenticate with any other IMS entities, as the P-CSCF asserts its identity. The P-CSCF is also involved in charging, QoS management and SIP message compression and decompression.

The **I-CSCF** (Interrogating-CSCF) is a SIP proxy at the edge of an administrative domain. When a SIP server follows SIP procedures (as per [RFC 3263]) to route a particular message, it obtains the address of an I-CSCF of the destination domain. The I-CSCF has a DNS name and it is used to route SIP messages destined to the domain it

belongs to from another domain. The I-CSCF routes the incoming SIP messages typically to corresponding S-CSCF. The I-CSCF is also involved in charging.

The **S-CSCF** (Serving-CSCF) is the central node in the IMS architecture for signalling. All the SIP signalling related to a terminal traverses the allocated S-CSCF. The S-CSCF performs session control (maintains also session states) and acts as a SIP registrar (i.e. maintains a binding between the location of a terminal and its SIP address of record). Another essential function of the S-CSCF is to provide SIP routing services (such as ENUM translation, if needed). Naturally, also S-CSCF is involved in charging.

An **AS** (Application server) is a SIP entity that hosts and executes services. Depending of the actual service, ASs can operate in different modes. These modes are the SIP proxy mode, the SIP UA mode and the SIP B2BUA (Back-to-Back User Agent) mode. A B2BUA is just two SIP UAs connected by some application-specific logic in a same AS. B2BUA is similar to a SIP Proxy, as it also receives and sends requests and responses. However, their biggest differences are related to the actions that they are allowed to perform. A B2BUA is allowed to modify headers, methods and SDP fields of the messages, unlike the SIP Proxy. Because a SIP B2BUA is a collection of SIP UAs, B2BUAs need to understand all the SIP methods, extensions etc. that normally only the corresponding UAs need to understand.

PSTN/CS Gateway

The PSTN gateway enables interworking with conventional circuit-switched (CS) networks. This interworking enables calls to be made between IMS terminals and terminals in PSTN networks. The PSTN gateway is decomposed into following functions:

SGW (Signalling gateway): the SGW does the control signalling conversions needed for interworking between the PS and CS domains (with SIP and ISUP, respectively). ISUP is used to setup, manage and release trunk circuits in the PSTN (therefore corresponds to SIP).

MGW (Media Gateway): the MGW does the required media conversions needed for interworking.

MGCF (Media Gateway Control Function): the MGCF is the central node of the PSTN/CS gateway that controls the SGW and MGW functions.

BGCF is related to the PSTN/CS gateway, as it chooses the appropriate PSTN/CS gateway (or network, if the interworking is to happen in another network).

HSS/SLF

HSS (Home Subscriber Server) is a database that maintains subscriber-related information of users. The SLF (Subscriber Location function) is used to find the correct HSS, if there is more than one of them in the network.

There are also other entities in the IMS architecture, such as MRF (Media Resource Function) for media mixing, transcoding etc., but we are focusing here only on the essential functions related to the IMS architecture.

2.1.2 IMS Architecture

The IMS architecture is based on (node independent) functions and interfaces between them. IMS implementation may combine two functions into a single node, or a single function can be split into two or more nodes. The functions presented in the previous section are presented in Figure 1. Connections between the functions in the figure are for signalling. Media path is usually routed directly between corresponding nodes.

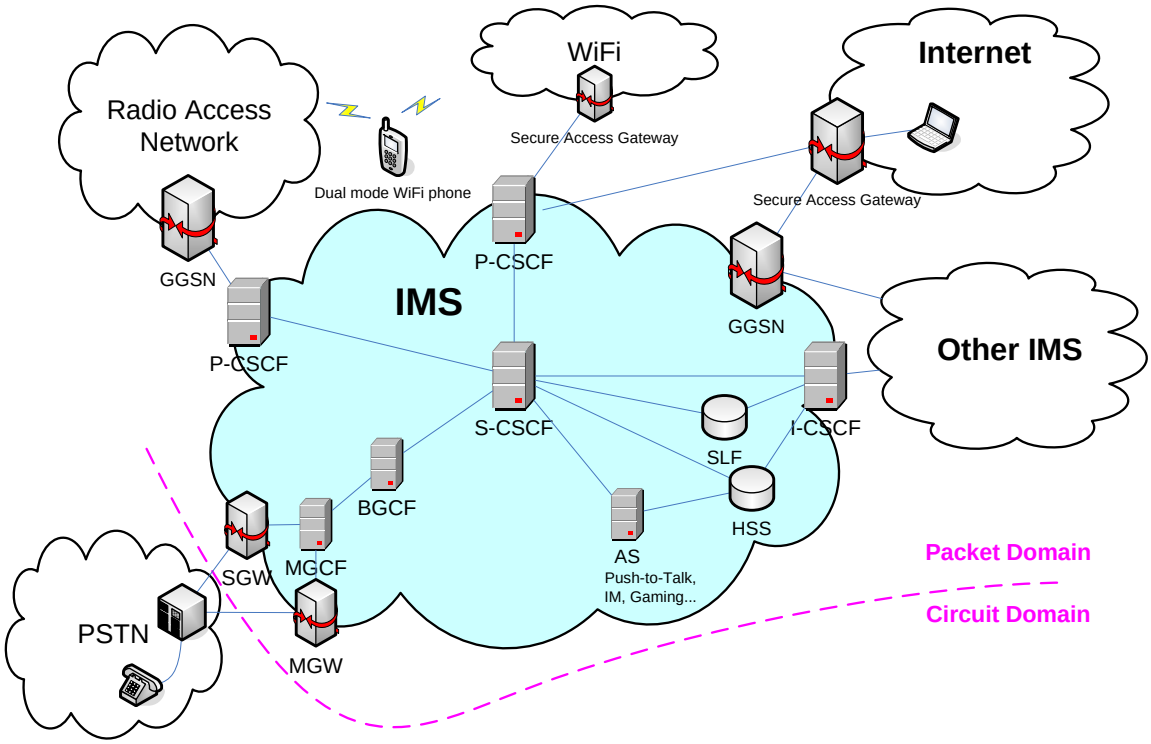

Figure 1 – General 3GPP IMS Architecture Overview [TS23.002]

2.1.3 Identification of Users in IMS

As in the PSTN, in the IMS, a user has a unique identity in order to identify the user. An IMS user is allocated with one or multiple Public User Identity. This identity (or identities) is used to route SIP messages for the user. This identity can be a SIP URI (Uniform Resource Identifier), such as sip:first.last@operator.com (defined in [RFC3261]), or a TEL URL, such as tel:+1-212-555-0293 (defined in [RFC2806]). An IMS user also has a Private User Identity (or multiple, as in 3GPP Rel6 [TS23.228]), but it is used exclusively for subscription identification and authentication purposes (like the IMSI in GSM). Having multiple Public User Identities enables to differentiate personal (e.g. private) and business identities of a user or to trigger a different set of services.

2.1.4 IMS Roaming and Interworking

It is important to have IMS networks that can be interoperable. Interoperability can be handled either using IMS roaming (Figure 2 and Figure 3) or IMS interworking (Figure 4). IMS roaming is comparable to normal GPRS roaming, where the IMS traffic is transferred in a GTP tunnel, as any other data. Thereby, IMS roaming is used to access the home IMS network from another network. In the roaming case, the visited network does not need to be IMS capable, as a GTP tunnel is used to access the home IMS network. The GTP tunnel is used across the inter-operator backbone network (which is usually GRX, see 2.1.5 for more details of GRX). Adequate QoS cannot be guaranteed in IMS roaming with GRX, as the GTP traffic is transferred by the QoS calls of "best effort". This may cause delay and/or varying throughput. However, this issue is given attention in the development of GRX in order to enable the use of QoS in GRX networks (i.e. using IPX in GRX networks).

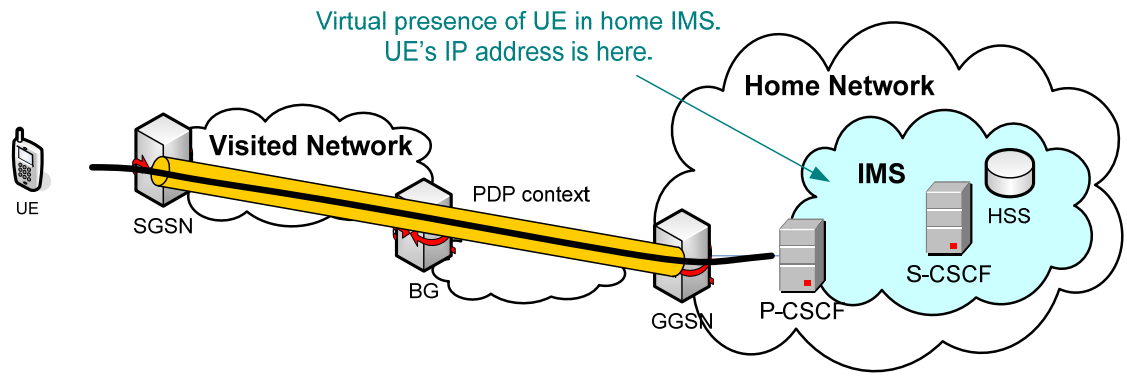

Figure 2 - IMS Roaming from Visited Network (GGSN in Home Network) [IR65]

Figure 2 depicts the usual scenario of IMS roaming (simplified), where the GGSN is located in the home network. This enables more comprehensive control for the home operator. As operators want to have adequate control over their subscribers, they tend to prefer this scenario. However, the scenario of Figure 3 (also simplified), where the GGSN is located in the visited network, would be preferable later on. This is because when the level of real-time traffic increases, improved QoS control and optimized routing will be more important. [IR65]

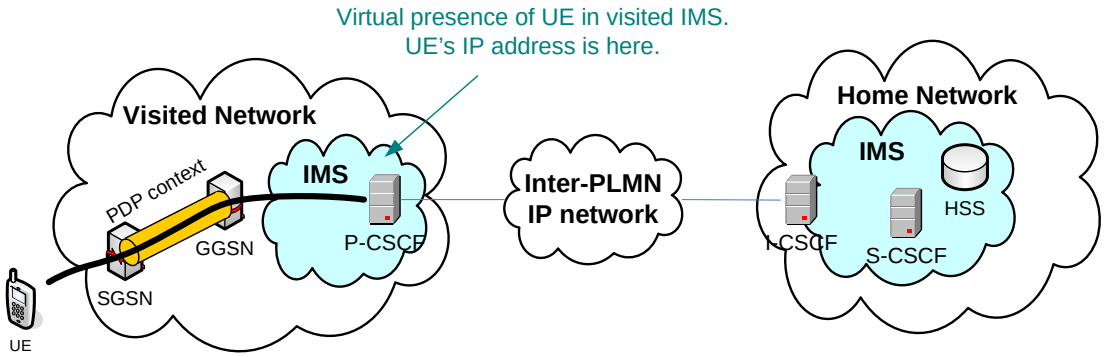

Figure 3 - IMS Roaming from Visited Network (GGSN in Visited Network) [IR65]

IMS interworking means that SIP control (i.e. signalling) and transport (i.e. data) communication is enabled between two different IMS networks through an inter-PLMN IP network. With IMS interworking, an IMS user can connect with another IMS user of another IMS capable network. Figure 4 illustrates a typical IMS interworking scenario between two different IMS networks. SIP signalling goes through the IMS network, but the media session is routed directly between the User Equipments (UEs) using the PS networks (signalling will be depicted later in Figure 9b). [IR65]

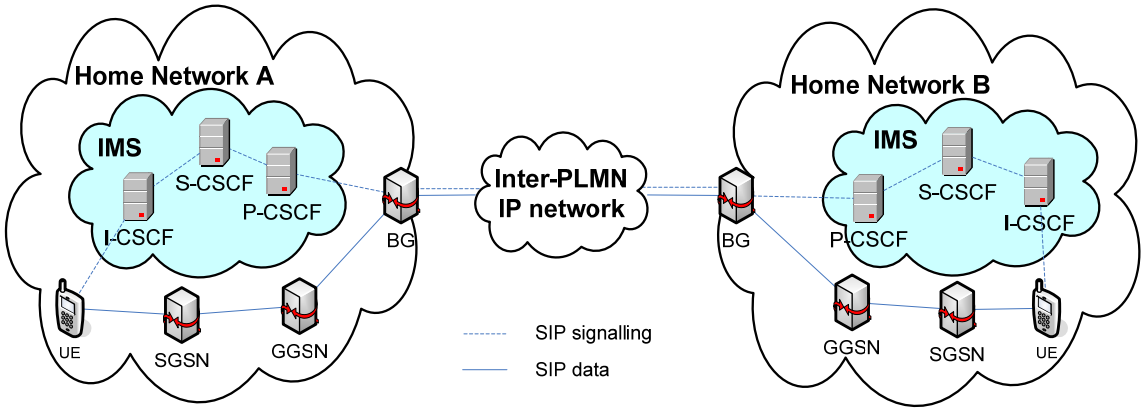

Figure 4 - IMS Interworking Between Two Different IMS Operators [IR65]

2.1.5 Other IMS Networks

There are other networks that are partly based on the IMS specifications.

- **DOCSIS (by CableLabs)**

Data Over Cable Service Interface Specification (DOCSIS) is an international cable modem standard developed by CableLabs and contributing companies. DOCSIS defines the communications and operation support interface requirements for a data over cable system. E.g. Welho, the biggest cable television company in Finland, uses DOCSIS 1.1.

CableLabs has adopted the signalling core of the IMS specifications for PacketCable. PacketCable specifies interoperable interface specifications for delivering advanced, real-time, interactive multimedia services over DOCSIS access networks. [Cablelabs]

- **TISPAN**

The **Telecoms & Internet converged Services & Protocols for Advanced Network (TISPAN)** is a standardization body of ETSI, specializing in fixed networks and Internet convergence. The focus of TISPAN is to define the European view of the Next Generation Networking (NGN), although TISPAN also includes much participation from regions outside Europe. TISPAN has adopted the IMS architecture given in release 6. Therefore, SIP has an important role also in TISPAN. TISPAN and 3GPP are now working together to define a harmonized IMS-centric scope for both wireline and wireless networks. [Tispan.org]

2.1.6 GRX & IPX

In this section we present the networks that are used in an operator environment for interworking between different operators. In the P2PSIP context, GRX/IPX is involved when a P2PSIP user is communicating with a user or service in another operator network, but also when a P2PSIP call is being made using a foreign 2G/3G network. In the latter case, the packets of the session are transferred over a GRX network as any other data packets in an inter-operator data transfer. Interworking aspects for P2PSIP are discussed further in Chapters 4 and 5.

The **GPRS Roaming Exchange (GRX)** is an inter-operator backbone network commonly used for interworking between GSM operators. Therefore, non-GSM operators cannot participate in the GRX. While the GRX is only recommended (but not required) by GSMA to be used for interworking, using other than GRX (i.e. private

point-to-point IP connections) is in practice very difficult, because the inter-operator backbone networks have their own DNS root servers. Private point-to-point IP connections (without GRX or IPX) are used e.g. in the core network of TeliaSonera between the Nordic countries. Another reason for the obligation to use GRX for interworking is that GRX routes are not allowed to be advertised outside the GRX networks. As the MNOs are connected to the GRX environment, it is logical for them to use it for roaming and interworking between other MNOs. GRX supports GSM, 3G (and 2.5G) and WLAN (authentication) data roaming traffic between GSM mobile network operators (MNOs). Simple QoS can be used with GRX for GPRS roaming (i.e. GTP), but IPX (which is evolved from GRX) is needed for more sophisticated QoS (with different QoS classes) in roaming and interworking cases. These cases can be such as IMS VoIP or video sharing between two different IMS domains. The peering point of the Amsterdam Internet Exchange (AMS-IX) is used (however, not required to be used) to connect the GRX carriers that provide the GRX connectivity for MNOs. There are dozens of GRX providers today that are connected to the AMS-IX. Hundreds of operators are connected to these GRX providers. Figure 5 illustrates a simplified structure of the physical GRX architecture. [AMSIX07] [Davies06]

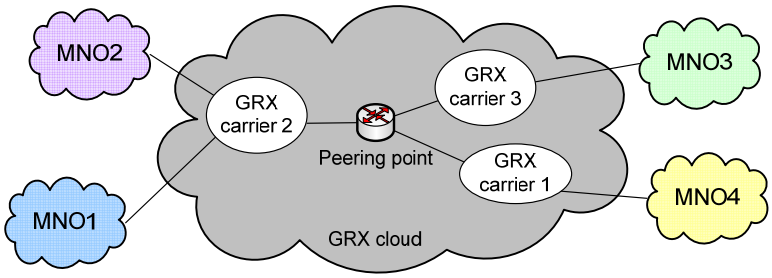

Figure 5 - GRX Physical Architecture

The **IP Packet Exchange (IPX)** is a global IP backbone for IP service interworking and roaming (for any access technology roaming, such as WiMAX). IPX is simply an evolved version of GRX and it provides the same base functionalities as GRX, but adds many important functions. Examples of these additions include QoS and interworking between different communities of operators and service providers (see Figure 6). The concepts of IPX have been built upon the models and concepts of GRX, and existing GRX routing domains can be used for IPX. Like GRX, IPX is a closed inter-operator backbone network to provide connectivity among operators. However, GRX is only for MNOs, while IPX enables also other operators and service providers to use the network. Otherwise, the IPX architecture is similar to that of GRX (Figure 5).

Future IMS traffic between different operators could be transmitted using IPX. Figure 6, where a GRX domain is used for IPX, illustrates this. In this scheme, the existing GRX networks could be exploited by using GRX for routing and connectivity, and IPX to offer services such as proxy and agreements. An IPX proxy is a SIP proxy with additional functionality for fulfilling the requirements of mobile operators. An IPX proxy is transparent for the IMS terminal and the core system. With an IPX proxy, it is possible to run any SIP-based service via IPX. The advantage of using IPX proxies is that an operator needs to know only the IPX (SIP) proxy in order to route SIP messages to any terminal outside its own domain. [TeliaSonera06]

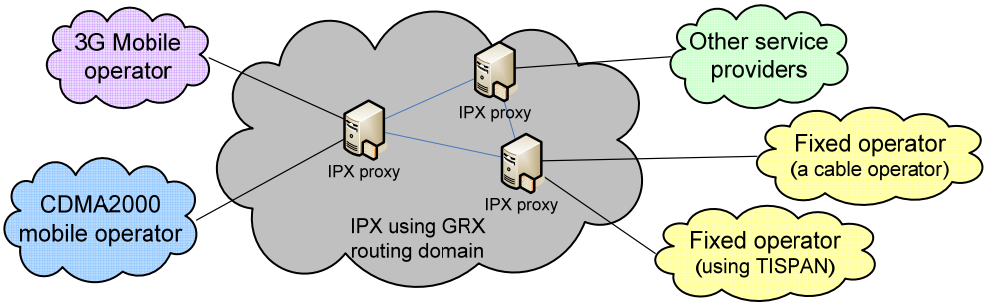

Figure 6 - Future Architecture of SIP Interconnection Between Different Operators via IPX

IMS interworking with P2PSIP is discussed in Section 4.2. In order to better understand IMS and its possible interworking with P2PSIP, familiarity with the SIP is necessary. In the following section we will describe the conventional SIP and the 3GPP SIP used in IMS.

2.2 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) is a standardized protocol (by the IETF) to establish, modify and terminate multimedia sessions. A multimedia session can be an audio call, a video conference, Instant Messaging (IM), shared whiteboard or a gaming session. The presence feature (i.e. to show an online status of a user, e.g. “away” or “online”) can also be used in SIP. Regardless of the session, SIP is not dependent of the type of the multimedia session (e.g. codecs used). Also, the mechanism used to describe the session does not make a difference for SIP. SIP is only a signalling protocol used to distribute session descriptions among potential participants. After successful session establishment, SIP can be used to modify the session, and finally to terminate the session. SIP supports five facets for session control. Using SIP, a user can be located (1), and its availability and willingness can be discovered (2). Also, user capabilities (i.e. supported media parameters) can be determined (3). After these three phases, the session can be set

up (4), but also managed (5) later (i.e. modified or terminated). The discovery of a user's location provides mobility by enabling users to be reached regardless of their network location. [RFC3261] [Camarillo02]

Conventional CS telephony network has used intelligent networks and simple and dumb endpoints. Unlike in CS telephony network, SIP assumes intelligent endpoints and dumb network. SIP is an end-to-end protocol like IP, and routers in underlying IP network just route the IP packets. SIP servers, which can be used to route SIP requests, do not need to process session descriptions of SIP requests. Only few SIP headers of the message are needed by the SIP server for basic SIP message routing. Therefore, SIP servers can be minimally stateless without session state storing. Stateful SIP servers can also be used, if session states need to be known (e.g. in calculating session durations or in helping to contact a user from various locations) [Camarillo02].

SIP is designed to be interoperable so that any implementation of the core protocol is interoperable with any other implementation. When two (or many) parties are about to establish a session, one party can propose an extension. If this extension is not supported by some party involved, a SIP negotiation ensures that a fall back to a "rudimentary" SIP session can be done. [Camarillo02]

2.2.1 Conventional SIP Architecture

Conventional SIP (i.e. IETF SIP) uses a client-server architecture, where there are separate servers for user registrations etc. The SIP architecture consists of SIP entities that are described in Section 2.2.1.1.

Figure 7 shows a typical SIP configuration, referred to as "SIP trapezoid". This configuration has two different SIP domains with SIP proxies at the borders of the domains. Also, exemplary SIP addresses for the two SIP phones are shown in Figure 7.

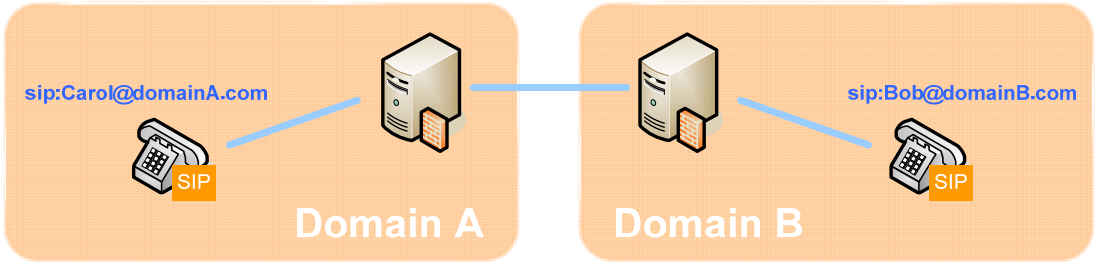

Figure 7 - The SIP trapezoid

2.2.1.1 SIP Entities

We present here the main SIP entities of the conventional SIP architecture. These enable users to communicate with each other (and with services such as a voice mail). Servers have an important and essential role in facilitating the communication for users. The distinction of SIP server roles is logical and not physical. Therefore, e.g. a registrar server can be co-located with a proxy server.

User Agent

A user agent (UA) is the SIP entity that interacts with the end user. The user interacts with the UA using an interface, often a program window with a selection of buttons (i.e. soft phone or similar). UA does not necessarily need user interaction, but can be configured to automatically respond or forward invitations on the user's behalf. [Camarillo02]

Redirect Server

A redirect server helps in locating SIP UAs by providing alternative locations where the user can be reachable. A Redirect server does not issue any SIP requests of its own. After receiving a request (other than CANCEL), it either refuses the request or gathers the list of alternative locations from the location service and returns a final response of class 3xx (these number codes are presented in the next section) [RFC 3261]. A Redirect server can be configured to implement group addresses. This functionality can be used to return a different location (e.g. different person on duty) for some address depending on the time. [Camarillo02]

Proxy Server

The proxy server helps in locating a user, so a UA has to try only one location, when there is a proxy server in the path between UAs. The Proxy server usually handles incoming invitations for a domain it serves. [Camarillo02]

Registrar Server

The registrar server accepts SIP registrations and stores these associations (also called bindings) into the location server. A registrar for a domain is usually co-located with a proxy server of that domain. [RFC 3261]

Location Server

The location server stores and returns the possible locations of users. Registrars upload the user location information to the location server, where are then located the most current locations of registered users. Proxy and redirect servers consult location servers to find the locations of users. SIP does not specify how to interact with a location server. Therefore, some other protocol (such as LDAP) is used instead. [Camarillo02]

2.2.1.2 SIP Messages

SIP implementation uses request/response signalling model and is text based. In these aspects, SIP is similar to HTTP. The format for encoding protocol messages is also very similar between SIP and HTTP. SIP messages are exchanged in order to establish (and terminate) a session. The exchange of a set of messages between two UAs is referred to as a SIP dialog. [Camarillo02]

There are six types of **SIP requests** defined in the core specification of SIP to be used for SIP dialogs. These request types are:

- **REGISTER** (used by users to inform a registrar about their current location)
- **INVITE** (request used to invite users to participate in a session)
- **ACK** (acknowledges the reception of a final response to an INVITE)
- **BYE** (used to terminate a session and the dialog associated with it)
- **OPTIONS** (used to query capabilities of another UA or a proxy server)
- **CANCEL** (to cancel a pending session establishment before final response)

Every SIP request contains a *method* field that denotes its purpose. [Camarillo02]

SIP Response messages: A server issues one or several responses upon the reception of a request. A response has a status code (100-199 provisional, and 200-699 final responses) and a reason phrase. Examples of SIP response messages are “180 Ringing”, “200 OK”, “Redirect 302” and “404 Not Found”. [Camarillo02]

The most common (there are more than the ones listed above) SIP messages to establish (and terminate) a session can be seen in Figure 9a along with the 3GPP signalling. Their mutual difference is discussed in Section 2.2.3.

2.2.1.3 SIP Session Setup

In general, before a session can be set up, the users have to be registered with a registrar. In conventional SIP, a user registers its UA with the registrar server in order to be

reachable. [RFC 3263] describes how to locate SIP servers (However, UAs can also be contacted directly). According to [RFC3263], SIP uses DNS procedures to enable a client to resolve a SIP URI address (e.g. sip:bob@example.com) into an actual network location. This network location is an IP address, port and transport protocol of the next hop contact (in this case a server or an UA).

Figure 8 depicts an (simplified) example of registration process, where one UA ("Alice") is already registered and another ("Carol") registers with the same domain (sip.org). Also the signalling to send an INVITE message to another UA is shown. The registration procedure of UA is defined in [RFC3261]. The procedures of Figure 8 go as follows:

Carol sends a REGISTER SIP message (1) to the registrar server. The registration is stored (2) in the location server. After Carol has registered in the sip.org domain, Alice sends an INVITE message (3) in order to contact Carol and to establish a session with her. The location server is consulted (4) to find the location of Carol (they are located in the same domain in this example). The location server responds (5) to the proxy that Carol can be reached at "sip.carol@home.sip.org". After this, the proxy can forward the INVITE message to the Carol (6). Finally, the media session (7) is successfully established. A more specific example of a SIP session establishment is depicted later in Figure 9a.

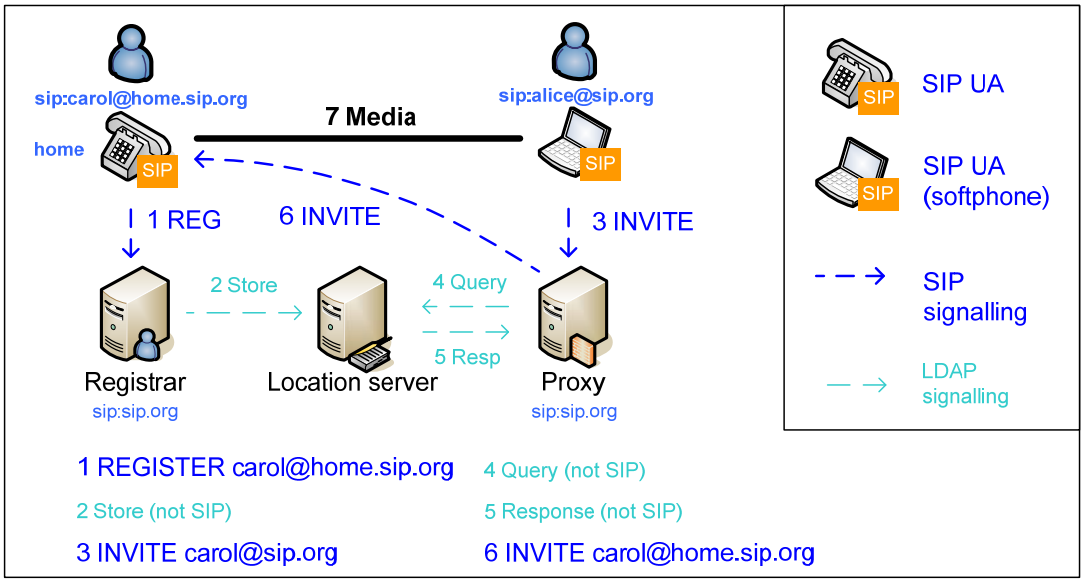

Figure 8 – SIP Registration and Session Invitation Example [RFC3261]

To be able to establish a session, the session has to be described. SIP is not used to describe the session, and therefore it can be used to establish many kinds of sessions (e.g. video or voice call with some specific codec). Normally the Session Description Protocol

(SDP, [RFC 4566]) is used to describe and negotiate needed parameters for a session. Parameters, e.g. for a multimedia session, are the IP address and the port number where the media needs to be sent and the codecs used to encode the voice and video of the participants.

2.2.2 3GPP SIP

SIP has also been adapted to 3GPP IMS, where it is called 3GPP SIP. 3GPP SIP differs from conventional SIP by being modified to better suit 3G networks, which are built the old way (i.e. the conventional telephony way). This property of 3G breaks the IP end-to-end model.

For a reliable session establishment, adequate resources need to be reserved in the network. Without resource reservation, even with successful signalling, the session may fail. Wireless access technology used in 3GPP causes the session establishment to be more demanding due to the environmental constraints (such as scarce and shared bandwidth at the air interface). The 3GPP version of SIP is necessary especially in unpredictable low bandwidth access networks. In general, the signalling should be kept to a minimum within wireless access networks due to these environmental constraints and in order to minimize the latency. However, in order to guarantee the QoS requirements for a SIP session in 3GPP environment, the more in-depth and longer-lasting (compared to the IETF SIP) signalling of 3GPP SIP is needed. Robust Header Compression (ROHC) [RFC 3095] is used to cope with issues such as long round trip times (i.e. latency) and high loss rates of various wireless access technologies. Also Signalling Compression (SigComp) [RFC3320] for SIP (and other) can be used to optimize the performance in 2.5G and 3G networks.

2.2.3 Difference Between Conventional and 3GPP SIP

The 3GPP SIP session establishment procedure is more in-depth than that of conventional IETF SIP in order to cope with the requirements mentioned above. This causes the differences of the IETF and 3GPP SIP versions, which can be seen in Figure 9. The session establishment procedures of the two versions are aligned to emphasize the differences. Therefore, the gaps in Figure 9a do not represent pauses in the signalling. Usually a 3GPP SIP procedure is always longer-lasting than the conventional (and simpler) one. The mechanisms (e.g. for resource reservation) used in the 3GPP SIP may

be used also in regular IP environments, but as they do not have to be used there, they usually are not.

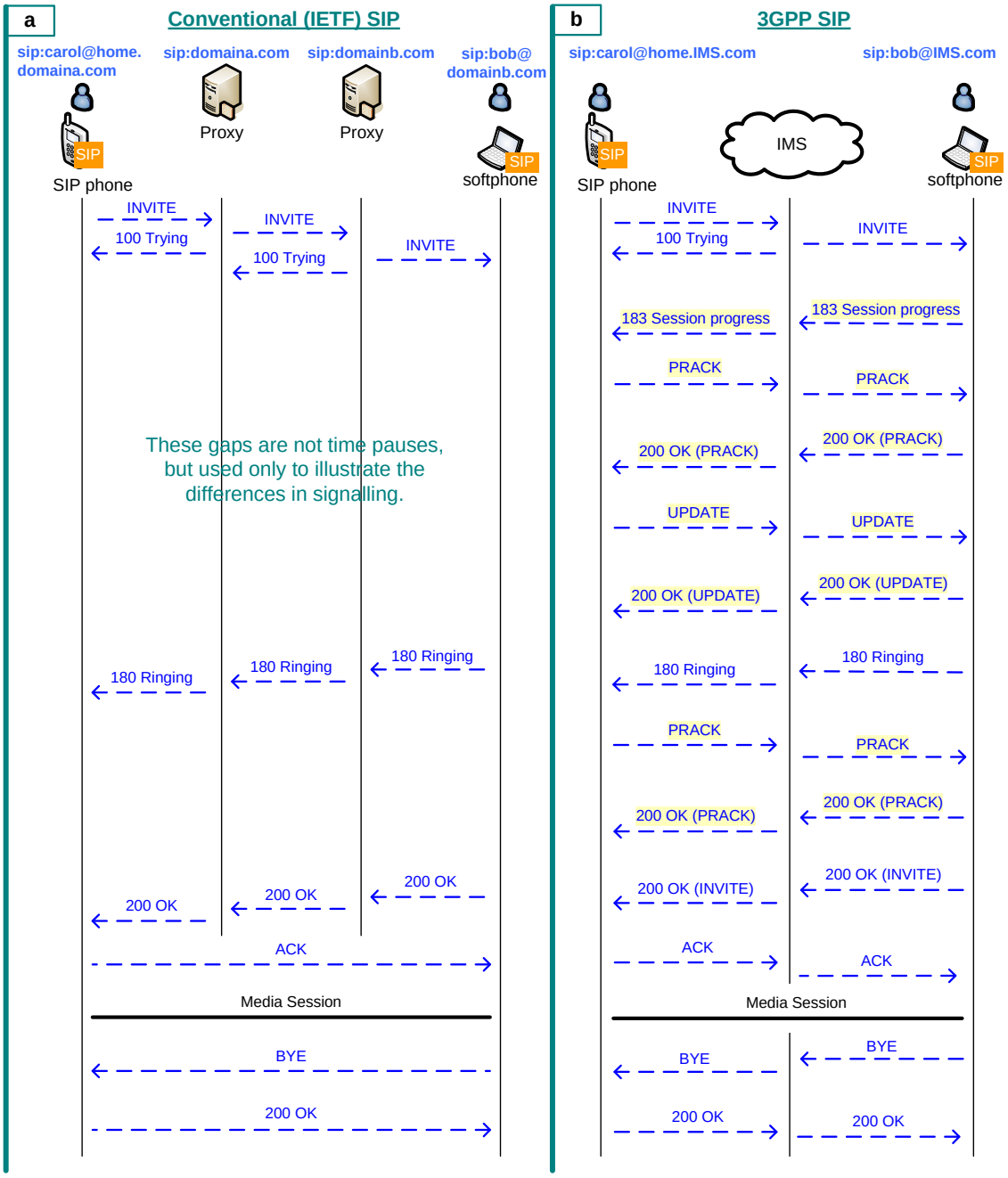

Figure 9 – IETF and 3GPP SIP Session Establishment Signalling [RFC 3261] [TS24.228]

As can be seen in Figure 9b**,** IMS signalling is more in-depth than in conventional SIP. The figure also shows that the last ACK and BYE (and its OK response) are proxied in the 3GPP version (this is possible also in SIP, if wanted to be used). Proxing of messages enables the control of sessions in IMS e.g. for billing purposes. Only the media session is (usually) not relayed, as it could overload the proxies.

Interoperability needs to be taken care of when interworking between 3GPP SIP and the conventional IETF SIP. This can be done in IMS using a specific gateway to handle the conversion between the two implementations of SIP.

2.3 Introduction to Peer-to-Peer Networking

Peer-to-peer (P2P) systems and applications are used in the Internet to share resources (i.e. computing power, data storage and sharing, and bandwidth) between computers. Resources are therefore distributed all over the P2P network. Pure P2P networks do not have any centralized control or organization [IEEEDoval03]. Therefore, they differ fundamentally from the traditional client-server (CS) model (see Figure 10a). Resources are fully decentralized and the nodes have an equal role; no hierarchy or central servers are needed. Nodes in a P2P system (see Figure 10c) are called peers and they function simultaneously as clients and servers. Between these (P2P and CS) models lies the hybrid model (Figure 10b), where a server is used for lookups of resources, but the data is distributed and transferred in a P2P manner. Napster (see Section 2.3.5.1) is an example of a hybrid model.

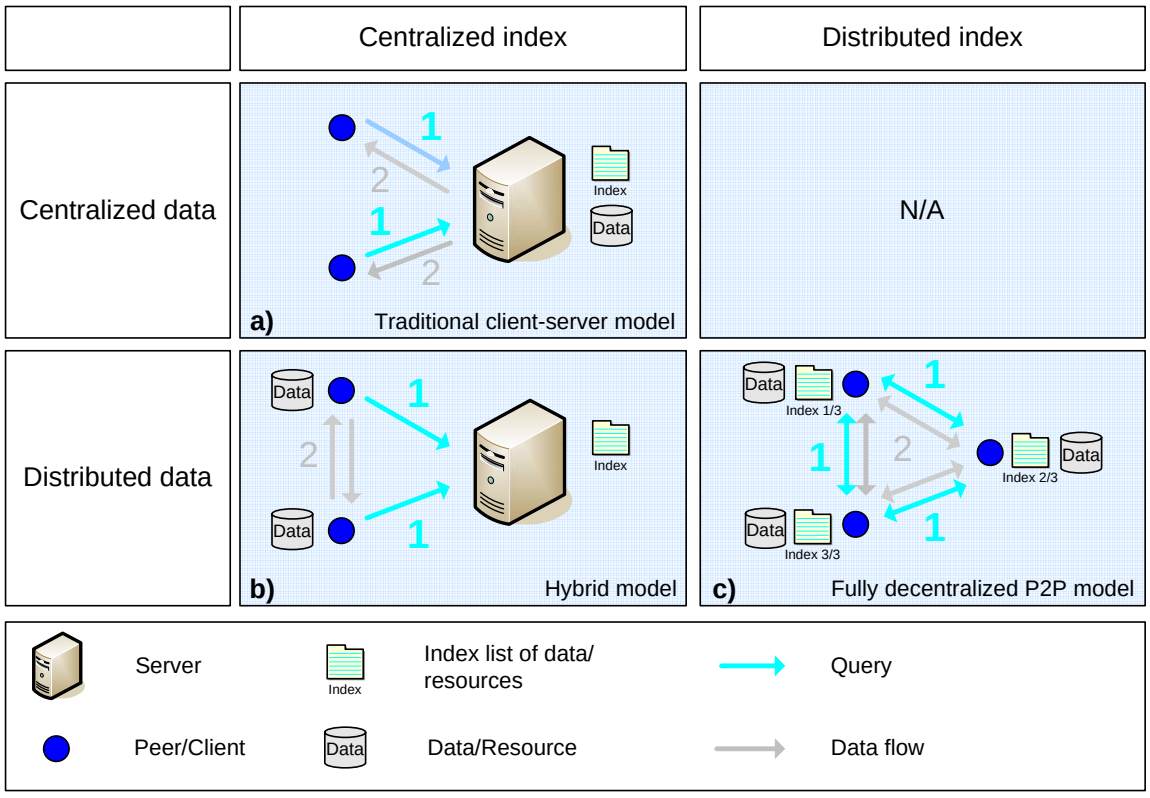

Figure 10- Search Model Comparison [Parameswaran01]

Today many P2P systems are used for file sharing. P2P file sharing networks often involve illegal and copyright-violative sharing of movies, music etc. Some operators

even impede P2P traffic in their network in order to prevent excessive network load that P2P file sharing networks often cause [Mellin04]. Measurements show that as much as 60-80% of network traffic is caused by P2P traffic, while only 30-35% of all subscribers use P2P [CacheLogic06]. BitTorrent, one of the most popular P2P file sharing networks, alone accounted for 30% of all Internet traffic.

BitTorrent and other P2P file sharing networks are just one way to use P2P. P2P networking has also been widely exploited for making voice calls and for instant messaging (IM) over the Internet. Skype [Skype] is a good example of a P2P system that is widely being used in the Internet (Skype will be discussed in more detail in Section 2.4.1). In addition to file sharing and media communication, P2P can also be used e.g. for emergency information flow ([Bahora03]), SPAM detection filtering ([Damiani04]) as well as for sharing computing power (e.g. [SETI@home]).

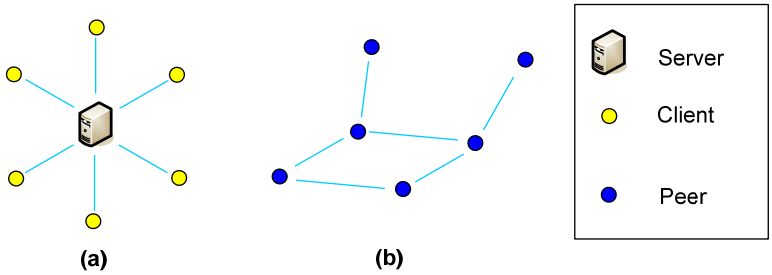

Figure 11 - Client-Server and Peer-to-Peer Topology

Figure 11 shows the difference between the traditional basic (as there may be multiple servers that form a system) star-formed client-server model (a) and the ad-hoc P2P model (b) of a network topology. Participant nodes in a P2P network can be situated all over the world, as long as there are physical links that can be used to interconnect the nodes. In a pure CS model, a resource to be searched is always only one hop (a hop equals a connection between two nodes) away. In a P2P model, a resource to be searched in a P2P overlay network may take one or more hops to be found. Also, as the resources are decentralized and the location information of the resources is distributed, every peer has to participate in other peers' resource lookups. After a resource has been found, usually a direct connection between the two peers can be used. Thereby, peers are usually only helping in resource lookups, but the resource utilization (e.g. file download or a voice call) is made directly between the corresponding peers. A fully decentralized P2P network is very difficult to shut down, as there are no central servers or other entities that the network is dependent of.

In general, P2P networks potentially offer an efficient routing architecture that can be **self-organizing, massively scalable and robust**. They can also provide **good fault-tolerance, load balancing and explicit notion of locality.** [IEEEsurvey04]

2.3.1 Concept of Peer-to-Peer Overlay Networks

Peer-to-Peer (P2P) networks are overlay networks on top of the IP network topology. The topology of an overlay is logical, so the underlying physical topology is usually different from the overlay topology (see Figure 12). Each peer node (i.e. node in the overlay) maintains a set of virtual links to other peers (that become its neighbours), and these links form the overlay network. Every peer knows the location of at least one another node in the P2P overlay. An overlay network is formed by some protocol that uses some specific algorithm to manage the virtual links of the overlay. The protocol also determines the lookup mechanism of the P2P overlay, as the resources have to be found somehow in the absence of a centralized entity. The protocols for network maintenance and search operation can also be separate, like in Gnutella (more of Gnutella in Section 2.3.5.3) [Aberer03].

The absence of a centralized entity also presents the problem of how to join some P2P overlay. The process of finding some node of a P2P overlay is called bootstrapping. There are different ways to locate a bootstrap node, such as multicasting, cached addresses and pre-configuration. These are discussed in more detail in the context of P2PSIP in Section 3.3.2.

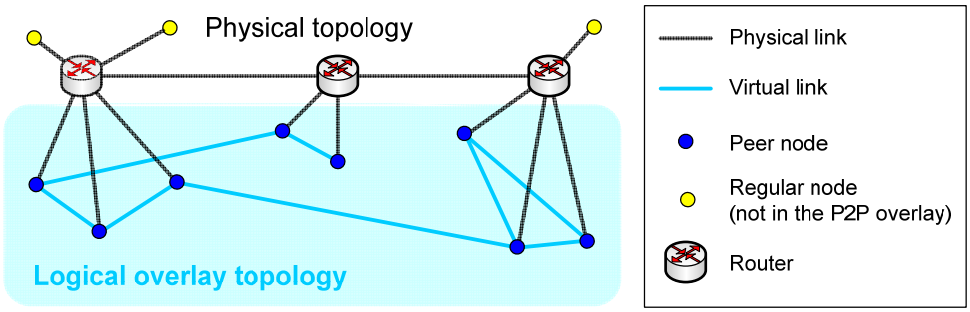

Figure 12 – Overlay Topology vs. Physical Topology

The network architecture of Peer-to-Peer (P2P) overlay is essentially different when compared to the conventional CS architecture. The main goal of P2P overlay networks is to share the resources (such as bandwidth, storage, computation power) of participating peers [p2psip-interwork-01]. Thus, taking advantage of this distributed resource network, the usage of centralized servers can be avoided. However, even though good scalability

(together with other benefits mentioned above) is possible with P2P systems, P2P systems with poor scalability also exist.

There are different lookup mechanisms and they also depend on how their overlay topologies are arranged and managed. There are thus many different ways to implement a P2P overlay network, and many different protocols with their algorithms have been developed for P2P systems. P2P overlay networks can be divided into two subgroups — unstructured and structured overlay networks — depending on how the peers are connected with each other. The fundamental problem of decentralization is resource discovery, e.g. finding a particular node, service or file. This is done differently in unstructured and structured networks. Today, structured overlay networks are more common among the P2P systems. We will present these, along with the characteristics of some of these two subgroups, in more detail after the following section on supernodes.

2.3.2 Supernodes in a Peer-to-Peer Overlay Network

In a basic P2P overlay network, the peers have equal roles and they participate equally in the lookup queries. However, supernodes (i.e. superpeers) can be used together with regular peers. These supernodes are more capable peers and they function as server-like peers causing a hierarchical difference between regular peers and supernodes.

A supernode is a well-known P2P node (i.e. with a static public IP address and a DNS name) that has some guarantee of high availability, computing resources and available networking bandwidth. Accordingly, they can provide more resources for other peers and they are usually more stable than regular peers. This stability (i.e. often available online with the same identifier) can be exploited e.g. for Network Address Translator (NAT) traversal for peers behind NATs (that separate private networks from the public Internet). NAT traversal problem in the context of P2PSIP is described in Section 3.4.

A regular peer (i.e. P2P node) may also become a supernode, if the requirements listed above are fulfilled. Thereby, it does not necessarily need to have a static public IP address or DNS name, if it is otherwise well-known and has sufficient bandwidth capacity. However, these are useful capacities especially if an operator provides supernode functionalities for a network.

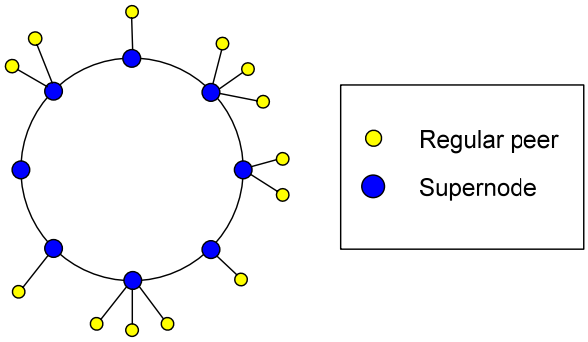

Figure 13- Supernodes Introducing a Hierarchy

The use of supernodes implies a hierarchical structure instead of a flat structure. However, a flat structure can also have supernodes, if the regular peers do not participate in the overlay signalling (and are thereby alike clients). Instead, the supernodes act on behalf of these regular peers in the P2P overlay. In this case, only the supernodes run the P2P algorithm. This would also apply to Figure 13, if the regular peers were merely clients and therefore would not run the P2P algorithm.

In the further context of P2PSIP terminology, we use the term superpeer instead of supernode (for consistency).

2.3.3 Different P2P Overlay Networks

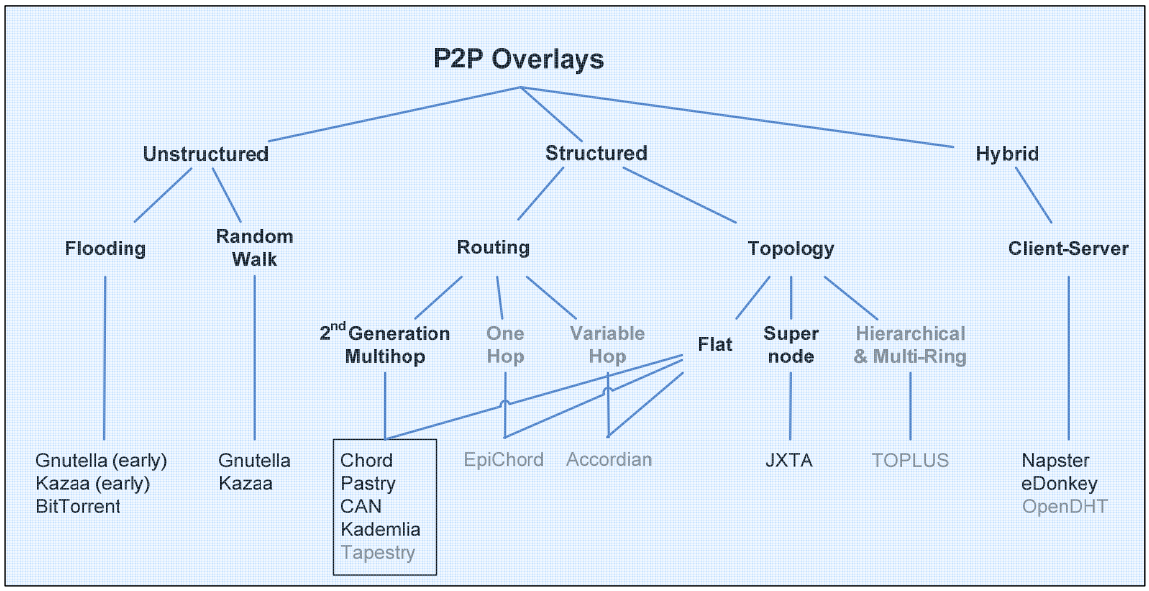

Figure 14 - P2P Overlay Taxonomy [Buford05]

Figure 14 depicts the taxonomy of different P2P overlays. P2P overlays can be divided into unstructured and structured overlays, but P2P overlays based on a hybrid structure also exist. The hybrid structure was described in Section 2.3 and was shown in Figure 10b. Unstructured P2P overlays are divided into two categories: ones with a flooding-

based lookup method and ones with a random walk-based lookup method. Both of these have random topology of peer connections. Structured P2P overlays with a structured and logical topology are more advanced. Structured P2P overlays can be classified based on the routing mechanism or on the topology. Our main interest is in Chord, Pastry, CAN and Kademlia, which have a flat topology and the routing of which is classified as second generation multihop-based routing. This means that they use incrementally converging routing with multiple hops in order to find the target. The protocols in this category are the most prominent protocols for the P2PSIP overlay implementation. Other related protocols are also presented to give an overview of different P2P overlays. However, the protocols in Figure 14 with gray font are not presented; they are only shown in the figure to give examples of other categories in the taxonomy of P2P overlays.

2.3.4 Unstructured Peer-to-Peer Overlay Networks

Many file sharing networks (especially the uncommercial ones) in the Internet have been based on unstructured P2P networks. An unstructured network is based on an overlay of randomly connected peers. Therefore, an algorithm that is used within the overlay does not organize the structure of the overlay, but the network is self-organizing. Nodes join the overlay network with some loose rules, without any prior knowledge of the topology [IEEELua04]. Proximity is not always taken into account in unstructured P2P networks [Acosta05]. This means that neighbour peers might be located in the same subnet (like in the same building) or may as well be on the other side of the world. *Some networks adapt to the underlying physical topology, but such optimization is not required for the algorithm to work properly* [IEEEDoval03].

NATs and firewalls cause difficulties in P2P connections, and therefore unstructured systems have concentrated on these practical problems in order to make the system work [Singh04]. This is an important issue address in P2P systems, as the majority of Internet computers are behind a NAT. The NAT issue for P2PSIP is discussed in more detail in Section 3.4.

2.3.4.1 Resource Lookup in Unstructured P2P Overlay Networks

A resource lookup in an unstructured overlay network is not very efficient, as the overlay structure is not deterministic. A node in an unstructured P2P network is in principal

unaware of the resources its neighbour peers maintain (neighbours are learned right after the initial connection). There are two ways to implement a lookup in unstructured overlays. One is the **flooding-based lookup** method, and another is the **random walk-based lookup**. They were both presented in the taxonomy Figure 14.

In the **flooding-based** method, a lookup is based on a "blind search" where the request is flooded in the network by sending it to every neighbour. If neighbours of a receiving peer do not have the resource the peer is looking for, they send the request to their neighbours. The request floods in the overlay until their Time-To-Live (TTL) counter reaches its limit (this counter is decreased after every hop). This counter is used to avoid the request to be flooded to the entire overlay and to avoid the overlay network to be congested of search requests. However, this may cause the search to fail, when some peers are outside the TTL limit and therefore cannot be reached. Flooding-based search is inefficient especially in large networks. Every node within the TTL range of a query has to participate in the lookup either by answering or forwarding the query. A flooding-based lookup has a theoretical limit of N hops (i.e. complexity of O(N)), where N is the number of nodes within the query's range (range defined by TTL). The limited search horizon is not critical (but is rather accepted) in open file sharing networks such as Kazaa, because they are used for general file sharing and do not require every file to be reachable for everyone. In applications such as reliable distributed data storage, where the resource has to be found, this limitation is unacceptable. This kind of application with reliable search mechanism can be implemented using more efficient structured overlays, which are discussed in Section 2.3.6. [IEEEDoval03]

In the **random walk** method, a lookup query is forwarded to a randomly chose neighbour at each step until the object is found. Multiple "walkers" can also be used to enhance the query process. Random walk querying is optimally only as fast as the flooding-based, but it reduces the network traffic by two orders of magnitude in many cases. [Lv02]

2.3.5 Examples of Unstructured P2P Networks

We present here shortly some of the most well-known unstructured P2P protocols that are used in file sharing. They are presented mainly in order to identify some file sharing networks that use unstructured P2P algorithms. Their taxonomies are shown in Figure 14. Note that in addition to unstructured P2P networks, today many P2P file sharing

networks are based on structured networks and use Distributed hash tables (DHTs). Structured P2P networks and DHTs are described in detail in Section 2.3.6.

2.3.5.1 Napster

Napster, along with some others (such as Gnutella and Freenet), was one of the first P2P experiments. It is a hybrid system (see Figure 10b), as only the download capability is distributed. The search is done using the central Napster index server. Napster was shut down due to illegal digital music sharing. However, it was an important stepping stone and it paved the way for decentralized file-sharing programs such as KaZaA. [Lv02]

2.3.5.2 eDonkey

The eDonkey network is also based on a hybrid model. eDonkey uses multiple hubs, whereas Napster uses just one entity. Even though the eDonkey client distribution was forced to end (also due to the illegal usage of the network), the eDonkey network still stands as one of the most popular P2P file sharing networks [CacheLogic06]. This continuity of the network operation is possible, because it is not operated by any single central entity (as Napster was).

2.3.5.3 Gnutella

Gnutella was developed a year after Napster, and in contrast to Napster, it is fully distributed. Gnutella gained wide popularity after Napster was shut down in early 2001. Initial poor scalability was enhanced e.g. with supernodes, and later with central “hubs” in Gnutella2. Also the search mechanism was improved. Gnutella is still operational, but accounts for less than 10% of total P2P network traffic [CacheLogic06].

2.3.5.4 FastTrack (used by Kazaa)

FastTrack is a P2P protocol for file sharing (mainly mp3 music, but also other file types). FastTrack is used mainly by Kazaa. Kazaa was created by the founders of Skype and it is the third most used file sharing network after BitTorrent and eDonkey networks [Parker05]. Kazaa does not have central entities, but any peer may become a supernode. A file can be downloaded using multiple peers, as the files are split into segments. Supernodes are used. Kazaa network has not been shut down, as the owners of Kazaa are not legally responsible for the actions of the users. [IEEELua04]

2.3.5.5 BitTorrent

The BitTorrent protocol is currently the world's leading (with over 135 millions users) peer-assisted digital content delivery platform [BitTorrent]. BitTorrent uses unstructured overlay topology, but also DHT-based (see 2.3.6.2 for DHT) BitTorrent clients exist (e.g. µTorrent). BitTorrent is not fully decentralized, as it uses websites to publish the information of files the people are sharing. These links enables the contact with a tracker, which gives a list of peers that are sharing the file. With these trackers, a client can join a "swarm" (i.e. a group) of peers and start downloading from multiple peers [IEEELua04]. This feature enables very fast downloading and is a major reason for the popularity of BitTorrent.

In addition to general (but often illegal and copyright-violating) file sharing, a growing number of individuals and organizations are using BitTorrent for fully legal material distribution (e.g. TV shows).

2.3.6 Structured Peer-to-Peer Overlay Networks

Structured overlay networks overcome the limitations of unstructured networks by organizing the topology with some structured content location mechanism such as DHT. Like an unstructured network, a structured network is an overlay having virtual link connections between the participating nodes. However, only structured overlay networks create virtual topologies based on node-content attributes (such as a hashed IP address of the node) [IEEEDoval03]. These peers are assigned with static identifiers by using a distributed data structure such as DHT. The identifier values (i.e. keys) determine the structure of the overlay, as the identifiers are organized logically. These keys and key spaces are discussed in more detail in the next subsection.

As a consequence of the deterministic structure of structured overlay networks, maintenance efforts to keep the correct structure are increased due to the churn (i.e. joins and leaves of nodes). The churn concerns especially structured P2P overlays, as structured overlays need to maintain a specific and valid structure of the overlay. If the churn handling of the algorithm is not efficient enough, it may cause the entire algorithm to be inefficient. Also, if churn was handled too aggressively, it could also make the algorithm inefficient, as then the maintenance signalling would load the overlay unnecessarily. However, even though the churn is needed to be taken care of in the

design of structured P2P algorithms, structured P2P overlay networks are in general well scalable.

Applications of structured overlay networks include large and reliable data-sharing, content distribution and application level multicast applications, and Internet voice and other media communication applications. [IEEELua04]

2.3.6.1 Resource Lookup in Structured P2P Overlay Networks

The general idea of resource lookup in structured overlays is presented here, but it is described in more detail below in relation to DHT and its implementations such as Chord (Chord is presented in Section 2.3.7.1).

A lookup in structured overlays is based on identifiers derived from the content. However, as a consequence of this, advanced keyword-based searches are not directly supported in structured overlay networks, but can be layered on top of a DHT [Harren05]. Every peer holds information on the resources offered by its neighbour peers, and every peer participates (if needed) in the search queries (either by forwarding or replying). In addition to this, as the overlay network is structured deterministically, every peer knows "whereabouts" a resource (or to be specific, the identifier (ID) of a resource) can be found, if present in the overlay network. This implies that, unlike in the blind search method, queries can be directed, and each hop brings the query closer to its target (either recursively or iteratively, see Figure 15). This reduces the need of messaging and peer involvement. Therefore, the load for the network is substantially reduced [Aberer03]. In addition, as a search does not need to be TTL-limited in structured networks, false negatives can be entirely avoided [Bryan06]. In the case of false negative, a resource to be searched would not found even if available in the network. This feature is very important in reliability-demanding systems (e.g. VoIP environment or distributed data storage).

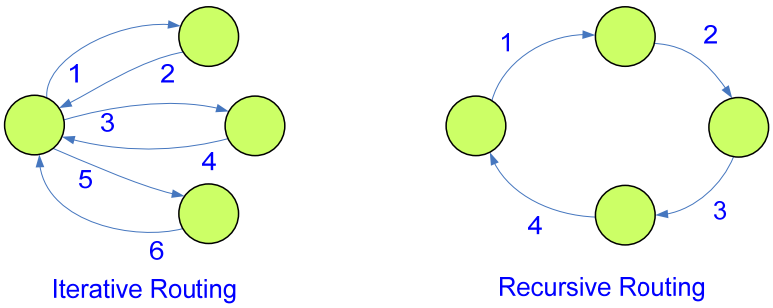

Figure 15- Iterative vs. Recursive Routing

In addition to **guaranteed data retrieval**, structured overlay networks have three other qualities. These are **provable lookup-time horizons** (typically O(log(N)), where N is the number of peers within the overlay), **automatic load balancing** and **self-organization** [IEEEDoval03]. The provable lookup time horizon means that as the network is structured, the maximum hops needed to solve a query is known and therefore bounded. Automatic load balancing is achieved by the function of DHT of distributing keys evenly over the nodes. Load balancing can be achieved also e.g. with file downloading, where a downloading peer automatically becomes a peer to provide the content for downloading. Self-organization is achieved using rules that define where the key identifier of a joining peer or resource needs to be located. The information of the new peer or resource is sent (in the same way that a lookup is done) to the peer that is responsible for that part of the key space where the new key belongs. Also, when the protocol notices that some ID in the responsibility range of the peer is lost, it takes appropriate actions to ensure that the structural rules apply and no old (and thereby invalid) mappings exist.

2.3.6.2 Distributed Hash Table (DHT)

As was stated earlier, DHT abstraction can be used to implement a structured P2P overlay algorithm. By being distributed, DHTs provide a location-independent substrate that enables general mapping between any information and a location within an overlay key space [Viana04].

DHTs were motivated in part by P2P file sharing networks such as Napster and Gnutella that suffered from scalability and/or security issues. DHTs has the benefits of Napster (i.e. guaranteed results) and Gnutella (i.e. decentralization), while still being well efficient and scalable. There are no standardized DHT implementations yet, but lots of simulations exist.

Distributed Key Space

Each peer has a set of keys of the entire key space (i.e. hash table), and the peers are responsible for the key space that is assigned to them (see Figure 16). Therefore, the entire key space is decentralized, and as the peers are organized into a graph using a DHT structure, each key can be found within the overlay network with the help of the peers. Every peer is assigned with a key that maps to the same key space and is also related to its responsible key space. Each resource has also a key (i.e. a resource-ID). The key can be obtained with a hash-function (such as SHA-1 [SHA-1]) from some keyword

or value that uniquely identifies the resource or the peer. For example, in Chord (explained later in Section 2.3.7.1) an IP-address of a peer is used in the generation of corresponding hashed key value [Stoica01].

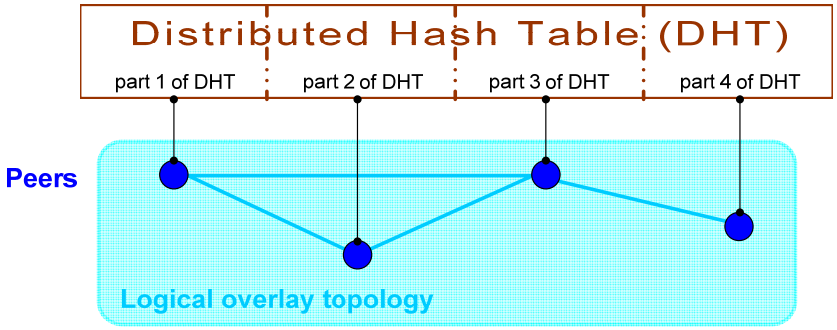

Figure 16- DHT Distributed to the Peers

In general, DHTs can be used in decentralized distributed systems to partition the ownership of a set of keys among participating nodes. Routing of messages to the unique owner of any given key of the key space is efficient and reliable even in large networks.

Consistent hashing

Most algorithms that use DHTs partition the key space using some variant of consistent hashing. Consistent hashing is designed to allow a node to leave and to join the overlay with minimal disruption. Every peer in the overlay network is assigned an identifier (ID) key *i*. All the keys, which are closest to the ID key *i* of the peer, are owned by the peer (how this is defined, depends on the DHT implementation). Consistent hashing can be used to map keys to peers using an abstract notion of distance between two keys. This range is defined by a function of consistent hashing technique. An essential property of consistent hashing is that when a peer leaves or joins the overlay network, no remapping of entire key space is needed (with traditional hash tables nearly the entire key space has to be remapped). This implies that only peers having adjacent IDs are affected when a peer is leaving or joining. [Karger97]

DHT Layer and its Operations

The use of DHT adds an additional protocol layer (i.e. the overlay network) between the TCP/IP and the application layer (see Figure 17). The DHT layer is used only for signalling, and e.g. media is not transported via this DHT layer. This algorithm is being run in all the peers participating in the structured overlay network. The DHT layer is an overlay between the DHT-related applications and the transport layer. One such

application (in development) is P2PSIP, which uses the DHT layer to implement SIP applications.

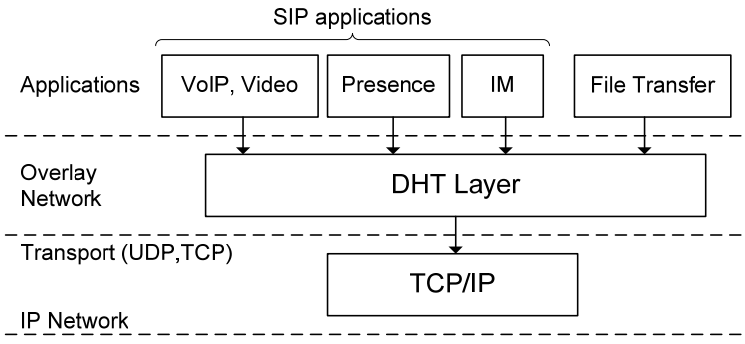

Figure 17 - P2P Protocol Layers for Control Signalling [Sinnreich06]

DHT Interactions

Figure 18 illustrates the four different types of API interactions between a DHT overlay and its peers. These are **Put(Key,Value), Remove(Key), Get(Key) and Value.** The first three are operations and the last (i.e. Value) is a response to the Get(Key) operation. After joining the overlay network, peers can use these operations to make a query for a key, or insert/remove a key and its value to/from the overlay network. To make a query on a resource, a Get(Key) method is used to receive the value. To insert a resource or a peer to the overlay network, a Put(Key, Value) is sent to the overlay (the key is the hashed identifier of the resource). These operations can be sent to any peer in the overlay, as the messages are forwarded to the peer responsible for the range of key space where the key belongs. Exception to this is, of course, when a value to the query (i.e. Get(Key)) is returned directly to the peer that sent the query. [IEEELua04]

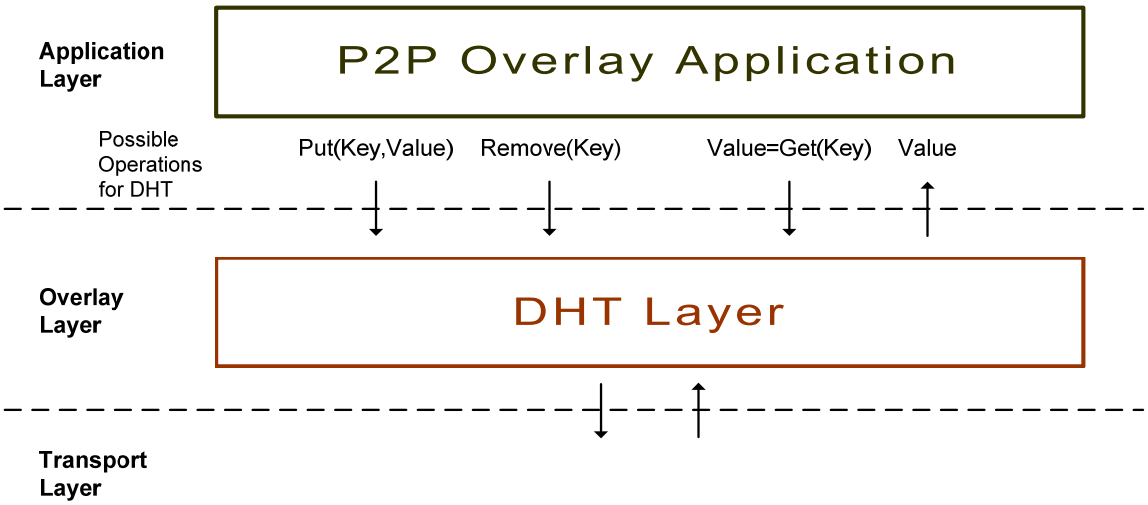

Figure 18 - DHT Interaction Operations

2.3.6.3 Benefits of DHT

As a summary, we present the properties that constitute the benefits of DHT. DHT-based networks are **self-organized, fully distributed and highly scalable [Carton04]**. Naturally, a bad DHT implementation may lack these beneficial qualities. However, at least the first four DHTs introduced in 2001, possess all these properties. Three of these four DHT implementations (namely CAN, Chord, Pastry, and Tapestry) are presented in Section 2.3.7. As DHTs are fully decentralized, there is no single point of failure. Fault tolerance is achieved through this decentralization as well as through tolerating (in some sense) peers continuously joining and leaving (i.e. churn). Scalability is related to decentralization, because the load and resources are distributed without a central server of storage, computing power and bandwidth. In order to realize these properties, the common technique in DHT is that any peer needs to coordinate with only few other peers of the overlay. The amount of work needed to perform an operation can be limited (by the nature of the DHT) typically to O(log(N)) involvement of the N participants of the overlay. This also entails a disadvantage of DHTs when compared to the client-server architecture. The lookup complexity is O(log(N)) hops to find the match, in contrast to a centralized client-server topology, where this is always O(1). This means that as the number of peers grows, the routing table of every peer increases logarithmically. However, this is an acceptable trade-off to achieve the benefits mentioned above.

2.3.7 Examples of Structured P2P Networks

Many of the first popular P2P networks such as Napster, Gnutella and KaZaA are unstructured. However, most of the recent P2P systems use a more advanced topology of structured algorithms (including also many enhanced versions of originally unstructured ones). BitTorrent and eDonkey are examples of very popular P2P networks that are used for file sharing. For voice and other media communication, Skype has proven the good applicability of P2P networking for communication other than just file sharing. Besides, P2P networks could also be used for emergency information flow as well as for SPAM detection and filtering [Mellin04].

We will now present some notable DHT protocols and implementations that could be used in P2PSIP. These are Chord, CAN, Pastry, Kademlia, Bamboo and JXTA. Main weight is kept in Chord in order to give one example of a DHT implementation that can be used in P2PSIP, while the others are merely shortly introduced.

2.3.7.1 Chord

Chord [Stoica01] is a simple and popular structured P2P algorithm that implements the DHT abstraction. Chord can be used to map a given key onto a node (i.e. a peer in the context of P2P network) in a Chord overlay. This mapping is the only function that the Chord protocol has. In the context of P2PSIP, the Chord algorithm is found to be the most prominent choice, as it is the most used one in the P2PSIP drafts (and as it is widely favoured in the P2PSIP community). Therefore, we will describe Chord in more detail than the other DHTs introduced here. Other algorithms may be allowed to be used in P2PSIP as optional alternatives, while support for one designated DHT will be required.

Identifiers (i.e. keys)

A Chord overlay has an identifier circle of modulo 2^m for peer IDs (m is an integer to define the ID space of a Chord ring). Usually, a 160-bit (i.e. m=160) key space is used in order to avoid collision of keys (i.e. two different mappings for a same key value). Each peer in a Chord ring has an ID. This identifier is chosen by hashing the IP address of the peer using a hash-function (such as SHA-1). The same hash function is also used to map any key (of data) to be stored by the Chord overlay onto a key-ID. The identifier length m has to be large enough in order to avoid a situation (called collision) of two peers having the same ID. Figure 19 shows and example of a 3-bit large Chord overlay, where there are three peers participating in the overlay. Naturally, the maximum number of peers in a 3-bit large Chord overlay is 2^3=8.

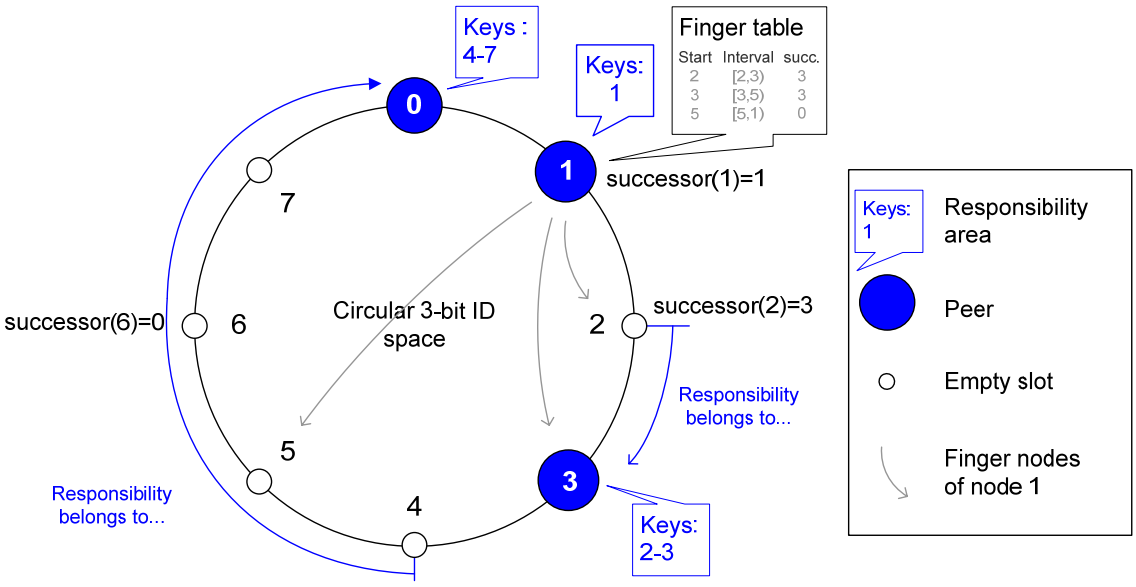

Figure 19 - Chord Ring with Three Peers

Mappings (i.e. Virtual Links) Between Peers

A peer knows O(log(N)) other peers. These consist of the *successor, the predecessor* and the *fingers.* The *Successor* is the following peer that a peer knows, i.e. in Figure 19; the successor of the peer with the key ID "3" is "0" (as the circle is navigated in modulo 2^m). Accordingly, the *predecessor* is the peer that precedes the peer. Fingers are used to enable a hop (i.e. a virtual link between two peers) further than just to the successor or the predecessor in the ID circle. *Fingers* (at most m entries for each peer) are every peer s = successor $(n+2^{i-1})$, where $1 \leq i \leq m$. s is the i^{th} finger of the peer n. For example, in Figure 19, the fingers for "1" are: "2", "3" and "5". Fingers may point to an empty slot. Successor in the finger table defines the consequent (i.e. successor) peer to that finger key.

Mapping updates

It is enough to use successors for correct routing, but the finger table and predecessor information are used to accelerate the routing (as using only successors it might take N hops to resolve a lookup). Routing tables need to be updated frequently to remain valid. However, as successor information is enough to maintain the Chord overlay operational, the basic stabilization is used to keep only peers' successor pointers up to date. Finger tables need to be updated regularly as well, but the basic stabilization is done more frequently, as it guarantees the correctness of lookups.

Joining a Chord Overlay

In order to join the overlay, the joining peer hashes its IP address and sends it to any peer within the Chord overlay. This initial peer to be contacted is called a bootstrap peer. There are several mechanisms that can be used to find a bootstrap peer, and the bootstrap mechanisms proposed for P2PSIP are described in Section 3.3.2. After the joining peer has contacted the bootstrap peer, it exchanges messages with its predecessor and the successor (related to its hashed key) to update the routing tables. The joining peer accepts part of the responsibility area of the keys (between its own key and that of its predecessor) from its successor.

Routing in Chord

Routing in Chord is done by forwarding (either recursively of iteratively, see Figure 15) messages to the largest peer-ID preceding the key-ID to be searched. This is done until

the direct successor of a peer has a larger ID than the key-ID (as it is responsible for the previous keys, as can be seen in Figure 19).

Lookup procedure

The lookup of a peer in the Chord overlay is done using the DHT abstraction. Thereby, a peer does not know all the peers in the overlay, but only some of them (only O(log(N)) other peers must be known for efficient routing). This improves the scalability when there are many participating peers in the overlay. In order to find a previously unknown peer in the overlay, a peer does a lookup. It knows "whereabouts" the key of the searched peer is (i.e. which peer is closer) and sends the lookup to that direction. This continues hop by hop as long as the peer that is searched is found. A lookup procedure requires O(log(N)) lookups, when there is N peers in the system. Every peer in a Chord overlay is equivalent in functionality.

Figure 20 depicts a lookup procedure in Chord with a 2^7 key space, five peers and four resources. A lookup is defined to be done recursively. Peer 32 wants to find the key-ID 90. It asks the closest ID that is proceeding to the 90. Thereby it contacts **(1)** the predecessor of 90, which is 80. 80 forwards **(2)** the query to 105, as 80 knows 105 is responsible for the ID-keys of 81-105. 105 tells the content of 90 to 80 as a reply **(3)**, and 80 forwards the answer to 32 **(4)**.

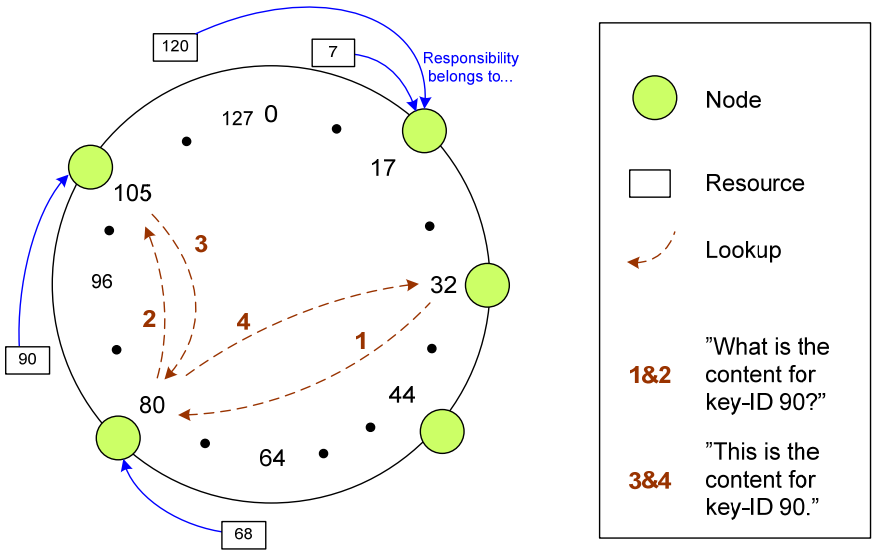

Figure 20 – An Example Resource Lookup Procedure in Chord (Recursive Routing)

2.3.7.2 CAN

The Content-Addressable Network (CAN) is basically similar to Chord, but it also has many differences. Rather than a virtual ring, CAN uses d-dimensional Cartesian coordinate space to implement DHT that maps keys onto values. CAN allows nodes to specify their own identity. State maintained by a CAN node does not depend on the network size of N, and the lookup cost increases faster than log N ($O(dN^{1/d})$). CAN requires an additional maintenance protocol for periodical remapping of the key space. CAN optimizes the forward path by the best round trip time (RTT) of neighbours. This implies that the queries are forwarded without interacting with the querier. Thus, the querier cannot verify the forward process of its lookup and the algorithm is susceptible to misrouting attacks. [Ratnasamy01] [Sit02]

2.3.7.3 Pastry

Pastry is similar to Chord, but differs from it in some details. Pastry is a prefix-based routing protocol and not based on numerical difference like Chord is. Pastry has a hybrid tree-ring geometry, while Chord has a ring geometry. Pastry is self-organizing and takes proximity into account by using a scalar proximity metric, such as the number of IP routing hops or geographic distance. [Viana04] [Stoica01] [Rowstron01]

Pastry is used in various applications, such as end-user application of Web caching, group notification and IM. [IEEEDoval03]

2.3.7.4 Bamboo

The geometry of Bamboo is similar to (but still differs from) that of Pastry, as Bamboo also uses hybrid tree-ring geometry. Bamboo is designed to handle churn, which is a big concern in P2P networks. Bamboo has lower routing latency than Chord (and even smaller under churn). This is a good feature especially when considering VoIP. The quick "local tuning" part of the routing algorithm of Bamboo is similar to the routing algorithm of Pastry, but it is incremental and more frequent. "Global tuning" of Bamboo routing maintenance is similar to the stabilization of Chord and is used for optimization of the static network. Tuning is only one part of neighbour discovery and state maintenance. Leaf set maintenance and routing table filling occur before the tuning of routing tables. [Rhea03]

2.3.7.5 Kademlia

Kademlia is a DHT implementation for decentralized computer networks and it has been used for file sharing. The Kademlia algorithm is based on calculating a distance of two node IDs. This distance is used to maintain a similar list to the finger list in Chord. The list is filled from IDs of the requests of reply messages the node receives. Kademlia is resistant to certain DoS attacks, as the list cannot be flushed of valid node-items. Lookup is similar to Chord, but Kademlia can perform multiple parallel requests for the same query. [Maymo02]

Kademlia is implemented e.g. in the fully decentralized Kad Network (used in file sharing), and usually a client can join the Kad Network by querying the eDonkey network for known Kad nodes. One such client is eMule. Some BitTorrent clients, e.g. µTorrent ([uTorrent]), also use Kademlia for decentralized tracking or trackless torrents.

2.3.7.6 JXTA

JXTA is an open source P2P platform that is defined as a set of XML based protocols. JXTA is a very mature P2P framework and it has been designed to enable decentralized communication for a wide range of devices (such as PCs, cell phones, PDAs). [JXTA]

JXTA is a modular platform that provides simple building blocks for developing a wide range of distributed services and applications. JXTA specifies a set of protocols rather than an API. Thus, JXTA technology can be implemented in any language on any Operating System. [JXTA]

JXTA is optimized for frequent churn (i.e. devices joining and leaving the network). Many other P2P protocols (such as Chord and CAN) concentrate more on reducing the lookup time. This results in their operations for handling churn being more expensive [Matthews05]. Nonetheless, e.g. Chord tolerates nodes churn rather well [Stoica01].

2.3.8 Reputation of P2P Traffic in the Internet

Free riding, common illegal misuse and excessive traffic load caused by many P2P file sharing networks have given P2P networking a bad reputation in general. As was stated in 2.3, a relatively small number of Internet users (about 30%) generates the bulk (about 80%) of the total Internet traffic. This is caused mainly by users of only few file sharing networks. This fact is telling of their efficiency (as regards their data transfer volume capability), but also of their popularity. The P2P algorithms have evolved and become

more sophisticated with time and they are robust and well-decentralized. Therefore, they are very difficult to shut down.

Most of the P2P traffic today is thus generated by the file sharing networks and, unfortunately, it often involves illegal copyright-violative file sharing. This has led to law suits: Napster, for example, was forced to shut down and to pay more than $30 million in one such case and the developer company of eDonkey agreed to pay $30 million in an out-of-court settlement to avoid the same fate. The file sharing networks were not developed for these kinds of illegal actions, but those being open for any kind of file sharing were quickly exploited also for this purpose.

Many operators apply traffic shaping in order to limit, or even impede, the high bandwidth applications such as BitTorrent. Others settle for only monitoring the traffic, because they are afraid of losing customers. In addition, if identified P2P traffic is filtered or slowed down, users find another way to use the P2P applications; i.e. they start using applications with encrypted connections. This would increase the load (encryption increases the amount of data) and operators would no longer be able even to identify the P2P traffic [Mellin04] [Mike06]. Also, from the operators' perspective, P2P networks such as Skype also have a bad reputation (even though they do not consume much bandwidth and are not illegal), because Skype and other similar Internet service providers reduce the operators' revenues from their services (especially international calls).

As some P2P applications can easily be (and are) exploited for illegal purposes, they facilitate the observation of users' psychological behaviour. A P2P network, which is intended for legal activities, but has no clear control, can be exploited for illegal purposes. When users have this opportunity, many of them tend to exploit it, as has been seen e.g. in the case of BitTorrent. BitTorrent is widely used for illegal file sharing, even though it was originally intended only to enable the sharing of large amounts of data generally in a distributed manner. The nature of a P2P network is shaped by the complex interplay between the technical, social and economic influences.

Figure 21 illustrates the correlation between the quality of service and the quality of content. Without clear control, a P2P network can be used for free riding (i.e. using the resources without sharing any). [Parameswaran01]

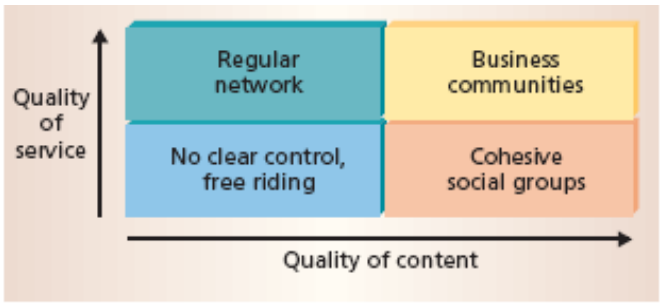

Figure 21 - Peer-to-Peer Service Quality Matrix [Parameswaran01]

The best quality of a P2P service can be achieved by a business community or by a cohesive social group. If a P2P network does not have any clear control, its quality cannot be guaranteed. Factors affecting group behaviour include not only the behaviour of other group members, but also the context of interaction amongst the members of the group. Thus, in a business community, rational rules govern transactions (while the membership is also usually controlled). In a social group it is more altruistic behaviour based on social norms and similar ideology that ensures the quality. [Parameswaran01]

2.4 Related (VoIP and Internet Messaging)

We present here some networks and forms of real-time communication related to P2PSIP.

2.4.1 Skype

In its own field, Skype [Skype] dominates the global VoIP traffic with its 220 million users (according to Q2 2007). Skype network has 3.5 to 9 million users connected at any one time [Wolff07]. Skype is based on the Kazaa architecture and it also uses supernodes. Thereby, a computer running Skype may become a supernode [Singh04].

Skype is a popular example of an overlay of a P2P communication network (even though it is not a fully decentralized system, because Skype uses some servers). Skype is a closed proprietary system. As such it is controlled by the Skype Company, and therefore it is not openly interoperable with other networks. Skype has earned its wide popularity by the possibility to make free calls all over the world without the need of any cumbersome configurations. Cumbersome configurations can be avoided; as only one service provider is used (i.e. Skype) and most of the required configurations are integrated in the Skype software (only an initial user registration is needed). Skype has widened its range of services, of which one of the newest is a chat room enabling service "Skypecasts" [Skype]. Another big service launch of Skype is a P2P based web TV service called Joost™. A major advantage with Skype is that it implements equivalent

Simple Traversal of UDP (STUN) [STUN] and Traversal Using Relay NAT (TURN) servers in the node itself to handle NAT traversal [Singh04]. In SIP applications, this is not the case, as explicit server configuration is used.

Skype is a good reference especially in performance, when developing the P2PSIP. However, it has been noted that Skype uses also some central servers [Baset06]. It is therefore not a pure P2P network, which the P2PSIP aims to be [Singh04]. Further analysis of the functionality of the Skype protocol can be found in [Baset06].

2.4.2 SOSIMPLE

The Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) Working Group (WG) has developed a set of standardized extensions to the existing SIP that add IM and presence support to SIP. Self-Organizing SIMPLE (SOSIMPLE) is based on existing SIP/SIMPLE architecture, but uses the DHT-based Chord (i.e. the P2P approach instead of the client-server approach). The developers of SOSIMPLE have continued the development in the form of P2PSIP under IETF, and now more extensively with other developers. Therefore, SOSIMPLE is a precursor of P2PSIP, and the development of P2PSIP has evolved from the SOSIMPLE. [Bryan05]

2.4.3 Instant Messaging (IM)

Instant messaging (**IM)** is a form of real-time communication between two or more people based on typed text. The text is conveyed via computers connected over a network such as the Internet. IM requires a client that is used to connect to an IM service. IM clients usually include a presence capability that allows the online status (e.g. “on-line”, “away”, and “offline”) of users to be seen by other users in a contact list. Some of the most popular clients are AIM, Ebuddy, Windows Live Messenger and Yahoo! Messenger. Skype has IM capability as well and it is also a popular IM client.

2.5 Summary

In this chapter we have given technical background information in order to make the concepts related to P2PSIP familiar. This background information serves as the foundation for the following chapters. The main focus was on giving a sufficient introduction to SIP, which is a standardized signalling protocol used in establishing multimedia sessions. There is also a 3GPP version of the conventional SIP, which is used in the IMS (the IP multimedia subsystem for operators) to provide Internet services in mobile networks. In addition to SIP, we also gave quite an in-depth introduction to the concept of peer-to-peer (P2P) networking, because of its essential role in P2PSIP, where the conventional client-server architecture of SIP is replaced with a P2P architecture. P2P networking dominates the Internet by constituting approximately 80% of the entire volume of traffic in the Internet. This is mainly due to the widely used P2P file sharing networks, which have efficient P2P file sharing properties to allow fast download speeds. The dominance of P2P traffic in the Internet shows the potential of P2P networking in general, not only for file sharing. However, in general, P2P networking has a bad reputation due to its bandwidth-consuming (and often illegal) file sharing network usage. Furthermore, Skype that runs on a P2P system is a rival service operator for traditional telecom operators. In P2PSIP, which will be presented in the next chapter, the P2P concept is adopted in order to provide an alternative for the conventional client-server architecture in SIP.

3 Peer-to-Peer SIP (P2PSIP)

Peer-to-Peer SIP (P2PSIP) is being developed under the IETF and will be a standardized protocol during the forthcoming years (the goal is set to late 2008 for the P2PSIP Peer Protocol.) P2PSIP makes it possible to establish end-to-end multimedia sessions (e.g. VoIP) with no or minimal centralized servers between the participants. The usage of P2P networking (instead of client-server architecture) in SIP makes it possible to distribute the functionality of SIP servers among the peers. Therefore, SIP servers are not needed, as peers can collectively handle message routing and maintain the distributed directory service of UAs and services using a DHT abstraction. SIP may be used to handle the signalling of the P2P overlay operations, but SIP signalling is reused as such for the session signalling of P2PSIP.

The nature of P2PSIP is similar to the well-known Skype, but unlike Skype, P2PSIP is not based on proprietary protocols, but will be an open and standardized system. As with Skype, the P2P-property of P2PSIP has the potential for scalability for millions of users to be connected to a single P2PSIP network.

Even though P2PSIP has the same basic idea as SIP to establish, modify and terminate multimedia sessions, P2PSIP aims to use only simple SIP. Simple SIP only uses message routing required for session initiation and leaves all the complexity of the applications to be handled in the endpoints. Therefore, simple SIP does not use the vast amount of extensions that add network services to the native SIP rendezvous and session initiation functions. This approach can reduce the number of required SIP related standards from roughly 100 to about 11. [sip-tools-01]

This chapter will give a general idea of the technical part of the P2PSIP and its functional features. Also general use cases are presented to show the potential usage purposes of P2PSIP for mobile operators. More specific use cases for mobile operators are discussed later in Chapter 5.

3.1 Motivation

Benefits of Using P2P Networking for SIP

In general, P2P networks have functionalities and features that overcome the disadvantages and limitations of the conventional client-server environment. These include better scalability, fault-tolerance, load-balancing etc. (these were discussed in

Section 2.3). Additionally, a P2P network can be self-organizing. By implementing an alternative to the client-server architecture of conventional SIP with P2P networking, full use of these advantageous features can be made.

The nature of a basic voice (for which SIP can be used) call is peer-to-peer, since only the corresponding endpoints are involved. Therefore, no third party is required for the call itself. In the conventional SIP, servers are usually used mainly for user registrations and to route the call signalling messages between the UAs. These provide a good opportunity to use P2P networking for SIP, where the functions of SIP servers are distributed among the peers. As the P2P property of P2PSIP makes it possible to run a P2PSIP network without the need of central servers, heavy VoIP infrastructures can be avoided. Therefore, reduced infrastructural and operational costs can be achieved. Also, as servers that are often operated by some third-party are not required, outside involvement in a group (e.g. an enterprise employees or such) can be avoided.

Benefits of Reusing SIP

In the current SIP, two UAs are already capable of communicating directly (SIP servers are optional). This capability for direct communication in SIP makes it rational to reuse SIP for the P2P approach of session establishment, which corresponds more with the nature of end-to-end communication. The wide usage of SIP in the Internet (and support in terminals) also brings interoperability benefits for P2PSIP.

Most recent networking endpoints, such as conventional desktops, notebooks, PDAs and even smartphones have powerful computing capabilities. Therefore, they are expected to be well capable of handling SIP and SIP-based applications. Increased number of mobile phones already have integrated SIP stack and SIP-based applications. This enables a wide variety of terminals to use SIP for personal communication (e.g. VoIP), but it also allows for the possibility to take part into P2PSIP overlays. It would be possible even for mobile size terminals with limited resources (e.g. smartphones) to use P2PSIP due to the good interoperability of P2PSIP with conventional SIP or via the proposed lightweight P2PSIP Client Protocol.

SIP also has many other good existing features that ease the development of P2PSIP as they are reused. These features include of the good security and existing NAT traversal mechanisms of SIP, as well as its sophisticated signalling mechanisms.

Standard vs. Proprietary Protocols and Their Interworking

Skype as a P2P VoIP network is a good example of how a large and world-wide multimedia communication network can be maintained without huge complexity, but also without heavy maintenance and infrastructure costs.

Nonetheless, a standardized and open solution like P2PSIP would enable faster evolution in service development than the proprietary ones such as Skype. The main drivers for growth of new and emerging technologies have proven to be open and standard platforms, universal applications, scalability, and interoperability [TeliaSonera06]. Skype (and other proprietary P2P networks) does not possess these properties, except that it is scalable. Skype takes interoperability into account only if it can have some business advantage of it. P2PSIP is interoperable with conventional SIP, and due to its open standardized nature, it can be made interoperable with other systems as well (e.g. with PSTN and IMS). Interworking with P2PSIP is discussed further in Chapter 4.

P2P to Provide Efficient VoIP Solutions

The evolution of voice calls appears to move inevitably towards a packet-switched environment with IP, and VoIP will most probably replace the traditional circuit switched voice some day [Mohanty05]. Some of the reasons for this are that voice can be carried more efficiently in packet-switched network and that a wider variety of services can be provided in such a network (than in circuit-switched networks). This trend of moving towards packet-switching boosts the major motivation (i.e. the reduction in infrastructure and operational costs) to use P2P between end-user devices for commercial VoIP services [p2p-usecases-00].

Cost-efficiency is important. It is generally assumed that basic VoIP call services are free. However, an operator or some service provider that implements a VoIP service may, of course, charge users for using the VoIP service. Usually, commercial VoIP services need to generate revenues from something else than the actual VoIP calls in order to bury the costs of running the VoIP infrastructure. Also, someone has to pay for implementing the VoIP infrastructure. There are different ways of doing business with VoIP, but revenues often incur from termination fees (of using PSTN gateways) and other additional services (e.g. voice mail, IP-PBX). However, revenues can also be generated through advertising e.g. with short texts or small animated windows within the VoIP client, but as well with video clips in the beginning of video calls. Nevertheless,

these are better suitable for PC clients, as many mobile terminals are not capable of running such animations or video calls.

P2PSIP could offer a more cost-efficient way to provide VoIP solutions than the infrastructure-based (e.g. SIP) VoIP solutions. This does not imply that all the endpoints would need to fully participate to routing and other obligatory functions that are needed to run a P2P system. Some endpoints can use e.g. delegated proxy peers to communicate with a P2PSIP overlay, but P2PSIP could also be run just among SIP servers to implement an efficient server farm using P2P networking (this will be explained later in Section 3.6.4).

The possibility of providing VoIP solutions with P2P networking may appear attractive especially for virtual operators and service operators without heavy existing infrastructures. However, even virtual operators might still need to have some servers, for example, to handle charging and subscriber management. It may also be interesting e.g. for companies to implement an inexpensive internal VoIP network. Some companies (e.g. Avaya and Peerio) already provide VoIP solutions based on the idea of P2PSIP. Nonetheless, P2PSIP (just like SIP) is not intended to be a replacement for existing TDM (Time Division Multiplexing) telephony systems, such as 2G/3G and PSTN.

A Citation from an article “The challenge of P2P Internet communications to network based services” from Elektrotechnik & Informationstechnik (2006) [Sinnreich06]:

> *P2P communications are the opposite to complex infrastructure based Voice over IP (VoIP) and multimedia systems such as IMS and TISPAN and may render them largely obsolete for reasons of cost, complexity and ease of innovation at the edge of the network.*

Another citation from the same article:

> *Complex infrastructure based communication networks are becoming obsolete by the emergence P2P communications. A fair guess is however the present business models in the telecom industry will have to change radically, for example charging for telephony and providing profitable VoIP is becoming questionable. Major Internet companies, such as AOL, Apple, Google, Microsoft, Skype and Yahoo already have recognized this fact and their communication services have vastly different business models compared to the telecom companies.*

Especially the second statement is quite radical, and the change (if realized) would take time, but it still has a point. The first statement is also rather bold, because it does not take into account the possibilities of regular SIP. Open and free SIP networks available in the Internet can also allow innovation at the edges.

Some prospect polarization between P2PSIP and IMS SIP has been observed among the SIP community, while the significance of the conventional CS SIP has diminished [Ott07]. Therefore, the importance of P2PSIP might become significant when it is developed. Impacts of P2PSIP are discussed in more detail in Section 5.3.

3.2 Architecture

In this section we provide a general description of the P2PSIP architecture. Specific details are not described, mainly because we want to focus on the essential properties for a general understanding of P2PSIP, but also because many issues still remain unresolved in the P2PSIP development.

3.2.1 General Architecture

The P2PSIP architecture uses a DHT algorithm for the P2P overlay, which is run by the Peer Protocol in every peer. The DHT layer (was shown in Figure 17) is used as a substrate for the P2PSIP operations. Therefore, the DHT layer also defines the structure of a P2PSIP network. The overlay structure of P2PSIP is presented in more detail in the following Section 3.2.4. The P2P property of P2PSIP requires that every peer (except P2PSIP clients) participate to the routing of the messages within the overlay. Message routing is described in Section 3.2.5 and message types in Section 3.2.7.

Every peer and resource has an identifier (ID) in a P2PSIP system. This ID can be used to locate peers within the overlay. The DHT defines how the IDs are stored in the overlay (i.e. in peers), and every peer has a defined ID space it is responsible for. In addition to an ID, a resource can be located using a more user-friendly identifier, namely a resource URI. This URI is similar to a SIP URI. An example of a resource URI is "sip:bob@p2psip.org;resource-ID=723fedaab1". More of identifiers can be found in Section 3.2.8.

Figure 22 depicts the general architecture of a P2PSIP overlay. As can be seen in Figure 22, P2PSIP peers (blue circles within the overlay ring) can provide different resources (squares on the peers' side). A peer can have multiple resources, and a UA is also a resource. Resources are discussed in more detail together with peer behaviour and functions in 3.2.6. Some resources (such as a PSTN gateway, proxy and redirect peer) can be used for interworking with other networks. Interworking is discussed in Chapter 4.

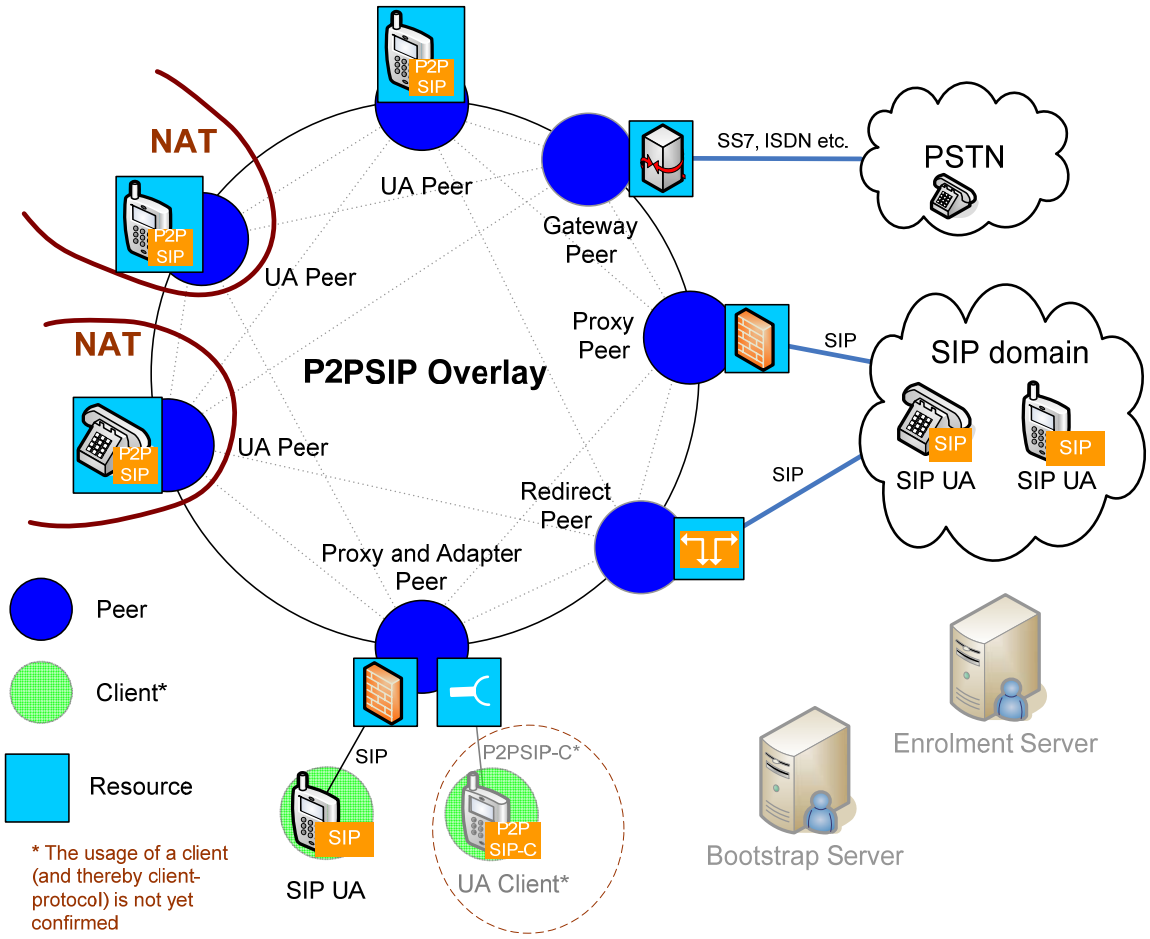

Figure 22 – Example of P2PSIP Overlay Architecture

The example of Figure 22 uses a ring topology (used in Chord), but it could also be some other structure (such as mesh) that depends on the DHT algorithm. NAT traversal is the most important issue when choosing the most appropriate approach (i.e. superpeer/ordinary peer vs. equal peers). The NAT traversal problem and these two approaches are described in more detail in Section 3.4.1.

The functionality of P2PSIP could be enhanced with few servers (seen as distinct entities in Figure 22), even though they are not needed in the core P2PSIP operations. These would be an enrolment server (to give credentials) and a bootstrap server (to introduce a bootstrap peer) for initial entry to a P2PSIP overlay. However, while these may not be obligatory especially in small P2PSIP overlay implementations, they are desired in many other use cases in order to enhance the security and thereby also the quality of the system. Enrolment server and bootstrap server are discussed more in Section 3.3. Security aspects of P2PSIP are concerned in 3.5.

3.2.2 P2PSIP Peer Protocol

P2PSIP reuses SIP messaging for session management, but independently of SIP servers (i.e. SIP over P2P). Additionally, P2PSIP is aimed to use SIP messages (with some extensions) also for the P2PSIP Peer Protocol. This protocol defines how peers collectively provide user and resource location service in a SIP environment with no or minimal centralized servers. The P2PSIP Peer protocol is run in every peer within the overlay.

The P2PSIP Peer Protocol uses some specific DHT algorithm for the overlay operations (including overlay maintenance and procedures to contact the correct endpoint) that replace the server functions of SIP. For actual session establishment, the conventional SIP is used in P2PSIP. Support for one defined DHT algorithm (might be Chord) is required; other are optional.

The first goal of the P2PSIP WG is to develop a protocol that provides a distribution location service as an alternative mechanism for the RFC 3263 functionality (i.e. locating SIP servers). The location service is to determine the correct destination of SIP requests without centralized servers, using only peers. As was explained earlier, conventional SIP is used in session management. Therefore, the peer protocol only routes the SIP messages to the correct destinations.

The current P2PSIP WG proposal for the P2PSIP Peer Protocol is called “dSIP”, which uses Chord as the DHT algorithm. dSIP uses the conventional SIP with some added extension headers and parameters to transport the needed DHT parameters (such as the DHT overlay name, Peer-IDs etc.). The final P2PSIP Peer Protocol might also include some new SIP method(s) for transporting the DHT parameters (as Hautamäki et al. proposes a LOCSER-method in a P2PSIP draft [p2psip-peer-protocol-00]).

3.2.3 P2PSIP Client Protocol

P2PSIP may also include P2PSIP Client Protocol, which would be used for P2PSIP clients to communicate with the overlay. The existence (and nature) of a P2PSIP client is still under debate in the P2PSIP WG, but if it is used, it may be a “less-capable peer” or just a SIP UA. If a P2PSIP client was a SIP UA, no specific client protocol would be needed, because SIP would be used instead (this is the case in the dSIP proposal). In the absence of a P2PSIP Client Protocol, an adapter peer would be equal to a proxy peer.

If separate clients exist, one alternative is that they do have the ability to add, modify, inspect, and delete information in the overlay, but they are not routing or storing any overlay information. Another proposition proposes that the client may store overlay information on the behalf of its adapter peer. Note that the term client does not imply that this node would be a SIP User Agent Client (UAC). [p2psip-concepts-04]

3.2.4 Overlay Structure

A P2PSIP overlay consists of peers, which collectively serve as a directory service for locating resources (e.g. users, voicemail box or a proxy). Every P2PSIP overlay has a name to identify and separate them from other P2PSIP overlays. The overlay structure is defined and maintained by the P2PSIP Peer Protocol with its DHT algorithm (peers must run the same algorithm within the same overlay). For example, the overlay structure of Chord is explained in Section 2.3.7.1.

Interconnections are defined in the routing tables of every peer and route updates are being made periodically to tolerate churn. In Figure 22, the peer interconnections (gray dash lines) form nearly a full mesh, because there are so few peers in the example overlay. However, as the number of peers grows, interconnections grow only by O(log(N)), where N is number of peers. Therefore, the number of interconnections does not grow nearly as fast as the number of peers grows (which implies a lightweight structure with scalable routing). These interconnections are used to route messages within the overlay, and only O(log(N)) hops are required to route a message to its correct destination within the overlay. This characteristic is inherited from using DHT and causes the session establishment latency to be likely bigger than in CS SIP environment, where the lookup complexity is O(1) due to direct link to a server maintaining the registrar.

3.2.5 Message Routing

Routing in P2PSIP is based on the DHT operations of the DHT algorithm used. In general, it follows the properties of routing in structured overlays (Section 2.3.6).

When a peer wants to send a message within the P2PSIP overlay, it uses a hashed ID of the destination (hashed identifiers are described in more detail in Section 3.2.8). The peer consults its routing table of known peers to discover the closest peer to the target ID it is aware of. When a peer receives a message that is not destined to itself, it similarly consults its routing table to choose the peer closest to the target ID and forwards the

message there (or replies with the next hop information, if iterative routing is used). Either is iterative or recursive routing is being used, the message routes to the final destination hop-by-hop with the help of peers.

3.2.6 Peer Behaviour and Functions

In a P2PSIP overlay, a peer can provide many functions. These functions may be functions that in conventional SIP are provided by servers (such as registrar, location service, proxy, redirect server etc.). The role of a peer depends on the resources it provides, but minimally, a peer in a P2PSIP overlay must participate in the basic DHT overlay operations (i.e. routing and storing some location information, as was explained in Section 2.3.6.2). These obligatory functions and roles make it possible to run the distributed location service to replace the procedures of locating servers in conventional SIP, but also e.g. the registrar server. Other SIP server functionalities can be replaced with the resources the peers can provide (such as proxy and relay).

3.2.6.1 Some Common Peer Roles in P2PSIP

Peers may have many different roles in P2PSIP. We present here some of the most common peer roles. Other roles do exist and new roles and resource types can be developed to a P2PSIP environment, as P2PSIP is inherently open to support many kinds of resources. The resources usually identify the roles of the peers. Most of the resources presented here can be seen in Figure 22.

User Agent (UA) Peer

A peer can be a UA itself. An UA in P2PSIP is analogous to a conventional SIP UA, but requires the support for P2PSIP Peer Protocol.

Adapter Peer (for a P2PSIP Client)

A peer can provide direct access for P2PSIP clients by being an adapter peer. The adapter peer performs the DHT behaviour and “server-like” operations on behalf of the client it supports. This allows the client to interact with the overlay via the adapter peer without being a peer of the overlay. In this alternative, a client wants to take advantage of the overlay, but is unable or unwilling to provide any resources or fulfil the minimal P2PSIP participation obligations (see Section 3.2.6).

The adapter can be implemented by a small software, or it may be a code within a conventional SIP server.

As per the P2PSIP Peer Protocol proposition dSIP ([p2psip-dsip-00]), the adapter essentially acts as a proxy (i.e. adapter peer is a proxy peer in the dSIP proposition) for the unmodified SIP UAs.

A **Proxy peer** and a **relay agent peer** can be used for interworking with conventional SIP domains and SIP UAs in general [p2psip-interwork-01]. Proxy functionality's role is to make the conversion between the conventional SIP signalling and the P2PSIP signalling. Note that SIP UAs outside the P2PSIP overlay are not equal to the SIP UA behind an adapter peer of the overlay. SIP UAs from different domains can only establish (and accept) SIP sessions via proxy (and relay agent) peers. Interworking with SIP (and other) is discussed in Chapter 4.

Bootstrap Peer

A bootstrap peer is a P2PSIP peer that is the first point of contact for a joining peer. A bootstrap peer selects the peer that will serve as the admitting peer and helps in locating it. Therefore, a bootstrap peer only refers the joining peer to an admitting peer. A joining peer uses bootstrap mechanisms (explained in Section 3.3.2) to locate a bootstrap peer. [p2psip-concepts-04]

Admitting Peer

An admitting peer helps a joining peer to join the P2PSIP overlay. The admitting peer will help the joining peer to learn about other peers in the overlay and whatever is required to become a fully-functional peer. This also includes helping the joining peer to establish connections to other peers as appropriate. The choice of the admitting peer may depend e.g. on the joining peer's appointed ID. Therefore, the admitting peer may be the peer "closest" (in the ID space) to the future position of the joining peer in the overlay. The choice of the admitting peer is typically done by the bootstrap peer. It is allowed for the bootstrap peer to choose itself as the admitting peer. [p2psip-concepts-04]

3.2.7 Message Types in P2PSIP

There are (at least) three kinds of message types in P2PSIP. These are Peer/Client Protocol messages, SIP messages and RTP (or other media transport protocol) messages.

Peer Protocol messages are used (between the DHT layer and P2PSIP application layer, see Figure 18) for P2PSIP overlay maintenance and other DHT operations. The current proposal (as per [p2psip-dsip-00]) is that the Peer Protocol uses SIP REGISTER

messages for this purpose. Hautakorpi and Camarillo [p2psip-peer-protocol-00] have proposed an alternative for the REGISTER message usage, because the SIP REGISTER message is not originally intended for other usage than to add, remove and query bindings. Therefore, they propose using LOCSER, a new SIP method (with a XML body) for DHT overlay maintenance operations. Either way, it is assumed that SIP is the protocol used to establish the connections over which the Peer Protocol runs [p2psip-bootstrap-mechanism-00].

Client Protocol messages are not yet issued in the P2PSIP WG, as the existence of a client protocol is still unclear. Therefore, the message types for the Client Protocol are not presented here.

For the actual session establishment (SIP INVITE etc.), conventional SIP messaging is used after the correspondent is located (using the P2PSIP Peer Protocol). This enables interoperability between conventional SIP and P2PSIP UAs, when a P2PSIP proxy (or adapter) peer is used to handle the P2PSIP overlay operations on behalf of the conventional SIP UA. After the session establishment, RTP (or another media transport protocol) is used as in conventional SIP.

Message format details are not yet fixed, so at least the following issues are still to be decided in the WG: whether to use TCP or UDP, whether to use binary or ASCII format for the Peer Protocol and whether to use compressed headers.

3.2.8 Hashed Identifiers and P2PSIP URIs

This section is based on the current proposal of the P2PSIP Peer Protocol [p2psip-dSIP-00] and therefore details may change. However, by using the details of dSIP, the principle of identifiers creation and usage in P2PSIP can be understood.

Every peer and resource in a P2PSIP overlay has an ID that is used to locate it within the overlay. This ID is a hashed value that is calculated using a hash algorithm (i.e. SHA-1 in P2PSIP). The 160-bit SHA-1 algorithm must be supported by the implementations and the IDs of the same overlay must be calculated using the same algorithm. These hashed IDs are used by the DHT layer (in every peer) and Peer-IDs also affect the overlay (as an ID defines the location of a peer or resource within the overlay). Peer-IDs and Resource IDs map to the same key space (i.e. the 160-bit SHA-1 hashed key space). The hashed key space (i.e. the DHT) is distributed, and therefore every peer has a responsibility area

(as was discussed in Section 2.3.7.1 for Chord). Thereby, peers know in which direction to route messages in the overlay.

P2PSIP URIs are human friendly, but they also include the hashed value. P2PSIP URI for a peer includes the hashed value of the IP address (of which it is calculated). P2PSIP URI for a resource includes its hashed SIP URI. Examples of both are shown in the next paragraph.

Hashing Peer-IDs and Resource-IDs

All IDs are calculated using a hash algorithm. The particular DHT algorithm may specify an alternative mechanism for determining Peer-ID. Similarly, a security model may require the assignment of the Peer-ID from a central authority. Otherwise, a peer obtains its ID by hashing a string value assembled from its IP address and port. The IP address for this must be the public IP address of the peer (a NATed peer must use STUN to discover its public IP address). The Resource-ID is obtained by hashing the resource SIP URI. Thus the P2PSIP URI for this resource would be "sip:bob@p2psip.org;resource-ID=723fedaab1" (hash value of the Resource-ID shortened for clarity). Example P2PSIP URI of a peer is "sip:P@10.6.5.5; pID=ed57487add", where "P" stands for peer, and "pID" is the hashed value (also shortened for clarity) of the IP "10.6.5.5". This P2PSIP URI is used in P2PSIP messages. It is more human friendly, but it must include the hashed ID, as it reduces the load of peers when processing messages. However, when messages are to modify the data stored in the overlay, IDs must be calculated for verification (hashed IDs in messages are only for courtesy). Spoofing or addition of incorrect data to the overlay can thereby be avoided.

[p2psip-dSIP-00] proposes a new SIP header DHT-PeerID to be used to express the Peer-ID of the sending peer as well as to identify the name and parameters of the overlay. Example of a DHT-PeerID is "<sip:peer@192.168.1.1;peer-ID=a04d371e>; algorithm=sha1;dht=Chord;overlay=chat;expires=600".

3.3 P2PSIP Overlay Operations

In this section we will describe the common P2PSIP overlay operations.

3.3.1 Enrolment

Before a peer can join an overlay or a resource can be registered, enrolment is required. This process is a one-time process (i.e. not done in every login to the overlay) to obtain

the identifier (ID) and optionally a set of credentials within a P2PSIP overlay. Credentials are used for granting resources and devices the right to function in the system by authenticating the distinguished name (e.g. sip:bob@example.com). Once a user has credentials, peers within the overlay can validate the credentials, so usage of a global PKI is not required. Therefore, the enrolment may also be based on receiving a password. In general, the enrolment service (an enrolment server was shown in Figure 22) defines the set of end users and resources that may participate in the P2PSIP overlay. [p2psip-concepts-04] [p2psip-security-00]

The mechanism for credentials could be a PGP key [PGP.com] or a password (these do not require enrolment server) or a Public Key Infrastructure (PKI) such as a X.509 certificate [ITUX.509]. The enrolment service also defines the policies used in the overlay (e.g. the charging policies, if any, and the subscription renewal time, if required). [p2psip-concepts-04] [p2psip-security-00]

The enrolment service can provide a crypto key pair that may reside even in a SIM card. Therefore, SIM authentication could be used in P2PSIP. This would be a benefit for a Mobile Operator (MO).

3.3.2 Peer Joining and Registration

While servers in conventional SIP are located using DNS (described in Section 2.2.1.3), in P2PSIP the procedures differ from this, as server functionality is provided by the peers. The first step for a node in P2PSIP is to join an overlay. The problem is how the overlay can be found because stable entities (such as a server with a fixed IP address and a DNS name) cannot be assumed. One (or many) peers participating in the overlay must be found in order to be able to join the overlay. A peer that serves as an initial point of contact into the overlay is called a bootstrap peer. There are multiple ways to find a bootstrap peer and those methods can be used successively. As per [p2psip-concepts-04], the address of the initial bootstrap peer may be gained by methods such as

- **multicast mechanism** (within the same local area network)
- **bootstrap server** (central entity to introduce the bootstrap peers)
- **static locations** (e.g. pre-configured address or a web page link)
- **cached peers** (a previous successful joining address)

A joining peer can use e.g. **multicast mechanism** in order to find bootstrap peers on the same local subnet (or multiple subnets joined in the same multicast domain). When using multicast, the joining peer sends a message ([p2psip-bootstrap-00] proposes SIP Option

message) to the pre-defined multicast address that the bootstrap peers listen to. If a **bootstrap server** is used, it introduces a bootstrap peer of the overlay the joining peer wants to join. The bootstrap server may or may not be part of the P2PSIP overlay. Either way, as per [p2psip-bootstrap-00], it does not speak the P2PSIP Peer Protocol. Bootstrap peers are registered (indicating also the overlay they are associated with) with this server that is a SIP registrar and proxy. A joining peer may also use **static locations**, in which the address of a bootstrap peer is obtained by pre-configuration or out-of-band mechanism, such as using a web page. A joining peer can also use address(es) of **cached peers** from the previous successful connections.

The goal of a P2PSIP system is to be independent from any central servers. Therefore, it is preferred (by [p2psip-bootstrap-00]) to try first with multicast, and then to use e.g. a bootstrap server (if available). The different mechanisms might also be used in parallel. After a bootstrap peer has been found, an admitting peer is consulted to allow the joining peer to join the overlay. This admitting peer might be, for example, a future neighbour of the joining peer in the overlay. However, a bootstrap peer may play both (i.e. bootstrap and admitting) roles in cases where this referral is not done.

The Joining Procedure

Figure 23 depicts an example where a peer joins the "chat" overlay using a bootstrap server for locating a bootstrap peer of the "chat" overlay.

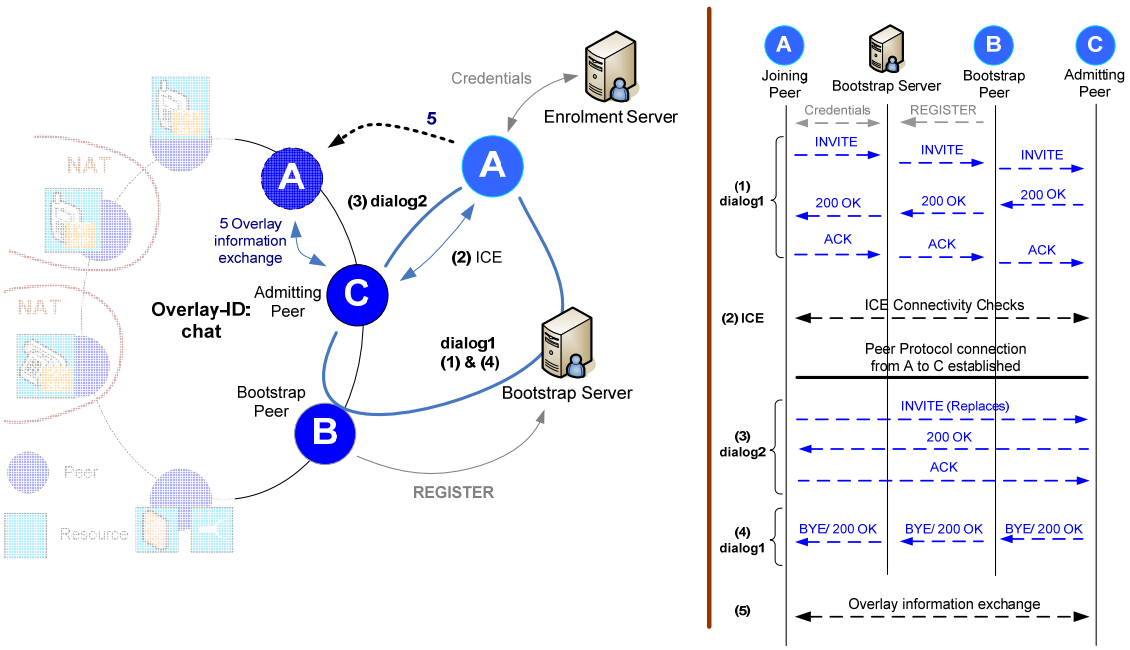

Figure 23 –Peer Joining a P2PSIP Overlay (Using a Bootstrap Server) [p2psip-bootstrap-00]

Firstly, the joining peer needs credentials from the enrolment server (on-time process only). Then the joining peer sends **(1)** a registration message ([p2psip-bootstrap-00] proposes INVITE and [p2psip-dsip-00] proposes REGISTER) to the bootstrap server. The INVITE message (as per [p2psip-bootstrap-00]) is forwarded from the bootstrap server via the bootstrap peer to the admitting peer (this path forms the dialog 1). The bootstrap server also acts as a rendezvous point and helps (together with the bootstrap peer) to establish a direct connection with the admitting peer. After being admitted to join the overlay, the joining peer and the admitting peer perform ICE (Interactive Connectivity Establishment) connectivity checks **(2)** in order to establish the Peer Protocol connection. ICE connectivity check is used to handle NAT traversal, if needed (NAT traversal and ICE is discussed more in Section 3.4). After the connection is established, the joining peer sends a new INVITE message **(3)** to the admitting peer with a "Replaces" header and terminates the first dialog **(4)**. As a result, a new SIP dialog is established and the first one terminated, as the joining peer does not need the help of the bootstrap server and the bootstrap peer anymore. Finally, the joining peer exchanges overlay information **(5)** with the admitting peer in order to become a fully operational member of the overlay. This overlay information enables the joining peer to learn about other peers (i.e. its neighbours) in the overlay. It also enables the joining peer to obtain information about the resources it will be responsible for (as every peer has a responsibility area of the entire ID space). A peer registration includes an expiration time, which indicates how long a recipient (e.g. neighbour) may keep knowledge of this peer. [p2psip-bootstrap-00] [p2psip-dsip-00]

3.3.3 Resource Registration

After a successful peer registration, a resource registration can be done. A resource registration has to be done separately in P2PSIP, as it is not related in any way to the peer registration (which only allows the peer to join the overlay). A UA registration (and a resource registration in general), is analogous to a conventional SIP registration (the only difference is that the registrar role is played by some peer in the overlay). Figure 24 depicts an example of a UA registration. A standard SIP REGISTER message is used and it is sent to the overlay **(1)**. The DHT mechanism of the overlay (in practice the peers) handles the (in this example, recursive) routing **(2)** of the message to the peer responsible for the ID space area, where the Resource-ID of this resource needs to be located **(C)**. The responsible peer **(C)** sends a 200 OK message **(3)** to the peer providing the resource

via the same path. The resource registration is routed similarly to a peer registration. Thereby, the mapping of the resource is at the peer that has the closest Peer-ID to the Resource-ID to be registered. The resource itself is in the peer **(A)** that provides the resource**.**

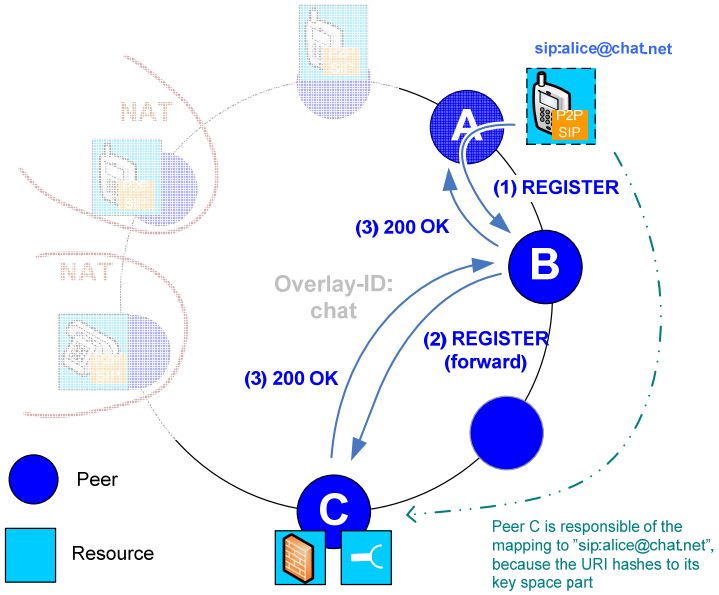

Figure 24 - Resource Registration Procedure (using recursive routing) [p2psip-dsip-00]

Resource registrations are replicated (not shown in Figure 24) to additional peers in order to have redundancy. Redundancy is needed especially to avoid data loss in the event of a peer failure. The replicates are placed at unrelated points around the DHT, as a replica number is added to the resource name, which causes the replica to hash to a different DHT key value. This redundancy also allows minimizing the security attacks of an attacker to compromise more than one registration for a single resource (security threats are discussed more in Section 3.5.3).

Resources can also expire (expire header of REGISTER message is used), so they have to be updated regularly in order to keep the overlay up to date. Thereby, the P2PSIP overlay does not contain broken mappings if e.g. the peer providing some resource is lost. [p2psip-dSIP-00]

3.3.4 Resource and Peer Registration Lookup

Resource queries are constructed as described in Section 10 of [RFC 3261]. [p2psip-dSIP-00] proposes a peer to send a SIP REGISTER message with no Contact header to query a resource (see Figure 25a). This same mechanism can be used to locate a peer

responsible for a particular Resource-ID. A querying UA should not trust to a response, if it cannot verify the response (e.g. to verify the signed registration with a certificate of the user to be searched). Therefore, in absence of a certificate, a replica registration of the resource to be searched should be queried. If the response of the replica indicates the same as the original response, the information is assumed to be correct. This assumption can be done, as the replica location in the DHT is unrelated to the primary registration and therefore a single attacker is unlikely to be able to compromise both entries.

3.3.5 Session Establishment

Session establishment in P2PSIP is done entirely in the normal SIP fashion (i.e. using SIP messages such as INVITE and MESSAGE). However, before the caller can establish the session, the callee UA (or other resource) has to be located. This is done by finding the peer where the callee's information is located (as was explained in Section 3.3.4. and is shown in Figure 25a). After the callee's information has been found, a normal SIP session establishment is done between the caller and the callee's actual location (Figure 25b). This may have to be done using NAT traversal, if the peer, where the resource is located, is behind a NAT. In Figure 25b, because the peer D is behind a NAT, and because A and D do not happen to have a direct connection (as not required initially by the routing table), peer C is used to contact peer D. NAT traversal is explained in 3.4.

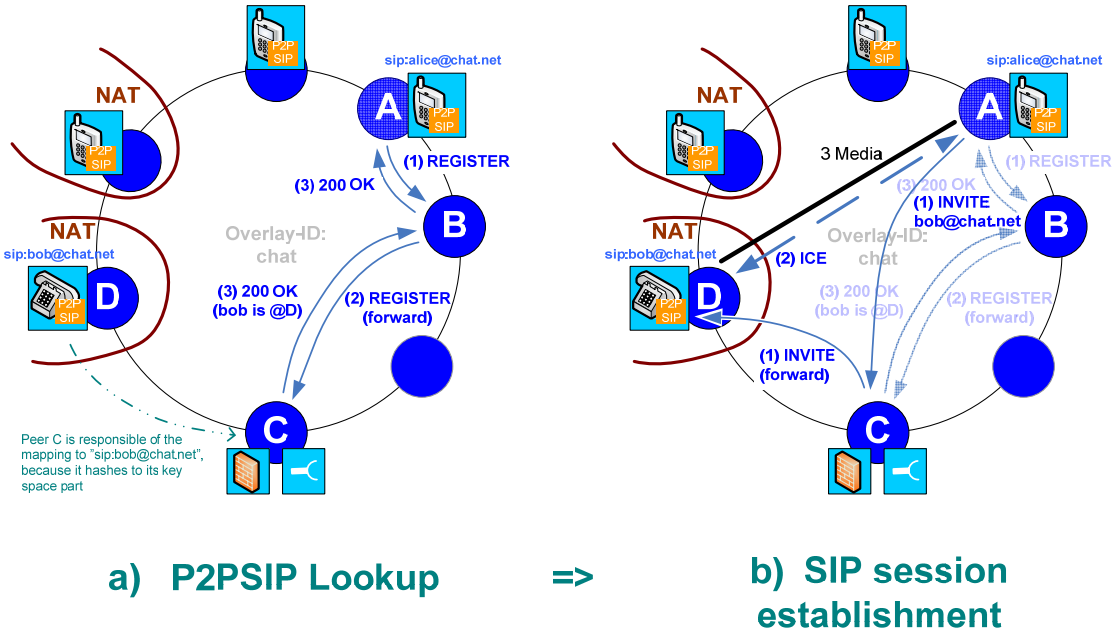

Figure 25 - Example of a Session Establishment in P2PSIP [p2psip-dsip-00]

If the searched resource is available and the lookup returns a valid contact along with a 200 OK SIP message (**(3)** in Figure 25a), the call can be initiated directly between the

UAs (or other resources) using the standard RFC 3261 operation. An INVITE can be also routed through the overlay (as done in Figure 25b), if necessary e.g. for NAT traversal.

3.3.6 Presence

The P2PSIP WG has defined that presence functions are performed using conventional SIP. However, when presence servers are not used, presence information in P2PSIP can be carried over the P2PSIP overlay. [dSIP-00] proposes to use a pair-wise subscription to carry presence information. When the client comes online, it sends a SUBSCRIBE-message over the overlay to everyone on its buddy list (see Figure 26). Peers may use the PeerIDs of their friends' peer as additional routing table entries or neighbours (essentially, cached values) and consult them first.

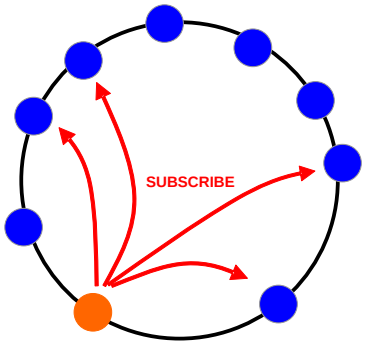

Figure 26 - Presence Update of a User Coming Online

This P2P distribution of presence information is important in order to enable easy implementation of presence capability in a P2PSIP, but it is not necessarily the only solution to implement presence in P2PSIP. SIP/SIMPLE can be considered also in a P2P environment (SIMPLE was introduced in Section 2.4.2).

3.4 NAT Traversal for P2PSIP

Network Address Translators (NATs) are commonly used in the Internet today and they introduce the problem of non-transitive connectivity. NATs make it difficult to contact a NATed node (i.e. a node behind a NAT), because the node has a private IP address which is not directly accessible from the public network. A node (e.g. a computer) behind a NAT can be reached only (without specific manual NAT configurations), if the NATed node has initiated the connection. Therefore, nodes behind a NAT form a closed private network, where nodes can trust each other and have more open access (e.g. enterprise intranets). Benefits of using NAT are also felt in private networks (such as in enterprise intranets), where private intranet IP addresses are independent of public IP

addresses. If the intranet would move (physically) or the used Internet Service Provider (ISP) would be changed to another, the IP block for the intranet IP addresses would change. By using private NATed IP addresses in the intranet, the change of public IP block will not affect the intranet IP addresses.

Some measurements show that even 74% of all computers are located behind at least one NAT [Illuminati]. Locally it is possible that all (or nearly all) computers are behind NATs, as NATs are often used in enterprise and local home networks. Without a previously-established connection with a sender (and a corresponding receiver behind a NAT), 90% of NATs will drop inbound packets [Guha05]. These facts oblige to take NAT traversal into account with P2PSIP (and in general with any SIP or P2P implementation), where peer-to-peer connections are made to form the overlay.

Major reasons for wide NAT usage are the shortage of IP addresses in the Internet and the security benefits of NATs. The former is due to the narrow address space of IPv4 in many countries and the latter due to the fact that NAT also acts like a firewall impeding the connection attempts from the outside.

In the IETF, BEHAVE, MMUSIC and NSIS WGs have concentrated on NAT traversal and e.g. ICE used in SIP and P2PSIP is developed by the MMUSIC WG.

3.4.1 NAT-Induced Problems in Overlay Networks

Straightforward deployment of P2P overlays (i.e. assuming every node would have unimpeded IP connectivity) on IP networks with NATs would cause the overlay's mechanisms to fail due to the following reasons:

Routers in the public Internet consider private IP addresses (used behind NATs) undeliverable. Therefore, messages related to private IP addresses would be discarded.

If multiple private address spaces were included in an overlay, the addresses would conflict and messages could not be delivered to correct destinations.

NATs do not usually allow packets to travel from "public" (i.e. outside the NAT) side to the "private" side (i.e. behind the NAT) before a packet is sent from the private side. Therefore, inbound connections are considered "unsolicited" and dropped.

3.4.2 Ways to Handle NATs for DHT signalling

In a P2P environment especially the unstructured P2P file sharing networks (and Skype) have managed to implement good NAT handling procedures, mainly by using superpeers. Superpeers can be used to provide connectivity to a DHT overlay for NATed peers by using superpeers as proxies for the NATed peers. Also standard protocols such as STUN [STUN] and ICE [ICE] can be used to handle NAT traversal (i.e. to do "NAT-hole-punching"). STUN allows applications to discover the presence and type of NATs and the public IP address that the NAT has allocated to them. ICE is used to determine how to use these protocols to establish best connectivity between two peers [Bryan06]. Therefore, ICE is used for session establishment between two peers willing to communicate together and it does not require any network device configuration. ICE also allows end-to-end encryption to be used.

NAT traversal (e.g. with STUN) is more successful with UDP, and more difficult with TCP. However, [Guha05] estimates an 88% success rate for TCP and a 100% success for UDP, when certain common types of NAT devices are present. The P2PSIP WG has not yet defined whether to use UDP or TCP for the P2PSIP Peer Protocol.

P2PSIP WG has not decided which mechanism to use to handle NATs either, but NAT traversal will in any case be taken care of in P2PSIP. In the following subsections we present the two main proposals for P2PSIP to handle NATs for P2PSIP overlay peer connections defined in the P2PSIP drafts.

Other NAT traversal mechanisms that could be used in P2PSIP are introduced in [p2psip-nats-and-overlays-01]. Those are Universal Plug-n-Play (UPnP), Application Level Gateways (ALGs), Session Border Controllers (SBCs) and manual configuration. They are not discussed in detail here (as they do not used in the current P2PSIP drafts), but can be studied from [p2psip-nats-and-overlays-01] (however, SBCs will be shortly presented in Section 5.2.3.4).

3.4.2.1 Using Persistent Connections Between Peers

Peers that are behind NATs can fully participate in the overlay with a "fully distributed" solution, where every peer has equal importance and an equal role. Thereby, in this scheme, peers behind NATs can be contacted via other peers that already have a connection with this NATed peer. Thereby, the NAT-induced problems presented in Section 3.4.1 can be avoided. These already existing connections can be used for

relaying messages and to make new (Peer Protocol, SIP or RTP media) connections. Each peer has a small number of P2PSIP Peer Protocol connections to other peers (partial mesh). [p2psip-NATs-01]

New connection using ICE can be made with the procedure presented in Figure 27.

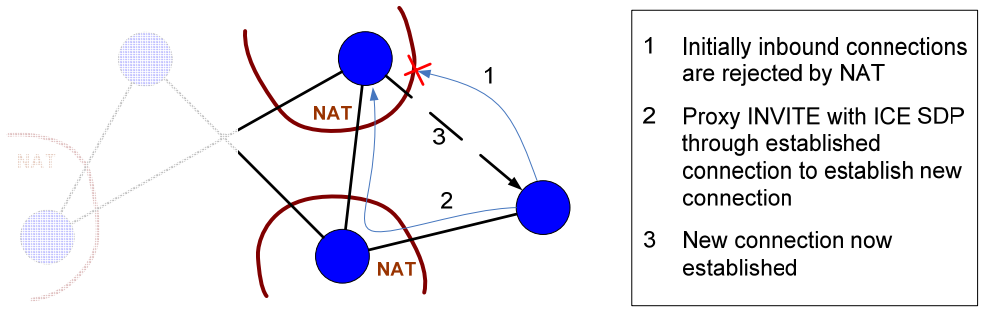

Figure 27 - Using ICE to Open New Connections

This approach does not require a public IP address for joining the overlay. This is a benefit when compared to the superpeer-model (in the following section), as no certain number of superpeers with public IP address is needed for efficient overlay operation. However, this fully-distributed model may require up to O(log (N)) hops for the routing of messages. “Keep-alive” messages are required to keep the connections alive, as NATs usually closes these opened ports after an idle time. [p2psip-NATs-01]

3.4.2.2 Using Superpeers

A hierarchical topology of superpeers can be used also for NAT traversal. Some peers are promoted to be superpeers, while other peers are ordinary peers. Superpeers are chosen from the peers with public IP addresses and other “good” properties, such as high availability, high bandwidth and computing power, are highly desirable. Other peers (usually peers behind NATs) are ordinary peers. Figure 28 shows a P2P overlay with superpeers **(S)** and ordinary peers **(O)**. Superpeers usually have connections with many ordinary peers and with some superpeers. Ordinary peers initiate the connection establishment with superpeers. This makes it easy to traverse any intervening NAT and two peers are only three hops away in the overlay. In the P2PSIP context, superpeers may be called unrestricted peers, and ordinary peers may be called restricted peers (not yet confirmed in the P2PSIP WG). [p2psip-NATs-01]

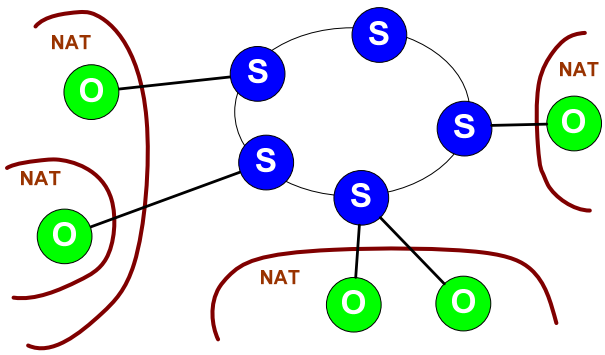

Figure 28 - The Superpeer Solution [p2psip-NATs-01]

As was explained in Section 3.4.1, this kind of solution is very popular and simple and it is widely used in the P2P file sharing networks. This scheme is very efficient, but requires a sufficient amount of peers with public IP addresses to operate as superpeers. It also concentrates the network load on a small percentage of the participating nodes and cannot be used in networks without publicly addressable peers.

The proposal of using superpeers also includes a property, where one of the many peers behind the same NAT could be elected to be the representative peer for connection with peers outside the NAT. This approach would minimize the effort required for NAT traversal and keep-alives. [p2psip-NATs-01]

3.4.3 Ways to Handle NATs for Media

When a SIP session is being established between the correspondent P2PSIP peers, NAT traversal mechanisms of conventional SIP are used. As the actual SIP session establishment in P2PSIP is analogous to that of conventional SIP, the session establishment procedure does not differ in these two environments. Therefore, ICE with SIP is reused to establish a SIP dialog between the corresponding peers. NAT traversal techniques for media transport (usually RTP) are also performed the same way as in the conventional SIP. Proxy and relay peers may be used, but after they are located using the lookup mechanism of P2PSIP, their usage is also analogous to that of conventional proxy and relay servers. NAT traversal for SIP media is described in detail e.g. in [Schwartz-05], where the NAT traversal for conventional SIP signalling is presented.

3.5 Security

P2PSIP has many security issues that have to be taken into account. A P2P environment itself involves many security threats that a client-server (CS) environment (e.g. a conventional SIP environment) does not have, because a CS environment can use

centralized servers that can be trusted. Peers in a P2PSIP overlay are required to handle most of the security themselves (but yet automatically by the P2PSIP). However, some centralized entities are desired. These are an enrolment server (see Section 3.3.1) and a bootstrap server. An enrolment server is required if a PKI is wanted, e.g. for big P2PSIP implementations, and bootstrap server helps in finding an initial bootstrap peer. They both improve the security of the P2PSIP overlay. P2PSIP must offer security models that serve both small scale implementations of few people and wide implementation of millions users. Shared secret (i.e. a password) is applicable to the former and PKI to the latter (as shared secret has scalability issues). Both approaches make use of the Identity digest-string header of [RFC 4474] (with small modifications). Shared secret uses HMAC-SHA1 [RFC 2104] hash of the digest string in the SIP identity field, and PKI is with e.g. a X.509 certificate. [p2psip-security-req-00] [p2psip-dsip-security-00]

[Cao06] discusses how to provide secure services in P2P communication networks, where e.g. voice mail service is prone to be compromised by the third party.

We present here the security requirements as well as the proposed (by P2PSIP WG) solutions for each of them. After the requirements, general security threats concerning P2PSIP are identified. These threats and requirements are as per [p2psip-security-req-00]. In general, the proposed solutions are simplified by assuming that all the participating peers have unique identities and credentials. Also is assumed that stored overlay data will be authenticated by the storing peer. The mechanisms to implement these are out of scope of P2PSIP WG, but existing standardized mechanisms are re-used.

3.5.1 End-user Requirements

User wants to interact with other users and resources in a secure and reliable way in a P2PSIP network. Therefore, a P2PSIP system must fulfil the following aspects.

Certainty of user identity

Users must be able to trust the corresponding resource or user to be the one they believe it is (and not a malicious one).

Proposed solutions

- Users/resources are required to have credentials issued by an enrolment server, or a shared secret can be used, if PKI is not used.
- Identity can be validated from SIP identity header.

Easy and secure enrolment to the P2PSIP system

Proposed solutions

- Use of an enrolment server that can be trusted (or using a pass phrase in small networks).

Secure and reliable lookup and discovery of resources

User must trust that intermediate routing peers cannot interfere (e.g. by modifying, inserting or eavesdropping) signalling, as these peers may be untrusted peers. Also the resources are needed to be authentic.

Proposed solutions

- Hashed IDs are used to hide the signalling entities
- Resource tickets are used to enable a querying entity to validate the resource
- P2P TLS connections should be used to achieve authenticated end-to-end security [sip-tools-01]

Secure and reliable end-to-end multimedia communication

Proposed solutions

- SRTP as per [RFC 3711]. SRTP is existing security standard for conventional SIP to secure RTP (RTP is used to transport multimedia data) connections. Key management without PKI infrastructure could be done with ZRTP [zimmermann-zrtp-03], which is an extension to SRTP and enables users to authenticate themselves to each other by voice.[sip-tools-01]

3.5.2 System Requirements

Fulfilment of these aspects assures the proper function of a P2PSIP system and that a user gets proper service.

End user enrolment

A P2PSIP system should require enrolment and thereby peers can be granted or denied to join a P2PSIP system.

Proposed solutions

- Use of an enrolment server or shared secret (same as in Section 3.5.1).

Data access

Data stored in a P2PSIP system must be authentic and its integrity must be assured. Therefore, the possibility for unauthorized or invalid insertion of Peer-IDs or Resource-IDs must be prevented. Security requirements for the DHT implementation should be minimized.

Proposed solutions

- ID Namespace is protected by using ID hashing and cryptography to validate the hash

- A peer must not perform any action that changes state or returns information stored in the overlay without validating the Identity signature of the request message. For response messages this applies to any action.

Shared secret scheme does not protect from attacks on resources if a malicious peer has been able to join the overlay (i.e. has discovered the shared secret).

Detection and rejection of badly behaving nodes

Badly behaving nodes should be detected and excluded from the P2PSIP system.

Proposed solutions

- No solutions have been proposed by the WG.

Minimized dependence of centralized servers

Proposed solutions

- Server functions provided in conventional SIP are decentralized, but especially for the enrolment service, it is desirable to use a centralized server.

Preference of existing security mechanism

Proposed solutions

- Existing standardized solutions are used as much as possible, as they are usually well designed and they have proven reliability and functionality.

3.5.3 Security Threats

These following security threats concerning P2PSIP are solved (or at least mitigated) by fulfilling the previous requirements. They are presented to identify why the requirements are adduced.

Replay Attacks

Replay attacks are network attacks where a valid data transmission is maliciously or fraudulently repeated or delayed (e.g. to steal password for identity masquerading). This involves both the enrolment process and modification of the P2PSIP resource records in a P2PSIP overlay.

Message Insertion, Modification, Deletion

An attacker might be able to alter the messages being exchanged between two endpoints. If this kind of attack happens, the integrity of the P2PSIP system (including the enrolment procedure and data stored in the P2PSIP overlay) becomes compromised.

Man-in-the-Middle

Man-in-the-middle (m-i-m) attacks may occur in pairing and authentication procedures. Such an attack may lead to masquerading as well as to data leakage and modification. In

order to avoid (or at least mitigate) such attack, authentication is needed in the process of enrolment and when P2PSIP resource records are being modified in a P2PSIP overlay.

Offline Cryptographic Attacks

A system could be broken by breaking cryptography used in the system. However, if state-of-the-art (i.e. best available) security methods are used, this kind of attack is less likely than e.g. finding and exploiting software errors and vulnerabilities.

Unauthorized Usage

Without an enrolment system (or with a weak one), a malicious peer is able to attack the P2PSIP system from within the system. Therefore, adequate authentication and authorization mechanisms are needed to avoid unauthorized usage of the system.

Inappropriate Usage

The nature of distributed storage of P2PSIP resources may provide the possibility to use it inappropriately. Individual services of a P2PSIP system (messaging, real-time communication) have their respective security threats (e.g. spam, viruses etc.), but they are out of scope of this thesis.

Denial of Service (DoS)

If a P2PSIP system uses weak authentication in the DHT or the system is fairly open, a denial of service (DoS) attack can be considered possible (or even probable). One such attack is Sybil attack [Dinger06], where an attacker may obtain a large number of peer identifiers in order to dominate (or possibly control) the P2P network. This can lead to bringing down the system, or at least reduce the robustness of the system, as resources cannot be accessed. However, a P2PSIP system would need to be infiltrated with a fairly big number of peers, as the resources are distributed and their storing nodes are hard to predict. Redundancy used in P2PSIP makes also this kind of attack more difficult to affect the robustness.

Communication Security Threats

The communication security is an issue mainly in the enrolment process and in the communication between a client and its correspondent peer. In other places it is assumed to be handled by the actual SIP service implementation, and P2PSIP only adds the means for providing the communication endpoints a shared key for further security needs. The DHT facility and communication is unprotected (i.e. the DHT layer does not use encryption), but the stored data in the overlay is protected.

3.6 Possible P2PSIP Use Cases

P2PSIP has many different possible use cases, but we present here only the general use cases as per the P2PSIP draft [p2p-usecases-00] that are the most relevant for mobile operators. They are categorized according to the environments they apply to. More specific potential use cases of P2PSIP for mobile operators are presented in Chapter 5 along with the discussion of the mobile operators' role in P2PSIP. The following use cases (and others mentioned in [p2p-usecases-00]) are summarized in Table 1 of the Appendix A.

3.6.1 Global Internet Environment

Global Internet has no central administration or network control on a global scale of the physical network. Thereby, two remote nodes belonging to different administrative domains in the Internet can connect and communicate together. Most of the well-known P2P file sharing overlay networks are operating in this environment.

- **Public P2P VoIP Service Providers**

A public P2P VoIP service provider is a novel service provider that provides voice (and usually other) services in the Internet by exploiting P2P networking instead of client-server infrastructure. Skype is a very good example of this kind of service provider. However, Skype is a proprietary system and is not a pure P2P system, as it uses some central servers e.g. for login.

For a public P2P VoIP service provider, the major benefits are reduction in infrastructure and operational costs. P2P networking facilitates this, as it can (at least partly) replace server infrastructures. Therefore, less complex systems can be implemented to provide VoIP services.

This kind of use case is a threat for mobile operators, as P2PSIP facilitates to provide rivalling VoIP services. However, a mobile operator can potentially also find this scheme beneficial at some level. Mobile operators' role is discussed in Chapter 5.

- **Open Global P2P VoIP Network**

In an open global P2P VoIP network anyone can easily join and leave the network and there are no central authority (such as a single service provider) limiting or controlling the usage. This kind of network resembles the Internet itself, as everyone can reach

anyone else, and any device supporting the standard can be used. In such open system, the protocols used should be based on open standards.

P2P networking makes it easier to use own private or open P2P networks for VoIP and other multimedia, as P2P networks can run without server infrastructures that requires some centralized management. However, as in the previous use case, a mobile operator can potentially also find this scheme beneficial at some level. These are also discussed more in Chapter 5.

- **Presence Using Multimedia Consumer Electronics Devices**

As more and more multimedia consumer electronic devices have network connectivity, they could benefit of easily deployed P2P presence. VoIP may not be needed on some of these kind of devices, but presence, which enables instant sharing of multimedia content (such as videos, pictures etc.), will be highly appreciated.

A mobile operator could find this beneficial e.g. as a supplementary feature in its services. This use case is discussed more in Section 5.2.4.4.

3.6.2 Security Demanding Environments

There are situations where, despite having connectivity to the Internet or even e.g. to SIP proxies in a SIP infrastructure, users may not like to use the infrastructure. Reasons may be security concerns or that users may not be allowed to use the infrastructure.

- **Impeded Access Environments**

Some users may have impeded access to communicate with other users. This may be done by ISP to block e.g. a PC-to-PC VoIP communication. The ports commonly used by these kinds of services may be blocked by ISPs in order to assure the usage of the communication services of the ISP. A fully decentralized P2P system cannot be completely disconnected without removing the connectivity at the basic Internet level.

This is not regarded as a beneficial usage of P2P for a mobile operator, because this use case implies that a user can use other services from the operator's network that the operator does not want to be used. Therefore, it can be regarded as a threat to mobile operators.

3.6.3 Environments with Limited Connectivity to the Internet or Infrastructure

Where there is no physical network available for stable deployments of client-server SIP or other real-time communication systems, a P2P approach may be the only feasible solution. Even if there might be a physical network, it may be unstable or its usage might be expensive. Examples are isolated wireless ad-hoc network with limited Internet connectivity (or not at all) like outdoor public events, emergencies, battlefields or if there is only an expensive satellite connection available. In these cases a big advantage is to use easily deployable (no manual configurations needed) and localized communications.

- **Ad-Hoc and Ephemeral Groups**

In some situations a group of individuals meeting together, e.g. in a conference, may want to collaborate using an ad-hoc connectivity. These are usually ephemeral situations, so minimum (ideally zero) configuration is desirable. Using P2P communication, no need of Internet connectivity is needed, as long as all can interconnect their devices mutually.

This kind of use case as such does not imply beneficial usage for mobile operators, as users would not be using mobile operator's services for collaboration. If a mobile operator wanted to try to exploit this scenario, it could e.g. enable such functionality into its VoIP service as a backup system in the absence of Internet connectivity provided by the operator.

- **Extending the Reach of Mobile Devices**

A network of mobile devices can relay traffic between themselves to reach a base station, as long as at least one of them is connected to a base station. Thereby a mobile device could reach a base station even if the base stations would be out of direct reach. A system might make this feature optional for standard communication and mandatory for emergency calls.

This use case is discussed more in Section 5.2.3.5.

3.6.4 Managed, Private Network Environments

A corporate network or a school campus network may want to deploy a P2PSIP environment to achieve various goals. These goals could be such as cost and management overhead reduction, scalability, and system robustness. Client-server SIP

would be possible in these environments, but a P2PSIP could be used as well instead, or as a complementary system.

- **Serverless or Small Scale IP-PBX**

Small organisations without centralized IT support may want to integrate communication systems easily with self-configurative and self-organizing systems that should offer a feature set similar to those of client server type PBX (Private Branch eXchange) systems. Important features may be PSTN connectivity, call transfer, voice mail, IM or conference call service. This type of commercial products already exists in the market.

Even though this kind of use case would reduce using similar communication services of mobile operators, it would still enable the provision of some services. For example, PSTN connectivity requires operator involvement and calling to PSTN or PLMN networks also generates revenues for the corresponding operators.

- **Failover for Centralized Systems**

A traditional centralized SIP server, such as used in an IP-PBX, forms a single point of failure of an otherwise fault-independent network. Relying on P2PSIP as a backup to the centralized server allows the communications system to continue functioning normally in the event of planned or unplanned service interruptions of the central IP-PBX.

This use case is discussed more in Section 5.2.3.2.

- **P2P for Redundant SIP Proxies**

The benefits of P2PSIP for service providers could be to enable a farm of proxies passing resources (i.e. user registrations or other call information) with as little configuration (implies overlay self-organization) or traffic as possible. Ideally, minimal configuration between the devices should be required for redundancy and exchange of information.

This use case is discussed more in Section 5.2.3.3.

3.7 Summary

The P2PSIP WG in the IETF is developing protocols and mechanisms under the name of P2PSIP for the use of SIP without deployment of centralized SIP server architecture. P2PSIP aims to use simple SIP, which is only the native SIP of a rendezvous service to discover endpoints and to establish a multimedia session between them [sip-tools-01]. Therefore, all the applications are placed in the endpoints in P2PSIP and not in the

network. This enables to avoid the vast amount of SIP extensions that are used to produce network-based applications.

Establishing and managing sessions in P2PSIP is principally handled by peers using the structured P2P overlay architecture instead of the client-server architecture. The conventional SIP uses DNS queries (as per [RFC 3263]) to solve the SIP URIs in order to find the next hop towards the correspondent user or service. In P2PSIP this procedure is replaced with a mechanism of storing the hashed SIP URIs in the structured P2PSIP overlay, from where they can be searched to resolve the direct location of the endpoint. The location service and registrar server functionalities of the conventional SIP are also handled by the overlay in P2PSIP by distributing the SIP server functionality among the peers. Peers can collectively handle message routing and maintain the distributed directory service of registered UAs and services within the overlay. However, the actual SIP session establishment is done as in conventional SIP (while the routing and location discovery is handled by the P2PSIP overlay).

NAT traversal has to be taken care of in P2PSIP, as the majority of computer in the Internet are behind NATs and as P2P connections have to be made directly between peers. Existing NAT traversal techniques of the conventional SIP are reused in P2PSIP. Also security issues have to be taken care of in P2PSIP, as peers' resources are exploited for the overlay maintenance and operations (as in P2P networking in general). Therefore, peers' resources (such as data storage and computing power) should be secured that they could not be used for wrong purposes (e.g. to attack someone's computer).

P2PSIP has many benefits compared to the conventional SIP architecture. Running a P2PSIP overlay does not require centralized servers or Internet connectivity (however, some servers can be used to enhance the functionality of a P2PSIP overlay). Server independence implies that no third party is required to run the infrastructure formed by peers. The maintenance costs are thereby reduced. P2PSIP networks are distributed systems that can be scalable (by supporting millions of users) and fault-tolerant (due to the decentralization). P2PSIP is applicable to be used in a VoIP environment as well, even though it is not intended to replace the existing TDM networks (e.g. 2G/3G). The downside of the P2PSIP approach (when compared to a client-server architecture and especially to 2G/3G networks) is the latency in initiating a call, as a P2P network usually requires log(N) hops to reach the callee. However, this is a necessary trade-off to obtain the benefits identified above.

4 P2PSIP Interworking

A P2PSIP network can be interoperable especially with a conventional SIP domain, but potentially also with other networks. When introducing a new protocol or an entire system, its interworking with existing systems is important, since the existing systems will not be immediately replaced by the new system (even if it was substantially superior to them). Interworking usually implies better acceptance and wider applicability for new systems and protocols. Even the proprietary Skype network has not remained only a closed proprietary system, but has started to interoperate with other networks. Skype has, for example, introduced gateways for interworking with telephony networks in order to add more value by allowing users to call regular phone numbers from the Skype network.

This chapter introduces interworking cases for P2PSIP with the main focus on interworking of P2PSIP with conventional SIP and IMS. Also interworking with heterogeneous P2PSIP overlays is discussed in more detail.

4.1 Conventional SIP

UAs registered in a P2PSIP overlay network can interwork with those in conventional SIP networks. However, as P2PSIP and conventional SIP are not directly interoperable, some peers are required to provide resources for interworking. There are two additional (logical) elements used in P2PSIP for full interworking with conventional SIP. These are a proxy peer (i.e. gateway functionality for SIP signalling) and relay peer (i.e. gateway functionality for media session traffic). Connectivity with public domains requires some peers to be able to communicate with public hosts on the Internet. Furthermore, they need to be registered in the public naming service (DNS) for a fully qualified domain name (FQDN), which uniquely identifies the overlay they participate in. [p2psip-interwork-01]

Overlays such as the one in Figure 29, which have resources for both relaying data and routing SIP messages to and from public servers, can be considered equivalent to conventional SIP networks when viewed from the outside. Therefore, with this kind of setup, the P2PSIP overlay is transparent and fully interoperable with the conventional client-server SIP.

Figure 29 depicts an example where a conventional SIP UA (Carol) calls a P2PSIP UA (Alice) that has a P2PSIP address. The domain of this P2PSIP address has to have a FQDN (in other words, a global DNS name).

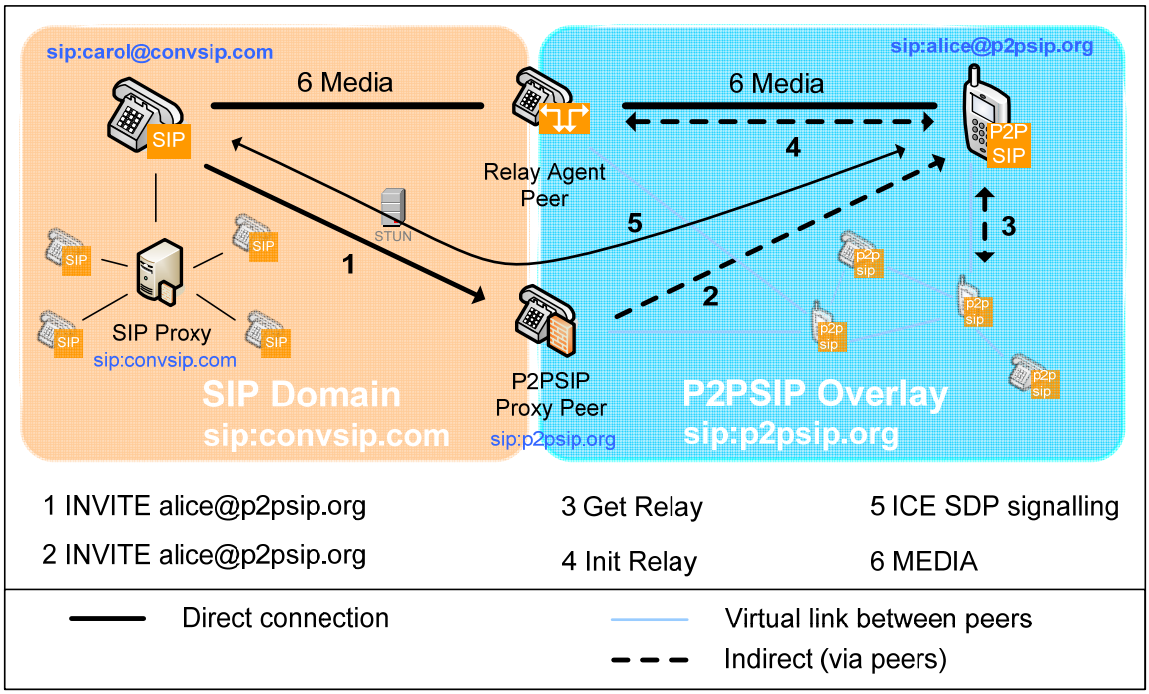

Figure 29 - Call Flow Between SIP and P2PSIP Clients [p2psip-interwork-01]

The messaging flow of Figure 29 goes as follows:

Carol (sip:carol@convsip.com, where "convsip" stands for "conventional sip") wants to call Alice (sip:alice@p2psip.org), who is registered in a P2PSIP overlay. Alice has a FQDN in order to be reachable for UA outside the "p2psip.org" overlay. Carol performs a conventional SIP location procedure (RFC3263) in order to find the address of one (or more) proxies for the domain sip:p2psip.org. Carol sends **(1)** the SIP INVITE to the proxy peer of the P2PSIP domain sip:p2psip.org (Carol's UA could also send the INVITE indirectly via the SIP proxy). The P2PSIP proxy peer forwards **(2)** the INVITE-message to Alice (sip:alice@p2psip.org) after using the DHT search mechanism defined in Section 3.3.4 in order to find the location of the Alice's UA. However, this procedure of finding the resource (i.e. Alice's UA) is not shown in the figure. Once Alice has received the INVITE, she accepts it and searches **(3)** a relay agent peer for media relaying from the overlay. After Alice has received the location of appropriate relay agent peer, Alice initiates the relay **(4)**. Once Alice has initiated the relay successfully, she negotiates the media session **(5)** using ICE (for NAT and firewall traversal), if Carol has declared to support it. This is done via the proxy peer (and may require a STUN server) in order to negotiate and agree the most appropriate session parameters. Finally, Alice and Carol can start the media session **(6)** using the relay agent peer for the media connection. [p2psip-interwork-01]

Another possibility for being reachable outside a P2PSIP overlay is that a user (Alice in the above example) is registered both in a P2PSIP overlay (p2psip.org) and through proxy peer(s), with a conventional SIP network (sip:convsip.org). The conventional SIP URI can be used to contact the P2PSIP user, as the conventional SIP proxy routes the messages to the proxy peer of the overlay, which knows the exact location of the user (Alice).

4.2 IMS Network and its Services

The IP Multimedia Subsystem (IMS) allows merging 3G cellular networks and the Internet. The benefits of IMS are Quality of Service (QoS), charging and integration of different services. With charging we mean that there can be different rates for different traffic, such as VoIP, IM, and surfing.

As the IMS does not depend on the circuit-switched domain, other than 3G devices within the IMS network are interoperable with the domain. In addition to this, as IMS uses SIP for session control, P2PSIP can be interoperable with IMS. Session control includes the operations to create, modify and terminate multimedia sessions.

If IMS would be let to interwork with P2PSIP networks in a way that P2PSIP overlay user could access IMS services and terminals, operators could make more profit by providing wider usage of IMS services for P2PSIP users. For example, a user having a 3G cell phone and a laptop could use the same services of IMS with his laptop (with P2PSIP) as he can with his 3G cell phone. IMS services could be offered also for other users (that operator's subscribers) for additional fee.

The service of big interest for a P2PSIP user is the gateway access to PSTN and PLMN (mobile network) networks. This kind of service has been already provided for Skype network users (even though not with IMS, but with its own system gateways). P2PSIP users could be interested to use also other IMS services (see Figure 30 for examples) that they find appealing. Use cases of MOs to provide a gateway to its networks is discussed also in Section 5.2.1.4.

Figure 30 depicts an IMS-P2PSIP interworking scenario, where a P2PSIP device outside the IMS (but could be as well inside the IMS) can access IMS services and terminals via the IMS. Access to the IMS can be also from a P2PSIP terminal using a broadband connection of the same operator, when the interoperability and QoS issues can be better addressed. QoS functionality of IMS can be used to interwork with other IMS networks

as well for P2PSIP, as QoS-guaranteed IMS interconnection can be done with IPX (IPX was presented in Section 2.1.6).

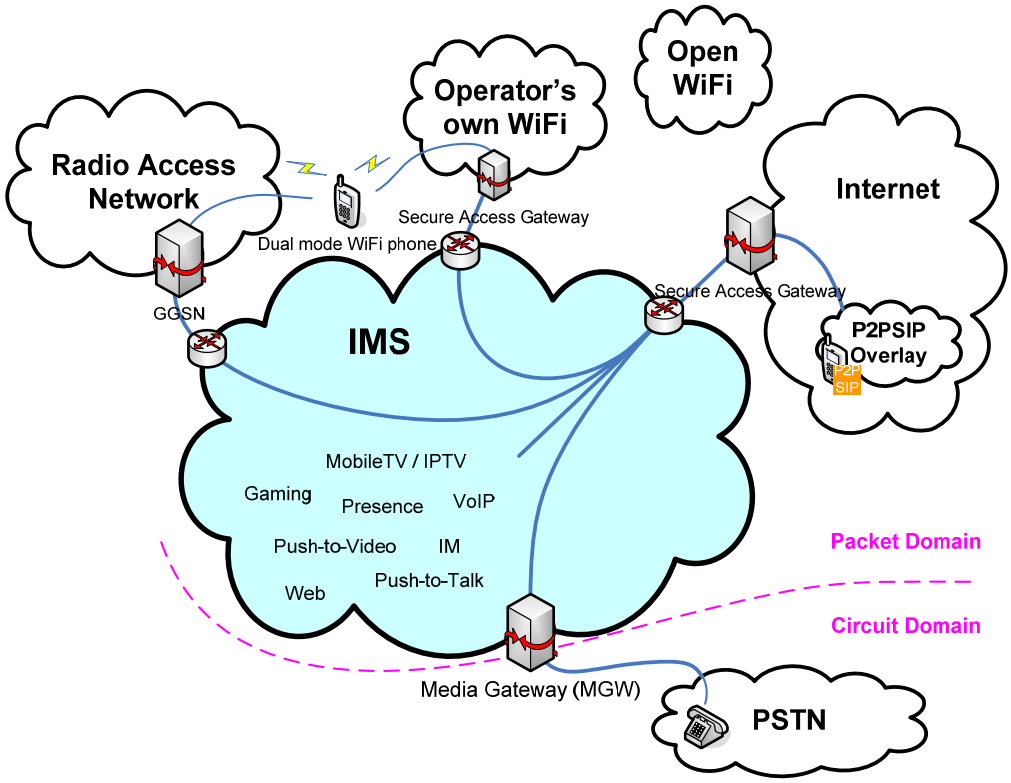

Figure 30 – P2PSIP-IMS Interoperability

The usage of P2PSIP signalling within the IMS infrastructure is presented in Section 5.2.3.4, where MO's roles for IMS with P2PSIP are identified.

P2PSIP could also be interoperable with other IMS networks, such as DOCSIS and TISPAN. These networks were presented in Section 2.1.5.

4.3 Other P2PSIP Networks

P2PSIP overlays may use a different DHT algorithm, as it is not required to use only one DHT implementation (e.g. Chord), but others as well (while supporting one base DHT). As conversion is required between P2PSIP overlays running different DHTs, some kind of interworking scheme is needed. We present here two ways of doing this: using hierarchical overlay among gateway peers and peers supporting multiple DHTs.

4.3.1 Hierarchical P2PSIP architecture

Heterogeneous interworking among different P2PSIP overlays could be implemented by using upper-level overlay of some peers as gateway (or proxy) peers. Such peers would preferably be superpeer-like powerful peers in order to have stable and efficient

gateways in the overlays. [p2psip-hier-arch-00] proposes a hierarchical P2PSIP structure by using a "global P2P overlay" that interconnects the gateway-peers (elected from each overlay) using an upper-level overlay. Figure 31 depicts this scenario. Such hierarchical architecture allows for interconnectivity between heterogeneous overlays, and low signalling overhead as well as easy management can thus be achieved [p2psip-hier-arch-00].

This scheme could also include the possibility for interworking with conventional SIP domains (as depicted in gray in Figure 31). This gateway server could comprise the same kind of proxy peer or gateway peer that are used in Section 4.1 (or with other networks discussed in this chapter).

This scheme would be analogous to the IPX scheme, where IPX supports interworking also with different kinds of operators (and not just MNOs like in GRX).

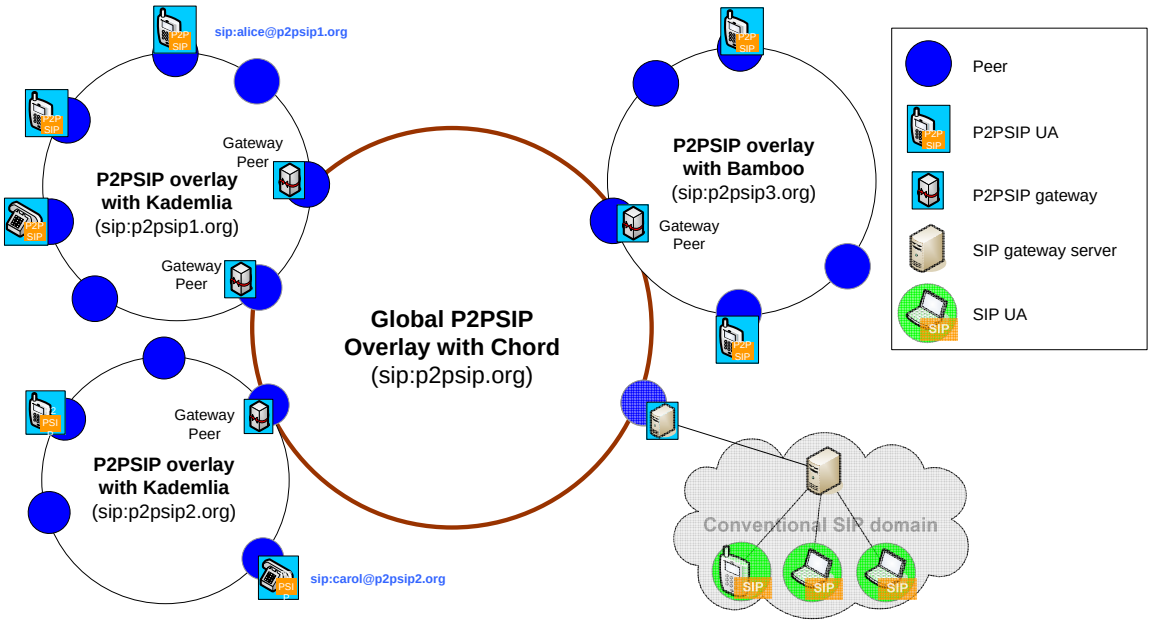

Figure 31 - Hierarchical interworking with heterogeneous P2PSIP overlays

Gateway peers are involved, if a UA (e.g. with a P2PSIP URI sip:carol@p2psip2.org) wants to call someone within another overlay (e.g. with a P2PSIP URI sip:alice@p2psip1.org). If the SIP URI implies that the destination SIP URI is not within the same overlay, the caller peer asks the overlay (using the P2PSIP resource lookup procedure) the location of a gateway peer (there may be multiple) for other P2PSIP overlays. After receiving the location of the gateway peer, the caller sends the original INVITE message there. From the gateway peer the INVITE is routed via the global P2PSIP overlay to the correct overlay (of the respective domain). The correspondent

overlays may be using different DHT algorithms, and therefore the gateway peers are required to support the DHT algorithm of the global overlay too.

This scheme assumes that one domain (e.g. p2psip1.org) could be used only in one overlay, because using multiple overlays for one domain would make it more complex (e.g. how to find the correct overlay for a user). Nonetheless, enrolment servers are in essential role, as they must be used to assign the domain names for the overlays.

This scheme does not restrict a user to register to multiple overlays. If a user registers a peer in multiple overlays, it will not have any proxy or representative obligations: it would be merely a regular peer in both overlays without any interconnection functionality. However, the P2PSIP URIs would be of different domains, as there is only one overlay per each domain in this scheme.

4.3.2 Inter-Domain Registration

Another way to implement inter-overlay interworking among P2PSIP overlays would be to use inter-overlay resource registrations. This means that peers cand register to multiple overlays in order to create bindings and to interconnect the overlays mutually. However, in this case the interconnection would be without any higher-level overlay. Thereby, they could freely act as representatives for the overlays without the need of dedicated proxy peers. By using peers connected in multiple overlays as representatives for the overlays, other peers could communicate with those overlays without needing to be individually registered to them. The representative peers registered in multiple overlays are naturally required to support the DHT algorithms of the correspondent overlays. Additionally, they could be required to have adequate credentials in order to be allowed to register to these domains, if admission control is used (admitting peers were described in Section 3.2.6.1).

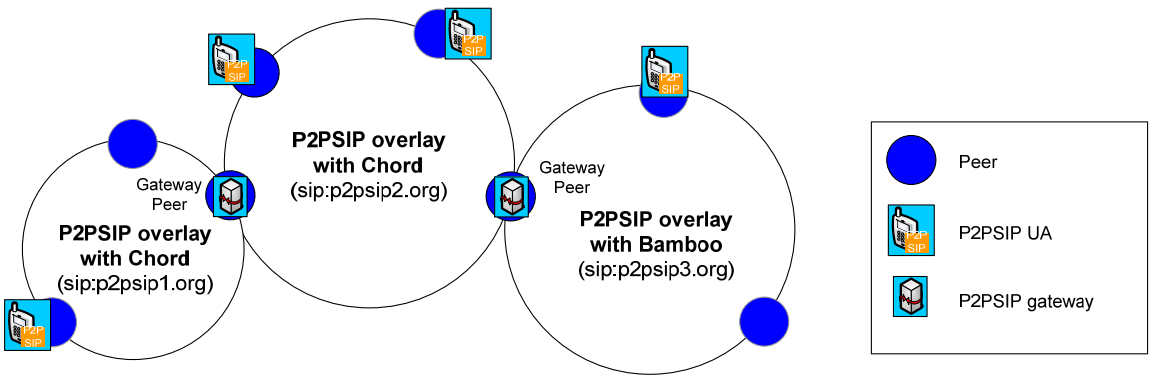

Figure 32 – Inter-Domain Registration

This scheme also assumes that there is only one overlay per domain.

Especially in large scale implementations, the use of this kind of a scheme would lead to some kind of a mesh between the overlays. It would possibly also incur some issues (such as scalability and robustness) due to possibility of more indirect connections than achieved with a higher-level overlay of proxies. Therefore, using a higher-level interworking overlay (as per the previous scheme) would be more logical, but could require some controlled administration of the higher-level overlay. In small-scale implementations, the inter-domain registration could be more convenient, as e.g. private overlays could interconnect without the need for outside involvement.

4.4 Fixed and Mobile Networks

Providing a gateway to PSTN and PLMN was introduced in Section 4.2, but the gateway is not required to be done using IMS. Therefore, a gateway at the border of a 2G/3G network and Internet would be feasible for interworking between P2PSIP and PSTN&PLMN terminals.

4.5 Summary

Good interworking of P2PSIP with other networks is important (not only for MOs). As P2PSIP is closely related to the conventional SIP, the interworking between P2PSIP and conventional SIP can be done at the border of the SIP domain and P2PSIP overlay (the P2PSIP standard covers this interworking case). Interworking with other SIP-based networks is also feasible, and especially interworking with IMS could be beneficial for mobile operators. Also interworking with telephony networks (PSTN&PLMN) is feasible and would be beneficial for mobile operators.

As different P2PSIP overlays might use different DHT algorithms, their interworking could be done either using upper-level overlay or by using inter-domain registrations.

5 Mobile Operators' Role in P2PSIP

We have now introduced the technical part of the P2PSIP and its interworking cases. We will now identify and investigate the potential roles and prospects for mobile operators (MOs) related to the forthcoming P2PSIP. Furthermore, we will try to predict some possible impacts of P2PSIP. The interworking cases introduced in the previous chapter involve operations on the part of the corresponding operator and they can therefore also be linked to the operators' roles.

Today's telecom market has become extremely competitive, one where service providers have to actively compete against rivals across varied service domains. The ongoing convergence of closed telecom environment and open Internet spurs the emergence of rivals across a range of services domains, as a more open environment and new technologies enable better innovation of services. For example, many mobile phones can access Internet services (e.g. Skype) using an operator-independent connection (e.g. WLAN). Service providers are obliged to adapt and add more value to their service supply. The main challenges for mobile (and fixed) service providers are to:

- Maintain their earning principles (or ideally even achieve revenue growth)
- Maximise profitability through reduced OPEX and CAPEX

(OPEX = operational costs in running systems, CAPEX = Capital expenditures of acquisition or upgrading physical assets such as equipment). [Mason07]

In order to achieve these goals, service providers are making changes not only in their strategies and operations, but also in their infrastructures. Infrastructure changes and optimizations include implementing IP-based infrastructures, which allow carrying voice and data more efficiently than in traditional circuit-switched infrastructures. Increased efficiency also implies that OPEX and CAPEX of infrastructures can be reduced. Such IP core networks are QoS-aware and are often referred to as Next Generation Networks (NGN). [Mason07]

While P2PSIP among other P2P networks opens up a relatively new approach to providing new services, it also challenges the existing services that are based on client-server architecture. This can at the same time present both a threat and an opportunity to a mobile operator.

5.1 Mobile Operators' Relation to P2PSIP

One of the main findings of this thesis is the identification of the roles and the benefits of P2PSIP for an MO. As the type of the MO affects how the MO positions itself towards P2PSIP, we will identify the differences between MOs in this respect before discussing their possible roles.

5.1.1 Different Mobile Operator Types

There are three main types of MOs. These are Mobile Network Operator (MNO), Mobile Service Operator (MSO) and Mobile Virtual Network Operator (MVNO). A MNO owns the wireless spectrum and its own network that it uses to provide network capacity for MSOs and MVNOs. Basically, MSO and MVNO are quite similar, as both provide services to their own customers and buy network capacity from a MNO. However, often MVNOs do not provide as wide a variety of services as a MSO does. Moreover, a MSO is usually in close cooperation with a MNO, yet it is not integrated with it. A MO that is both a MSO and a MNO is called a monolithic MO (or "vertically integrated MO"). [Smura06]

In this chapter, we will focus on the monolithic MO that is the common model for traditional telecom operator. A monolithic MO has originally been a telecom operator that bases its business on running a landline telephony network. Later on, when the "mobile revolution" started in the early 1980s, such operators (e.g. TeliaSonera) have usually become mobile operators as well. Therefore, their infrastructures tend to be extensive.

5.1.2 Adoption of P2PSIP for an MO

The applicability of P2PSIP for an MO depends on the type of the operator, as the profitability of applying P2PSIP is not the same. For example, an MVNO could find P2PSIP appealing, as P2PSIP does not require heavy infrastructures that MVNOs do not possess. P2PSIP may not appear that appealing for monolithic MOs, as it could conflict with the existing services and infrastructures (e.g. IMS). However, a MSO can carve itself a role in a P2PSIP environment without loosing revenues from its current services and infrastructures. If revenues were diminished because of using P2PSIP, they could be compensated by reductions in OPEX.

In general, an MO would adopt P2PSIP if its adoption fulfils the following conditions:

- It assures a level of certainty regarding customer retention
  (By binding customers, operators can better ensure their incomes)
- It allows the MO to shrink its OPEX enough to offer more new services or to replace old services while charging less
  (Enables more efficient operation, while still enabling to enhance services)
- It allows the MO to offer different services at different prices to different customers
  (As customers are different, they prefer different services or service packages)
- Its applicability does not disturb or conflict with legal authorities and emergency call requirements
  (Operators have to follow regulations)
- It allows costs to be covered in charges and fees
  (Operators need somehow to cover the expenses of implementing and running their services)

5.1.3 Different Ways of How an MO Can React to P2PSIP Traffic

A MO can react to P2PSIP and other P2P traffic in several ways. In general, an MO can do the following:

- **Ignore it** (this is often the first reaction)
  - Provide only the data pipe and look on (or be unaware)
- **Impede**
  - Filter P2P traffic
  - Force customers to use IMS (if available and possible)
- **Fill the gaps**
  - Upgrade reachability by providing adequate access-level service
  - Provide some services

We concentrate on identifying the prospects related to the last scenario, “filling the gaps”, as it represents a more productive way forward in the evolving and challenging telecom environment. However, the actual adoption of P2PSIP depends not only on its final properties and efficiency, but also on the status quo of the telecom environment when the P2PSIP standard is launched (estimated in mid-2008) and ready for implementations. Just doing nothing rather obviously carries no potential for increasing profits. By impeding P2PSIP usage and trying to force the customers to use e.g. the IMS (or just the plain non-IMS MO services) is not necessarily reasonable either. Such an approach does not necessarily support sustainable development of profitability and

competitiveness against other service providers in the long run, since P2PSIP can provide new ways of implementing services. Nonetheless, some operators are impeding or forbidding VoIP traffic over cellular and thereby trying to hinder the evolution of mobile VoIP [Morgan06].

5.2 Some Identified Roles for a Mobile Operator

We will identify here some roles that an MO can take by using P2PSIP, both in inter-operator networks and in the MO's own network. They are introduced, because they can bring potential benefits and income to MOs through new services. However, the introduction of any new services in general should be based on users' needs and rely on a user-centred design (without forgetting usability), while still maintaining profitability at an acceptable level.

5.2.1 Mobile Operator Participating to Inter-Operator P2PSIP Overlays

P2PSIP allows users to form their own P2PSIP networks without outside involvement in the Internet, but also without Internet connectivity (using e.g. direct WLAN ad-hoc connections between the devices). Therefore, as private P2PSIP networks will emerge, an MO could provide them access to the MO's services or even provide some P2PSIP-specific services (including also the provision of adequate access-level service). Thus, an MO could also benefit from users that are not its current subscribers. However, an MO should not encourage and facilitate the use of own and private inter-operator P2PSIP networks, if this would reduce MO's profitability.

5.2.1.1 MO to Provide Resources for P2PSIP Networks

A possible role for an MO could be in the provision of superpeers for inter-operator P2PSIP overlays as well as for MO-operated P2PSIP overlays that are discussed in 5.2.2. This server-like superpeer (or "peer-server") could provide interfaces to different MOs' services for the P2P communities as P2PSIP resources. Even though peers in a P2PSIP overlay would be defined (by the standard) to be all equal, an MO-run peer could be regarded as a superpeer, because it would be able to provide much more resources than the other peers. Furthermore, an MO-run superpeer would provide the kind of resources that the other (usually just UA) peers can not provide (e.g. a PSTN gateway).

Resources provided by an MO might include:

- **Voice mail** (possibly attached to a bootstrap or an enrolment server, but can be also P2P, when a server can store the indication of a voice mail stored in a peer)
- **Conferencing** (as it is heavy and difficult to handle with equal P2P connections, because mixing of multiple streams from the peers have high computation and bandwidth requirements)
- **Multimedia chat rooms (including IM)**

Other services (such as enrolment and gateways) are discussed later in this chapter. In general, P2PSIP is able to provide similar versatile services to IM&VoIP clients such as Skype and Messenger as well. The traditional telephony services (i.e. SIP call control functions) can also be implemented in the P2P manner, and are therefore feasible with P2PSIP [sipping-cc-framework-07].

The operator-run superpeers can also provide stability and reliability for P2PSIP overlays, as their high availability (i.e. always online) would stabilize churn (i.e. peers joining and leaving) of P2PSIP overlays. As far as mobile terminal usage of P2PSIP is concerned, some analyses show that 60-70% of phone calls are made indoors [Morgan06]. Google estimates that even 64% of mobile calls are made from within the range of a WiFi base station [Morgan06]. Thus, improving the stability of a P2PSIP overlay with operator-peers can enhance overlay stability, but analyses and estimations imply that a P2PSIP overlay of mobile clients could be stable enough in itself. The DHT implementation used by a P2PSIP overlay defines how the churn of nodes is being handled. Thereby, the evaluation of the corresponding DHT implementation can bring a better understanding of its functioning. However, this issue can be better examined when the supported DHT(s) for P2PSIP standard have been chosen (and even better examined when P2PSIP standard implementations are available). As was stated earlier, Chord appears to be on of the preferred DHT algorithms in P2PSIP.

Running superpeers only for general benefit is not typically in the interest of any commercially-driven entity. For this reason, an operator should have some way of generating revenues from running superpeers. However, by using superpeers, mobile operators could be able to incur revenues of providing such services as mentioned above. The business models allowing this are still open and need further investigation. However, providing chargeable services with superpeers would be feasible due to the self-management capability of such superpeers. This capability would be a key feature to

allow transaction states of SIP sessions to be stored in the overlay for maintenance and billing purposes.

5.2.1.2 Operator as a Security Authority in a P2PSIP Network

It is a known fact that when the number of users in any free community (without clear control) increases, free riding and the number of hostile users also increases (this was discussed in Section 2.3.8). At some point it makes sense to somehow restrict the access to the P2P community and control its usage. A MO could play a role in providing the access control and registration services for P2PSIP communities and thereby answering to this demand. From an operator point of view these kinds of use cases are also easily identified so that they can be billed.

From the security, access control and registration point of view, one solution is to use certificates for granting access. The operator part of some P2PSIP community could act as an enrolment entity by providing an enrolment server (described in Section 3.3.1) for the community. Once a user has subscribed to the enrolment service, the operator would assign a certificate to that user for usage in the corresponding P2PSIP community. As the P2PSIP overlay functionality is not tied to an enrolment service, the enrolment service can be provided by a P2PSIP overlay-independent entity, such as an MO. Each time a user wishes to join a P2PSIP community, it would have to prove its credentials to the P2PSIP community using e.g. its unique operator signed certificate.

5.2.1.3 Bootstrap Server and a Directory Entity

A P2PSIP network can use a bootstrap server to enhance the reachability of the P2PSIP overlay (and thereby its functionality), as was described in Section 3.3.2. As some peer of an overlay has to be found in order to join the overlay, an MO could facilitate this procedure and provide a centralized rendezvous point for this purpose. A bootstrap server could be provided together with an enrolment server.

As the same bootstrap server can serve several P2PSIP overlays, an MO could also use this kind of bootstrap service for providing a directory service for accessing various P2PSIP overlays. This kind of added value service would allow MOs' subscribers to form their own overlays and connect with other similar overlays. Also other than the MO's own subscribers could be allowed. The directory service could be implemented e.g. using some kind list within software running P2PSIP (or just a web page) for listing

the overlays that are registered with the bootstrap server and thereby controlling which overlays can be published in the directory catalogue.

Furthermore, this kind of service could include gateway proxy peers for the interworking scheme of heterogeneous P2PSIP overlays (that was presented in Section 4.3.1). The gateways for P2PSIP are presented in the following subchapter.

5.2.1.4 Gateways

A MO could provide different gateways between the P2PSIP and other telecom networks by using gateway peers. These gateways would do the conversion of the signalling (and media, if necessary) between the P2PSIP overlay and the corresponding network.

Gateway to Public Telephony Networks (PSTN&PLMN)

This would include such use cases as voice calling between P2PSIP device and landline telephone or mobile phone (i.e. PSTN or PLMN). From the operator's point of view this kind of use cases are also easily identified so that they can be billed.

The general idea of such gateway would be that it would be reachable as a P2PSIP resource with a commonly known SIP URI in a P2PSIP overlay. In order to facilitate the access control and charging procedures, the UAs using the gateway peer would be preferably within the same domain. The gateway could be an IMS-independent gateway in the 3G mobile core network (for a monolithic MO). Alternatively, it could rely on the IMS architecture in order to tie also 3GPP SIP devices to the reachability of the gateway service.

Gateway to Other P2PSIP Overlays via IMS

A MO could provide interconnectivity between its known P2PSIP overlays. These P2PSIP overlays could also be run by the operator (instead of being run only independently by subscribers). If an MO provided such service, it could use IMS to provide QoS-guaranteed media transport for the users, at least for its subscribers (both mobile and fixed). This could include using IPX to extend the interoperability beyond the MO's own IMS to other operators' IMS environments.

An operator could also provide peers for conversion between P2PSIP overlays that use different DHT algorithms, if this conversion will not be supported in the P2PSIP standard. This could include the provision of proxy peers for interworking among

heterogeneous P2PSIP overlay (this was presented in 4.3.1). However, this would not require using only IMS.

Gateway to Services and Devices in IMS

A MO could provide a gateway to its services and terminals for P2PSIP overlays (the IMS-P2PSIP interoperability was shown in Figure 30), as both IMS and P2PSIP are based on SIP. This kind of gateway resource could upgrade the reachability of IMS services for subscribers. Other users (that are not subscribers of the MO) could potentially also be allowed to access the IMS services, if they can be billed.

Gateway to SIP Domains

A MO could provide gateway proxies for interoperability between P2PSIP networks and SIP domains. This could be done using IMS to give a certain level of QoS as well. From the operator's point of view this kind of use cases are also easily identified so that they can be billed.

5.2.2 Operator Maintaining a P2PSIP Overlay

An operator could also provide multimedia services for its subscribers by providing all the facilities needed to run a P2PSIP overlay. This could include the operator also supplying the terminal clients (and possibly the terminals as well). Naturally, the services identified in the previous section would also be included here. A set of overlay services could be bundled or be customizable for subscribers. When an operator provides the entire overlay and the additional services, the reliability of the system can be enhanced (as e.g. IMS could be used to enable better QoS than is achieved e.g. in the Internet). When an operator would provide the terminal clients, users would benefit of an easy and reliable system, while the operator could increase their level of commitment to it.

Another benefit of an operator-run P2PSIP overlay would be that the operator could provide P2PSIP peers, and subscribers would only use P2PSIP clients or equivalent. In this way, subscribers would not be required to be loaded by the overlay maintenance operations. Thereby, they would not need to "tolerate" their resources being exploited for overlay information storage and message routing (this is important especially for mobile terminals with limited resources). The overlay structure could also be such that the subscribers' peers or clients would perform some overlay operations, but less than if all the peers of the overlay were equal. The correspondent operator could also give

subscribers the possibility to pay less, if they were peers that can be loaded with the overlay maintenance operations.

An operator should not encourage and assist the use of P2PSIP networks, if this was to reduce the total income of the operator. However, when the operator would provide the full service, it could be more profitable than if it provided only some additional services that would ease and encourage the formation of independent P2PSIP overlays.

5.2.2.1 Bundle Subscription Packet

P2PSIP could be used to provide a bundle packet for (3G, ADSL etc.) subscribers, where a P2PSIP client software would be in a mobile phone, PC and possibly other terminals. The user could use different terminals (and switch between them easily) to access service provider services (such as voice and multimedia calls, other multimedia and games, as well as any IMS services). This kind of subscription could be an alternative or supplementary to traditional mobile subscription.

5.2.2.2 P2PSIP in Enterprise VoIP Solutions

Service providers provide VoIP solutions for their customers as a cost-effective alternative for PSTN network within enterprises. P2PSIP can also be used in this way. P2PSIP may not (at least initially) replace such existing enterprise VoIP solutions, as they are quite well defined with call forwarding, IP-PBX services etc. However, because the existing VoIP solutions use SIP and SIP servers, P2PSIP could be used there to lighten the infrastructure and thereby allow more competitive VoIP solutions. At some point P2PSIP could even replace the existing client-server VoIP solutions. However, as stated before, at least enrolment and bootstrap servers are needed for an efficient and secure system. In order to accomplish the most sophisticated telephony functions, SIP call control can function in both third party call control mode and in P2P mode [sipping-cc-framework-07].

P2PSIP challenges the existing infrastructure-based VoIP industry, since it can provide the same services in a P2P manner, thereby eliminating the cost of servers needed in the functions that P2PSIP replaces. The P2P-property also eases the configuration process and recovery from network failures, because a P2PSIP overlay is self-organizing.

In a P2PSIP-based VoIP network, customers could choose services (by inviting “service-peers” to their network) and thereby customize the kind of VoIP network they want.

Some P2P-based (but not, at least yet, P2PSIP-based) VoIP solutions, which provide full VoIP services, already exist. One example is Damaka (www.damaka.com), which advertises that it provides service providers and operators vendor independent VoIP solutions based on P2P networking with SIP standard (but not P2PSIP).

5.2.3 Mobile Operators' own Infrastructure

This section covers mainly the implementation cases of P2PSIP, where the P2PSIP usage would be focused on operators' own infrastructures and would thus be transparent for end-users. Transparency ensures that the clients are not affected and can operate as before. Influence in implementing P2PSIP in an MO's infrastructure would impact signalling mechanisms between network nodes, but it would also possibly influence the infrastructure.

Telecom operators usually buy the network equipment from vendors and they are therefore dependent on vendor implementations. This may hinder the implementation of replacements for existing implementations. But in any case, if vendors were to provide less expensive equipment by exploiting P2PSIP, operators would naturally buy it.

5.2.3.1 Commercial VoIP Infrastructure

P2PSIP could be used in current VoIP solutions that an operator provides (and which usually include operator-owned equipment). These were identified in Section 5.2.2.2.

5.2.3.2 Backup System for Centralized Servers

As was identified in Section 3.6.4 on possible use cases, an operator could implement a cost-effective backup system for its SIP servers. The fault-tolerance of centralized SIP servers (such as an IP-PBX) would be increased when relying on P2PSIP as a backup system. Thereby, planned or unplanned service interruptions would not affect the functioning of the system.

Such backup system could be implemented by enabling the SIP end-points to support also P2PSIP. Thus, when e.g. a central IP-PBX would experience a failure, the handsets and softphones could be able to continue operating transparently in P2P mode until the IP-PBX switch would be replaced.

5.2.3.3 Server Farms

As was identified in Section 3.6.4 of possible use cases, P2PSIP could be used to implement a farm of servers (e.g. SIP proxy). This server farm scheme is depicted in

Figure 33. By implement such farm, an operator could benefit from increased redundancy, load-balancing and scalability of existing SIP networks. This kind of distribution is useful also for other network resources that require scalability and resilience, but without a single point of failure.

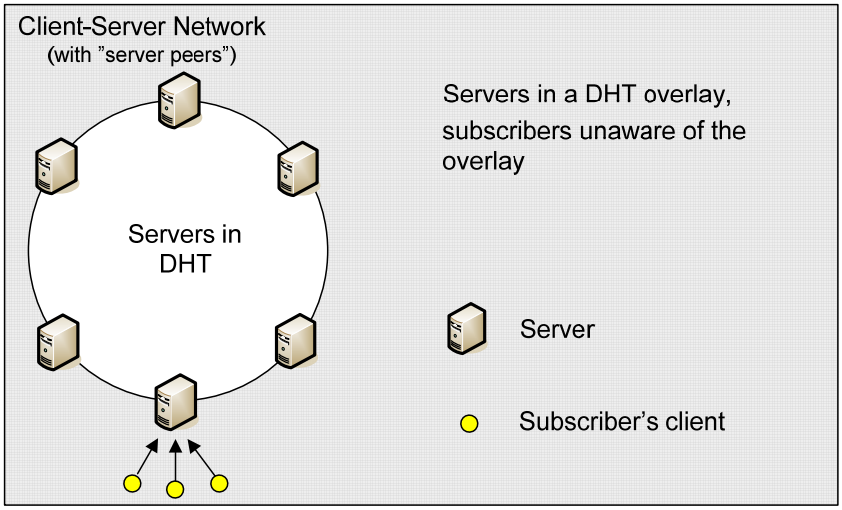

Figure 33 - SIP Server Farm with P2PSIP Overlay

In a server farm, the servers would run a P2PSIP overlay among themselves and would therefore be transparent to clients. Server management would be easier, as resource load share would be dynamic and balanced. This scheme also enables useful geographical distribution of resources. Furthermore, additional servers could be added (or removed) with minimal configuration.

5.2.3.4 IMS with P2PSIP

Mobile operators' views on SIP-based services and architecture so far have mainly been based on the centralized IMS architecture. Although IMS has been standardized for several years now and contains well-defined environment specifications, no larger commercial deployments exist. The main reasons are often stated to be the complexity and the cost of such large architecture, but especially the lack of attractive business cases. Mobile operators still have a strong desire to deploy SIP-based services based on IMS as well as to make use of their interoperable carrier-grade IMS systems. Even if the de-centralized and self-managing infrastructureless P2PSIP appears as a rival for IMS, it should also be considered as an add-on or an enhancement to the IMS architecture — from the mobile operators' point of view. Also, as was stated earlier, IMS QoS capabilities and such could be an enhancement for P2PSIP overlay operation.

IMS has its own well-defined (but not stable, as new revisions emerge continuously) architecture with SIP signalling between the numerous servers and other IMS functions. The classical IMS design is rather complex with numerous boxes and protocols, and despite its benefits, it requires costly infrastructure and detailed configuration (presented in Section 2.1). The IMS uses dedicated application servers to implement network-based applications. These application servers also communicate using SIP. However, the basic SIP (defined in [RFC 3261]) does not define the use of application servers in a SIP network. Therefore, using such servers conflicts with the end-to-end principle of the Internet and creates non-trivial technical problems in SIP implementations [sip-tools-01]. Adding new (network-based) applications may require large re-engineering in the network and thus complicates or blocks the introduction of innovations [sip-tools-01].

Using network-based applications inevitably leads to SIP network designs that are optimized for one business model or another. For example, in the IMS, the current business model and the resulting architecture require additional extensions and conventions to support many services. [sip-tools-01]

By embedding P2P concepts into the IMS infrastructure, operators could save money in both deployment and operation (i.e. CAPEX and OPEX). However, the properties of IMS (described in Section 2.1) are not easily achieved with P2PSIP (at the moment, matters like QoS, billing and session accounting are not addressed in the drafts). It remains to be seen how P2PSIP will be developed for these purposes, or do they need to be implemented on top of the P2PSIP (as the P2PSIP development is not concentrated only on commercial purposes).

Based on these aspects, this section will cover a few selected topics where mobile operators could find P2PSIP useful and beneficial with their IMS infrastructure. These are not the only ways to use P2PSIP in IMS. They are presented here as examples to give an idea of the possibilities of P2PSIP in the IMS context.

Distributed HSS

Since the HSS function in IMS is hard to manage, scale, replicate etc., a potential use for P2PSIP in IMS is to lighten the load of the centralized HSS (Home Subscriber Server) by distributing some (if not all) its functions. By distributing some of the HSS's functions, its dependence could be reduced and a more simplified, fault-tolerant and robust functionality could be achieved.

Finding corresponding S-CSCF (and routing information) in a large IMS network (e.g. 5 million users and 50 S-CSCFs) requires a couple of queries from the centralized HSS. By running P2PSIP among the S-CSCFs, the amount of (potentially heavy) querying load to the HSS could be reduced. In the routing of session data, the terminating S-CSCF (each user is dynamically assigned to an S-CSCF) could be found using the DHT overlay run among the S-CSCFs. Right after the originating side S-CSCF/peer would have transformed (by hashing) the Resource-URI (e.g. of the callee) into a Resource-ID, the peer-ID of the terminating S-CSCF would be identified within the DHT.

However, altering a complex and well-specified IMS system specification may be difficult to execute without it resulting in even more complex functionality.

P2PSIP as an Alternative for IMS

While P2PSIP may not supersede entirely the IMS architecture, it could be used to implement a more lightweight alternative for IMS. Some such P2PSIP-based commercial solutions exist already, even though P2PSIP is not standardized yet. For example, AG Projects Company (http://www.ag-projects.com/) describes their "SIP Thor" platform as follows: "*SIP Thor is a cost-effective alternative to classic IMS and enables today next generation SIP services like voice and video, fixed-mobile convergence, IM and Presence supported by today and tomorrow's end-user SIP devices"* [SIPThor].

5.2.3.5 Extending the Reach of Mobile Devices

A MO could implement a service (optional or mandatory), where a device can reach a base station even if the base stations is out of direct reach, as was described in Section 3.6.3. However, if the existing network coverage is already very good, this may not be an interesting case for an MO. On the other hand, some temporary network overload (e.g. in public events) could be reduced by using such a service, when other devices could relay calls to other base stations. To implement this kind of service, base station repeaters or even subscribers' own intelligent mobile phones could be exploited to distribute the load to near base stations. Naturally, this kind of service would require terminals to support the P2PSIP.

However, using P2P networking to relay the actual media is not very efficient, as every end-point by the path of a call are loaded. Thereby, this use case could be more useful to improve reachability for emergency calls in places suffering from network failure or without network coverage. Overloaded mobile network is not needed to be considered

here, as an overloaded network drops some ongoing calls in order to allow an emergency call to be made.

5.2.4 General Roles

In this section we will identify some general roles that are not dependent on whether P2PSIP would be run in the operator's own network or whether the operator would be providing services to inter-operator overlays. They apply to general cases where an operator is using P2PSIP for providing communication services.

5.2.4.1 Regulative issues

An operator could act as a legal entity towards authorities. However, this kind of role is very ungrateful and requires strong reasons as to why an operator would provide such services for any random P2PSIP network user.

5.2.4.2 Emergency Calls

An operator could act as an entity providing emergency calls. However, this kind of role is very ungrateful and requires strong reasons as to why an operator would provide such services for any random P2PSIP network user. If an operator happens to be part of some P2PSIP community there is always a risk that some regulative authority mandates the operator to provide emergency call services. This risk of being obliged to enable emergency calls in P2PSIP VoIP calls should be investigated carefully, because such use case would not most probably incur revenues.

The technical functioning of emergency calls in P2PSIP is most probably no different from conventional SIP, especially in the IETF emergency call work (ecrit WG). Therefore, P2PSIP is unlikely to have any problems as regards emergency calls requirements.

5.2.4.3 Lawful Interception

An operator could provide lawful interception (LI) services to authorities. However, this would require that the operator intercept every P2P session and related media flows. The interception could be done either with active integrated internal interception functions in the network nodes or with passive probes or sniffers (requires additional hardware) [Utimaco]. This kind of role is very ungrateful and requires strong reasons as to why an operator would provide such services for any random P2PSIP network user. Furthermore,

such an intercepting arrangement would effectively go against the idea and basic functionality of P2PSIP as the system would not be a true P2P system anymore.

LI policy for VoIP traffic is different from country to country. In some countries, e.g. in Netherlands, LI of VoIP is already active [Utimaco]. Thereby, MOs and ISPs might be required to provide necessary LI capabilities for delivering the IP flow to a Law Enforcement Agency (LEA). There are many LI standards for VoIP, and the implementation of LI for P2P VoIP is also being considered [Utimaco].

5.2.4.4 Presence and Instant Sharing

It has been noticed that e.g. Skype and Damaka, which provide P2P-based communication solutions, are not capable of providing accurate and always real-time presence functionality. It remains to be seen how the presence functionality of P2PSIP will work (it also depends on the client implementation and not only of the standard definition). If it shows signs of inaccuracy, an MO could try to enhance this, especially in the P2PSIP overlays that the MO itself provides for its subscribers.

Instant sharing was identified as a use case for P2PSIP in Section 3.6.1, and a service based on this could be in the scope of an MO looking to add value to its services.

5.3 Impacts of P2PSIP for Mobile Operators

The actual impacts of P2PSIP are difficult to estimate at this stage of development of P2PSIP, as its concept will be refined and its details may undergo some changes. However, the basic concept is already defined, and we can try to evaluate possible impacts based on the current status. Basically, P2PSIP can challenge operators to adapt their business models of charging for telephony. Internet service providers have already challenged operators with VoIP, but P2PSIP can provide possibly even more competitive alternative to server-based VoIP and operator networks. P2PSIP can also defy the provision of profitable VoIP, as it is not that dependent on running servers (that always require configurations and maintenance). P2PSIP can also influence the role and profitability of IMS at some level. We concentrate more on evaluating the impacts of P2PSIP on monolithic MOs, and not on the threats for MOs in general. [Morgan06] discusses in more detail the general status and the evolution of threats and impacts on mobile revenues.

Various things affect how P2PSIP will be received when the P2PSIP standard is finalized and allows implementing standard-based softwares. One matter that will affect the acceptance of P2PSIP is that the P2PSIP standard might be tardy when entering the telecom environment. Reasons for this can be e.g. that IMS might have been adopted and already widely accepted by then, or Skype client may have reached mobile phones and become more versatile and even more popular. In such cases, where the customers have already adopted and are satisfied with similar existing services, yet another such system may not be that appealing anymore. Should such scenarios materialize, P2PSIP would not provide that much added value and it might not be that big a threat for the MOs and Internet service operators such as Skype. Nonetheless, history has shown that the acceptance and adaptation of new technologies is difficult to predict. Even if the telecom market was already saturated, P2PSIP would still bring benefits also to MOs and other service providers in their implementations. By applying P2PSIP in their own infrastructure, they can provide commercial P2PSIP applications that can be transparent for customers (as then the services from the outside do not imply using P2PSIP). Other benefits were identified before.

Whether P2PSIP would or would not become a big threat for MOs and other service providers, there has been a true demand for such a system. The motivation to begin the development of P2PSIP has mainly been initiated by parties that want to develop the telecommunication environment in general, and not only with commercial benefit in mind. Therefore, the emergence of P2PSIP is welcome, and because of its versatile applicability, it can and will be used in various situations. It can therefore be useful also in environments where there may not be telephone operators or Internet connectivity available. This may result in P2PSIP diversifying the telecom environment and bringing the telecom evolution further. Furthermore, the potential for easy implementation and minimal configuration of P2PSIP lowers the threshold to establish P2PSIP communication communities. However, reliability and easiness of some functions that may seem minor affect the acceptance of P2PSIP. For example, well functioning NAT traversal mechanism is very important, as most of the Internet computers are behind NATs.

As was stated earlier, P2PSIP (as SIP) is not intended to be a replacement for TDM systems such as 2G/3G and PSTN. However, P2PSIP (among other VoIP) challenges telecom operators (and especially MOs) to adapt and provide services that correspond

with the general trend in the current evolution of the telecom environment. [Morgan06] estimates that mobile VoIP could turn into an existential challenge for the current income structure of the mobile industry beyond 2010. It may also take time before P2PSIP reaches the market (as it will not be standardized before mid-2008) and even then it may follow the general trend of mobile VoIP of not being an immediate threat when available. If a mobile operator decides to ignore or even impede P2PSIP traffic in its network instead of "filling the gaps", it should at least observe the market and be aware of the possible threats of not implementing it. This could happen e.g. because other service providers may be able to provide more attractive services at low cost by using P2PSIP.

5.4 Summary

Even though the P2PSIP standard is still being developed, its basic features are already defined and therefore they allow evaluating its potentials for mobile operators (MOs). P2PSIP can be a threat for an MO, but it also presents an opportunity to increase competitiveness against other service providers and to provide new services. Instead of ignoring or impeding P2PSIP traffic, an MO can carve itself a foothold in P2PSIP by providing some services and adequate access-level service. Some potential roles for an MO to play were identified in this chapter.

The type of an MO affects the applicability and impacts of P2PSIP for the MO. A monolithic MO with existing infrastructure positions itself towards P2PSIP differently from a virtual MO (that may not have any own infrastructure). Even a monolithic MO can identify beneficial use cases, where it can e.g. take advantage of its networks in service provision for P2PSIP networks. Some examples include providing gateways to telephony networks or IMS services. A MO can provide some P2PSIP-related servers (such as enrolment and bootstrap servers) for the enhancement of the functionality of P2PSIP overlays, or the entire P2PSIP overlay facilities for its subscribers.

Using P2PSIP for infrastructural use cases may also be beneficial for a monolithic MO, since it could enhance the efficiency of the infrastructure. Such cases include e.g. implementation of a distributed backup system for existing SIP servers, or distributing some (if not all) HSS functionality. P2PSIP may also decrease traffic among the mobile core entities, as direct peer connections would load predominantly the edge routers of the core network. Thereby, the core network could potentially serve the masses with reduced network scaling. A MO could even introduce a more lightweight (and less complex)

alternative for IMS. Such lightweight alternatives for IMS based on the P2PSIP ideology already exist. However, infrastructural changes may be difficult without support from vendors, as MOs are dependent on the vendors from whom they buy their infrastructures. In general, altering the IMS infrastructure with P2PSIP may turn it even more complex, especially in the case of significant structural changes.

The services and changes in infrastructure can be affordable and reduce OPEX and CAPEX. However, some important issues are still open (while not impossible to resolve) and some of them may take time to resolve. These issues include e.g. how to implement charging (of course a flat fee would be easy) and how P2PSIP assures a level of certainty regarding customer retention. These are not addressed (at least in the initial version) in the P2PSIP specification, because P2PSIP is mainly intended to be an open protocol that is not restricted for commercial purposes. In any case, P2PSIP does not restrict e.g. the implementation of charging service, as end-points (i.e. end-user terminals or server farms) can be used to run services in endpoints in a distributed manner.

6 Conclusions and Future Research

This thesis had two main objectives. The first was to give an introduction to the technical background related to the P2PSIP (Peer-to-peer SIP) that is being developed and, more importantly, based on the current Internet drafts, to shed light on the functionality of P2PSIP. The second objective was to evaluate some applications and prospects of P2PSIP for mobile operators, as well as to seek to identify some impacts of P2PSIP to them. The impacts and prospects are different for different kinds of mobile operator. We have mainly been focusing on monolithic mobile operators, which are both service operators and network operators.

Skype along with other P2P networks has demonstrated the robustness of P2P networks. They are widely used networks, yet they are able to maintain their efficiency. Mainly due to P2P file sharing networks, the Internet is dominated by P2P traffic. Skype and other similar players have challenged telecom operators with their cost-effective P2P-based architectures. A traditional client-server infrastructure is not necessarily required for versatile large scale VoIP communication and therefore P2PSIP can have an impact on both VoIP service providers and mobile operators. However, P2PSIP (or SIP) is not intended to replace existing voice telecom systems (such as 2G/3G and PSTN). Nonetheless, it may still challenge their earning principles, especially those that are based on stabilized and mature market areas.

With their current business models, P2PSIP may become a threat for monolithic mobile operators and other service providers. However, it can also be an advantage for them in the competition with other rivalling service providers. It also opens up possibilities for mobile operators to provide services that are not feasible with their current client-server systems (including systems such as VoIP and 2G/3G). As P2PSIP requires none or minimal managed infrastructure, it also has the potential to simplify complex infrastructures, as well as e.g. to enable the implementation of easy-configurable backup and redundancy systems. An important facilitator for this is (in addition to P2P networking) that P2PSIP aims to use simple SIP, where applications (=i.e. resources) reside at the endpoints. This simple SIP approach represents an attempt to reign in the vast set of SIP extensions that are used to define network-based applications in SIP.

While P2PSIP (and VoIP in general) may not threaten current mobile industry revenues substantially before 2010, after this turning point, according to [Morgan06], mobile VoIP

is likely to turn into an existential challenge. Also, as P2PSIP is not standardized yet and developing advanced P2PSIP implementations takes time, the full effects of P2PSIP may take time to be felt. However, commercial implementations to SIP and IMS, which exploit the P2PSIP ideology and can be used by service providers, already exist. These existing "pre-P2PSIP" (and later standard-based) implementations may bring about benefits already before the time mobile VoIP has been estimated to be challenging the traditional mobile voice market. However, it should be kept in mind that VoIP is not the only way to use P2PSIP.

We have identified some opportunities that P2PSIP presents for mobile operators to develop new services or alternatives for some existing services. Some potential opportunities concerning the infrastructure of a monolithic mobile operator were also identified. The main focus here was on acquiring an understanding of the characteristics of P2PSIP as well as to find business opportunities it opens for mobile operators. This also helps to better understand the threats and impacts it potentially entails for mobile operators. In some cases, P2PSIP can offer the opportunity to reduce OPEX and CAPEX and to provide more services while charging less, yet still preserving the revenues.

If an MO does not want to adopt P2PSIP when it would be feasible, it should still be aware of the potential impacts it entails on its business. Moreover, an MO should possibly be prepared to implement P2PSIP in case the threats of not using it appear to become significant at some point. The impacts and prospects of P2PSIP can be predicted more accurately once the P2PSIP standard is more refined. The state of the telecom market at the time of the launching of P2PSIP also affects the system's fortunes and its repercussions for the players in the telecom market. It also has an effect on the issue of how to align the prospects and impacts of P2PSIP with the mobile operator's strategies of voice and other multimedia over IP.

There are some interesting issues that can be identified for future research. Testing of existing experimental implementations, as well as of standard-based P2PSIP implementations once they emerge, can provide more information on the functionality of P2PSIP. The potential roles of MOs can also be investigated further and a particular focus on their business opportunities would be useful once P2PSIP is defined more accurately. Future work could also include specifying the impacts and prospects of P2PSIP in line with the forthcoming status quo of telecom markets, since this is difficult to predict beforehand.

7 References

[Aberer03] Aberer K. et al.,"P-Grid, A Self-organizing Structured P2P System", École Polytechnique Fédérale de Lausanne (EPFL), Distributed Information Systems Laboratory, 2003.

[Acosta05] Acosta W. and Chandra S., "Unstructured peer-to-peer networks - next generation of performance and reliability", in: INFOCOM, 2005.

[AMSIX07] Amsterdam Internet Exchange, http://www.ams.ix.net. Retrieved at 09.02.2007.

[Bahora03] Bahora A. S. et al., "Integrated Peer-to-Peer Applications for Advanced Emergency Response Systems", Proceedings of the 2003 Systems and Information Engineering Design Symposium.

[Baset06] Baset S. A. and Schulzrinne H., "An analysis of the Skype Peer-to-Peer Internet Telephony Protocol", In Proceedings of the INFOCOM '06 (Barcelona, Spain, Apr. 2006)

[Bittorrent] BitTorrent. http://www.bittorrent.com/

[Bryan05] Bryan D., Lowekamp B. and Jennings C., "SOSIMPLE: A Serverless, Standards-based, P2P SIP Communication System", Proceedings of the 2005 International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications (AAA-IDEA 2005), June 2005.

[Buford05] Buford J. and Ross K., "P2P Overlay Design Overview", Presented at IETF P2P-SIP ad hoc November 2005. Available at http://www.cs.uml.edu/~buford/irtf-p2prg/JBufordKRoss-IETF-Overlay-Systems-v4.pdf. Retrieved January 26, 2007.

[Cablelabs] Cablelabs, http://www.cablelabs.com/.

[CacheLogic06] CacheLogic, "The impact of P2P", 2006. Available at http://www.cachelogic.com/home/pages/isp/p2ptoday.php. Retrieved 22.01.2007.

[Camarillo02] Camarillo G., "SIP demystified". McGraw-Hill, 2002.

[Camarillo04] Camarillo G. and Garcia-Martin M. A., "The 3G IP Multimedia Subsystem". Wiley, 2004.

[Cao06] Cao F., Bryan D. A. and Lowekamp B. B., "Providing Secure Services in Peer-to-Peer Communications Networks with Central Security Servers", Proceedings of ICIW'06, 2006.

[Carton05] Carton B. and Mesaros V, “Improving the Scalability of Logarithmic-Degree DHT-based Peer-to-Peer Networks”. To appear in Proc. of EUROPAR 2004.

[Cumming05] Cumming J., ”Session Border Control in IMS”, Data Connection, 2005. Available at http://www.sipcenter.com/sip.nsf/html/WEBB5YP4SU/$FILE/Data_Connection-SBCinIMS.pdf. Retrieved May 16, 2007.

[Damiani04] Damiani E., Capitani di Vimercati S., Paraboschi S. and Samarati P., “P2P-based collaborative spam detection and filtering”. In Proc. 4th IEEE Conf. on P2P, Zurich, Switzerland, August 2004.

[Davies06] Davies R., “IPX technical Architecture Overview”, GSMA, May 2006. Not publicly available.

[Dinger06] Dinger J. and Hartenstein H., ”Defending the Sybil attack in P2P networks: taxonomy, challenges, and a proposal for self-registration”. First International Conference on Availability, Reliability and Security (ARES 2006), pp. 756-763, April 2006.

[Guha05] Guha S. and Francis P., “Characterization and Measurement of TCP Traversal through NATs and Firewalls”, Proceedings of Internet Measurement Conference (IMC), October 2005. Available at http://nutss.gforge.cis.cornell.edu/pub/imc05-tcpnat/. Retrieved March 28, 2007.

[Harren05] Harren M. et al., ”Complex Queries in DHT-based Peer-to-Peer Networks”, in proceedings of the 25th Distributed Computing Systems IEEE International Conference, pp. 339-348, 2005.

[ICE] Rosenberg J., "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", draft-ietf-mmusic-ice-13 (work in progress), January 2007.

[IEEEDoval03] Doval D. and O’Mahony D., “Overlay networks: A scalable alternative for P2P”. *IEEE Internet Computing*, vol. 7, no. 4, pp. 79-82, 2003.

[IEEELua04] Lua E. K., Crowcroft J., Pias M., Sharma R. and Lim S., “A Survey and Comparison of Peer-to-Peer Overlay Network Schemes”, C*ommunications Surveys & Tutorials, IEEE*, vol. 7, issue 2, pp. 72-93, 2005.

[IEEERipeanu02] Ripeanu M., Foster I., Iamnitchi A., “Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems

and Implications for System Design" *IEEE Internet Computing*, vol. 6, no. 1, pp. 50-57, 2002.

[Illuminati] Cadaco, M. and Freedman, M., "Illuminati - Opportunistic Network and Web Measurement", Available at http://illuminati.coralcdn.org/stats. Retrieved February 10, 2007.

[IR65] GSM Association, "IMS Roaming & Interworking Guidelines, Official Document IR.65", version 3.5. August 2006.

[ITUX.509] International Telecommunication Union, "ITU-T Recommendation X.509: Public-key and attribute certificate frameworks", 2005.

[ITWeek] Hoskyn J. ,"Orange and Vodafone cut VoIP from Nokia N95", ITWeek, April 20, 2007. Retrieved April 25, 2007

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

[Karger97] Karger D. et al., "Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web". In Proceedings of the 29th Annual ACM Symposium on Theory of Computing (El Paso, TX, May 1997), pp. 654–663, 1997.

[Lv02] Lv Q., Cao P, Cohen E., Li K. and Shenker S., "Search and Replication in Unstructured Peer-to-Peer Networks". In Proceedings of the 16th annual ACM International Conference on Supercomputing (ICS), 2002.

[Maison07] Mason Communications Ltd., " Fixed Mobile Convergence in Next Generation Networks: Drivers, Key Enablers and Challenges", 2007.

[Matthews05] Matthews P. and Poustchi B., "Industrial-Strength P2P SIP", Internet Draft, draft-matthews-sipping-p2p-industrial-strength-00.txt (work in progress), February 11, 2005. Available at http://www.p2psip.org/drafts/draft-matthews-sipping-p2p-industrial-strength-00.txt. Retrieved February 5, 2007.

[Maymo02] Maymounkov P. and Mazieres D. "Kademlia: A peer-to-peer information system based on the XOR metric". In *Proceedings of the First IPTPS*, March 2002.

[Mellin04] Mellin J., "Peer-to-peer networking - Phenomenon and impacts to carriers", September 2004. Available at http://www.netlab.tkk.fi/opetus/s38001/s04/pres/Jorma_Mellin.pdf. Retrieved January 5 2007.

[Mike06] "Mike", "Trying To Slow Down BitTorrent Traffic Will Backfire, Badly", Techdirt.com. Available at http://www.techdirt.com/articles/20061226/100457.shtml. Retrieved January 5, 2007.

[Mohanty05] Mohanty P. K., "Service Deployment Strategies for Telecom Operators", Appears in Telecommunications, 2005. ConTEL 2005. Vol 1, pp. 247-250, 2005.

[Morgan06] JPMorgan Securities Ltd., "European Telecom Services, Agents of deflation – disruptive technologies in European mobile", European Equity Research, August 2006.

[Ott07] Discussions with Professor Jörg Ott, TKK.

[Parameswaran01] Parameswaran M., Susarla A. and Whinston A.B., "P2P networking: An information-sharing alternative", *IEEE Computer*, vol. 34, no. 7, pages 31-38, July 2001.

[Parker05] Parker A., "P2P in 2005", CacheLogic presentation. Available at http://www.cachelogic.com/home/pages/studies/2005_01.php. Retrieved January 29, 2007.

[PGP.com] "Pretty Good Privacy", http://www.PGP.com

[p2p-usecases-00] Bryan D. A., Shim E. and Lowekamp B.B., "Use Cases for Peer-to-Peer Session Initiation Protocol (P2P SIP)", draft-bryan-sipping-p2p-usecases-00 (work in progress). Retrieved November 7, 2006.

[p2psip-bootstrap-00] Cooper E., Johnston A. and Matthews P., "Bootstrap Mechanisms for P2PSIP", Internet Draft, draft-matthews-p2psip-bootstrap-mechanisms-00 (work in progress). Retrieved March 12, 2007.

[p2psip-concepts-04] Bryan D., Matthews P., Shim. E. and Willis D., "Concepts and Terminology for Peer to Peer SIP", Internet Draft, draft-willis-p2psip-concepts-04 (work in progress). Retrieved March 19, 2007.

[p2psip-dSIP-00] Bryan D., Lowekamp B. and Jennings C., "dSIP", Internet Draft, draft-bryan-p2psip-dsip-00 (work in progress). Retrieved March 12, 2007.

[p2psip-hier-arch-00] Shi J., Ji Y., Zhang H. and Li Y., "A Hierarchical P2P-SIP Architecture", Internet Draft, draft-shi-p2psip-hier-arch-00 (work in progress, draft expired in February 2007), Retrieved June 25, 2007.

[p2psip-interwork-01] Marocco E. and Bryan D., "Interworking between P2PSIP Overlays and Conventional SIP Networks", Internet Draft,

draft-marocco-p2psip-interwork-01 (work in progress). Retrieved March 12, 2007.

[p2psip-security-req-00] Matuszewski M., Ekberg J-E. and Laitinen P., "Security requirements in P2PSIP", Internet Draft, draft-matuszewski-p2psip-security-requirements-00 (work in progress). Retrieved March 12, 2007.

[p2psip-dsip-security-00] Lowekamp B. and Deverick J., "Authenticated Identity Extensions to dSIP", Internet Draft, draft-lowekamp-p2psip-dsip-security-00 (work in progress). Retrieved March 12, 2007.

[p2psip-NATs-01] Cooper E. and Matthews P., "The Effect of NATs on P2PSIP Overlay Architecture", Internet Draft, draft-matthews-p2psip-nats-and-overlays-01 (work in progress). Retrieved March 14, 2007.

[p2psip-nats-and-overlays-01] Cooper E. and Matthews P., "The Effect of NATs on P2PSIP Overlay Architecture", Internet Draft, draft-matthews-p2psip-nats-and-overlays-01 (work in progress). Retrieved March 20, 2007.

[p2psip-peer-protocol-00] Hautakorpi J. and Camarillo G., "The Peer Protocol for P2PSIP Networks", Internet Draft, draft-hautakorpi-p2psip-peer-protocol-00 (work in progress). Retrieved March 12, 2007.

[p2psip-security-00] Jennings C., "Security Mechanisms for Peer to Peer SIP", draft-jennings-p2psip-security-00 (work in progress). February 24, 2007.

[p2psip-whysip-00] Zangrilli M. and Lowecamp B., "Why SIP should be used for encoding the P2PSIP Peer Protocol", draft-zangrilli-p2psip-whysip-00 (work in progress). March 13, 2007.

[Ratnasamy01] Ratnasamy S., Francis P., Handley M., Karp R. and Shenker, S. "Scalable content-addressable network" In Proc. ACM SGCOMM (San Diego, CA) August 2001.

[RFC 2104] Krawczyk H., Bellare M. and Canetti R., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC 2806] Vähä-Sipilä A., "URLs for Telephone Calls", RFC 2806, April 2000.

[RFC 3095] Bormann C. at al. "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.

[RFC 3261] Rosenberg J. et al., “SIP: Session Initiation Protocol”, RFC 3261, June 2002.

[RFC 3263] Rosenberg J., Schulzrinne H., “Session Initiation Protocol (SIP): Locating SIP Servers“, RFC 3261, June 2002.

[RFC3320] Price R. et al., “Signaling Compression (SigComp)”, RFC3320, January 2003.

[RFC 3711] Baugher M., McGrew D., Naslund M., Carrara E. and Norrman K, “The Secure Real-time Transport Protocol (SRTP)”, RFC 3711, March 2004.

[RFC 4474] Peterson J., Jennings C., “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)”, RFC 4474, August 2006.

[RFC 4566] Handley M., Jacobson V. and Parkins C., “SDP: Session Description Protocol”, RFC 4566, July 2006.

[Rhea03] Rhea S., Geels D., Roscoe T., and Kubiatowicz J., ”Handling churn in a DHT. Technical Report UCB//CSD-03-1299, University of California, Berkeley, December 2003.

[Routers07] Reuters, “Skype founders launch global online TV”, January 16, 2007. Available at http://money.cnn.com/2007/01/16/technology/skype.reut/index.htm?postversion=2007011615. Retrieved January 22, 2007.

[Rowstron01] Rowstron A. and Druschel P., “Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems”, in Proceedings of IFIP/ACM Middleware, 2001.

[Schwartz-05] Schwartz D. and Sterman B., “NAT Traversal in SIP”, Kayote Networks 2005.. Available at http://www.kayote.com/web/docs/WhitePapers/KayoteNetworksWhitePaper-NAT_Traversal_in_SIP.pdf. Retrieved May 5, 2007.

[SETI@home] http://setiathome.berkeley.edu/

[SHA-1] FIPS 180-1. *Secure Hash Standard*. U.S. Department of Commerce/NIST, National Technical Information Service, Springfield, VA, Apr. 1995.

[Singh04] Singh K. and Schulzrinne H., "Peer-to-peer Internet Telephony using SIP", Columbia University Technical Report CUCS-044-04, New York, NY October 2004.

[Sinnreich06] Sinnreich H., "The challenge of P2P Internet communications to network based services", Elektrotechnik & Informationstechnik (2006) Vol. 123, no. 7-8, pp. 277–282, 2006.

[sipping-cc-framework-07] Mahy R. et al. "A Call Control and Multi-party usage framework for the Session Initiation Protocol (SIP)", Internet Draft, draft-ietf-sipping-cc-framework-07 (work in progress). Retrieved May 22, 2007.

[SIPThor] AG Projects, http://www.ag-projects.com/

[sip-tools-01] Sinnreich H. ed., Johnston A., Shim E. and Singh K., "Simple SIP Usage Scenario for Applications in the Endpoints", Internet Draft, draft-sinnreich-sip-tools-01 (work in progress). Retrieved March 12, 2007.

[SIPThor] http://ag-projects.com/SIPThor.html

[Sit02] Sit E. and Morris R., "Security considerations for Peer-to-Peer Distributed Hash Tables", In Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS), Cambridge, MA, March 2002.

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

[Smura06] Smura T., Kiiski A. and Hämmäinen H., "Techno-Economic Analysis of Mobile Virtual Network Operators: Strategies, Investments, and Revenues". 2006. 5th Conference on Telecommunication Techno-Economics, 8-9 June 2006, Athens, Greece.

[Stoica01] Stoica I., Morris R., Karger D., Kaashoek M. F. and Balakrishnan H., "Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications", Proceedings of the 2001 ACM SIGCOMM Conference, 2001.

[STUN] Rosenberg, J., Huitema C., Mahy R. and Wing D., "Simple Traversal Underneath Network Address Translators (NAT) (STUN)", draft-ietf-behave-rfc3489bis-05 (work in progress), March 5, 2007.

[TeliaSonera06] TeliaSonera International Carrier, "Converging next-generation multimedia services across fixed and mobile platforms", TeliaSonera SIP/IMS White paper. September 2006.

[Tispan.org] The Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN), http://www.etsi.org/tispan/

[TS23.002] 3rd Generation Partnership Project: "TS23.002; Network Architecture", 2005. Release 6, version 6.10.0.

[TS23.228] 3rd Generation Partnership Project: "TS23.228; IP Multimedia Subsystem (IMS)", 2006. Release 6, version 6.15.0.

[Utimaco] Utimaco, "Lawful Interception for VoIP", June 2006. Available at http://www.iptel.org/voipsecurity/doc/06%20-%20Winschuh%20-%20Lawful%20Interception%20of%20VoIP.pdf. Retrieved at 16.5.3007

[uTorrent] µTorrent, http://www.utorrent.com/

[Viana04] Viana A.C., Amorim M. D., Fdida S. and Rezende J. F., "Self-organization in spontaneous networks: the approach of DHT-based routing protocols". In *ACM Wireless Networks*, Vol. 3, no. 5, pp. 589-606, 2005.

[Wolff07] Wolff P., "Is 500 million Skype downloads a lot?", Skype Journal, February 19, 2007. Available at http://skypejournal.com/blog/2007/02/is_500_million_skype_downloads.html. Retrieved March 20, 2007.

[zimmermann-zrtp-03] Zimmermann P., Johnston A. and Callas J., "ZRTP: Media Path Key Agreement for Secure RTP", draft-zimmermann-avt-zrtp-03 (work in progress), March 4, 2007.

8 Glossary

Ad-Hoc Network

Ad-hoc network is usually a spontaneously formed network for some specific temporary purpose. E.g. laptops could set up a wireless ad-hoc network in order to transfer some files. In a peer-to-peer (P2P) network, virtual links between the nodes can be considered to form an ad-hoc network.

Bootstrapping

When a peer joins a P2P overlay, it must contact somehow some peer of that overlay. The procedure of locating an initial peer of an overlay is called bootstrapping. The initial peer during this procedure is called bootstrap peer. There are several mechanisms that can be used to find a bootstrap peer (such as multicast, cached peer addresses, bootstrap server and static locations).

Churn

Joins and leaves in a Peer-to-Peer system.

Client-Server Architecture

An architecture in which some small number of servers provide services to a larger number of nodes clients. Client nodes initiate connections to servers, but typically do not communicate among each other.

Complexity theory and Big-Oh notation

Complexity theory can be used to describe the efficiency of algorithms used to solve problems.

The Big-Oh notation "O()" characterizes how the size of the input data affects an algorithm's running time. E.g. an algorithm with complexity of O(logN)) will grow only logarithmically, as algorithm with complexity of $O(2^N)$ will grow exponentially.

Conventional SIP Network

A SIP network where location and routing functionalities are provided by centralized elements, as described in [RFC3261]. [p2psip-interwork-01]

Distributed Hash Table (DHT)

Distributed Hash Tables (DHTs) provide a distributed lookup service similar to a hash table. (name, value) pairs are stored in the DHT and the maintenance responsibility is distributed among the peers using the DHT.

ENUM

Telephone Number Mapping (ENUM) is a set of conventions to unify the telephone numbering system E.164 with the Internet addressing system DNS by using an indirect lookup method, to obtain NAPTR records. The records are stored at a DNS database. [RFC 3761] defines how any ENUM number can be transformed in to a URI. Example transformation of "+1 23 456 789" is "9.8.7.6.5.4.3.2.1.e164.arpa". The end suffix "e164.arpa" is allocated to be used with ENUM E.164 numbers on the IP side of the network. E.164 is an ITU-T recommendation which defines the international public telecommunication numbering plan used in the PSTN and some other data networks. It also defines the format of telephone numbers.

Mesh

There are two types of mesh topologies: full mesh and partial mesh. In a full mesh topology, every node has a connection to every other node in the network. In a partial mesh, some nodes are organized in a full mesh scheme but others are only connected to one or two in the network

Node

A node is a device that is connected to a computer network. Nodes can be computers, cell phones or various other network appliances. On an IP network, a node is any device with an IP address.

Overlay network

An overlay network is a computer network which is built on top of another network. Nodes in an overlay are interconnected with virtual links that correspond to a path in the underlying network. This path may involve many physical links. For example, many peer-to-peer networks are overlay networks because they run on top of the Internet. The dial-up Internet is an overlay upon the telephone network.

Peer

A peer is a node that participates in a P2P network. In a basic P2P network, peers have equal role of importance.

Peer-to-Peer (P2P) Architecture

In P2P architecture peer nodes cooperate to perform tasks. Each peer has essentially equal importance and performs the same tasks within the network. Additionally, peers communicate directly with one another to perform tasks.

P2PSIP Client

A P2PSIP client is a node participating in a P2PSIP Overlay that is less capable than a P2PSIP Peer in some way. The role of a P2PSIP Client is still under debate, with a number of competing proposals, and some have suggested removing the concept entirely. If clients exist, one proposal is that they do have the ability to add, modify, inspect, and delete information in the overlay, but they are not routing of storing any overlay information. Another proposition proposes that the client may store overlay information on the behalf of its adapter peer. Note that the term client does not imply that this node is a SIP UAC. [p2psip-concepts-04]

P2PSIP Peer

A P2PSIP Peer is a node participating in a P2PSIP overlay that provides storage and transport services to other nodes in that P2PSIP overlay. Each P2PSIP Peer has a unique identifier, known as a Peer-ID, within the P2PSIP Overlay. Each P2PSIP Peer may be coupled to one or more SIP entities. Within the P2PSIP Overlay, the peer is capable of performing several different operations, including: joining and leaving the overlay, transporting SIP messages within the overlay, storing information on behalf of the overlay, putting information into the overlay, and getting information from the overlay. [p2psip-concepts-04]

P2PSIP Overlay

A P2PSIP Overlay is an association, collection, or federation of nodes that provides SIP registration, SIP message transport, and similar functions using a P2P organization, as defined by "P2P Network" above.

P2PSIP Resource

P2PSIP Resource is an addressable user endpoint, entity, service, or function within a P2PSIP Overlay. Examples include but are not limited to humans (i.e. user), automata, bridges, mixers, media relays, gateways, and media storage.

P2PSIP Bootstrap Peer

Bootstrap peer in a P2PSIP overlay is a peer that can be used for a joining peer to join the overlay. When one or many bootstrap peers are known, the overlay they are participating can be joined.

Presence

Presence service in a network enables users to convey their ability and willingness for potential communication with other users. Other users can see the status (e.g. online, away, offline) and know whether the user is willing or able to be contacted.

Roaming

Roaming is defined as the ability for a cellular customer to automatically make & receive voice calls, send & receive data, or access other services when travelling outside the geographical coverage area of the home network, by means of using a visited network.

User Agent (UA)

A user agent (UA) is the client application used with a particular network protocol. A user can communicate using a UA with others users of some network (e.g. SIP network).

Superpeer

A superpeer (i.e. supernode) in this document context means a well known P2P node with high availability, enough computing and network bandwidth capacity.

9 Appendix A

Table 1 - Use Case Attributes for P2PSIP [p2p-usecases-00]

Use Case	Number of Users *	Distribution of Nodes	Pure P2P?	Centralized Operations/ Management	Authenticated Users	Carrier-Class Robustness	Interaction with CS-SIP	DNS available
Public P2P VoIP Service Providers	millions	intra-domain	hybrid	yes	yes	yes	yes	yes
Open Global P2P VoIP Network	millions	inter-domain	hybrid	no	no	yes	yes	yes
Presence Using Multimedia Consumer Electronics Devices	tens	intra-domain	P2P	no	no	no	no	yes
Impeded Access	hundreds	inter-domain	P2P	no	no	no	no	yes
Anonymous Communications	tens	inter-domain	P2P	no	no	no	no	no
Security Conscious Small Organizations	hundreds	intra-domain	P2P	maybe	yes	yes	no	yes
Ad-Hoc and Ephemeral Groups	tens	intra-domain	P2P	no	no	no	no	no
Emergency First Responder Networks	thousands	intra-domain	P2P	no	self-cert?	no	when available	no
Extending the Reach of Mobile Devices	hundreds	intra-domain	P2P	no	no	no	no	no
Deployments in the Developing World	tens	inter-domain	P2P	no	no	no	when available	no
Serverless or Small Scale IP-PBX	tens	intra-domain	P2P	maybe	self-cert?	no	yes	yes
P2P for Redundant SIP Proxies	tens	intra-domain	P2P	yes	yes	yes	no	yes
Failover for Centralized Systems	tens	intra-domain	P2P	yes	yes	yes	yes	yes