Taxonomy of P2P Applications

E.H.T.B. Brands and G. Karagiannis
University of Twente, the Netherlands
e.h.t.b.brands@student.utwente.nl, g.karagiannis@utwente.nl

Abstract—**Peer-to-peer (p2p) networks have gained immense popularity in recent years and the number of services they provide continuously rises. Where p2p-networks were formerly known as file-sharing networks, p2p is now also used for services like VoIP and IPTV. With so many different p2p applications and services the need for a taxonomy framework rises. This paper describes the available p2p applications grouped by the services they provide. A taxonomy framework is proposed to classify old and recent p2p applications based on their characteristics.**

Keywords- p2p, applications, taxonomy, characteristics

I. INTRODUCTION

Peer-to-peer networks (also known as p2p) have gained immense popularity in recent years. Their ability to harness the computing power and resources of a large number of network computers makes them much more powerful than a centralized server. The number of p2p applications is growing fast and so is the number of different services p2p provides. Where p2p networks were formally known as file sharing networks, p2p networks are nowadays used for, for example, Voice over IP (VoIP), IPTV and distributed data storage.

With so many different services provided by p2p applications their characteristics vary widely. The questions arise: what characteristics make an application a p2p application and is a certain application really a p2p application? The Internet Research Task Force (IRTF) [1] defines p2p as: "a way of structuring distributed applications such that the individual nodes have symmetric roles, rather than being divided into clients and servers with quite distinct roles. A key concept for p2p systems is therefore to permit any two peers to communicate with one another in such a way that either ought to be able to initiate the contact."

In the past, several taxonomies and frameworks for p2p applications have been developed; see [2] [3] [4] [5]. The problem here is that all this research dates from several years ago. In a field of science like p2p networks, which is experiencing rapid growth, research is quickly outdated. This is why p2p-based VoIP is only barely described in the taxonomies listed above and IPTV is not described at all.

This paper describes a way to classify available and new p2p applications based on their different characteristics. New services in the field of p2p networks, like IPTV, are also taken into account. In this way this paper answers the call from the Peer-to-Peer Research Group, part of the IRTF, for a new taxonomy on p2p applications [6]. The taxonomy can help identifying the main characteristics of an application. Based on these characteristics developers can select existing solutions provided by other applications with similar characteristics. Researchers can use the identified characteristics of an application for doing a qualitative comparison among other applications with similar characteristics.

To create such taxonomy the following research question will be answered in this paper:

- How can p2p applications be accurately classified?

In order to answer this question correctly and completely four sub questions are proposed. These sub questions will provide a step-by-step answer to the main question:

1. What p2p applications are currently available?
2. What are the main characteristics of the available p2p applications?
3. How could the p2p characteristics be used to generate the p2p taxonomy?
4. How could new p2p applications be categorized in this taxonomy?

This research will mainly be based on literature study, analysis of requirements and taxonomy design. The four research questions are answered in four corresponding sections. The first two sections are based on literature study to the state of the art of p2p networking. The first section gives an overview of the p2p applications currently available. The second section addresses the main characteristics of these applications. In section three a framework is proposed for classifying available and new p2p applications. This framework will be derived from the answers of question one and two. Section four provides a way to use the framework, illustrated by an example. At the end there is a final section for conclusions and identified areas for future work.

II. CURRENTLY AVAILABLE P2P APPLICATIONS

In early 2000 Napster [7] was at its peak with nearly sixty million users [4]. At this time the phrase *peer to peer* came to be associated with systems such as Napster. People thought that p2p computing was really a new paradigm. Experts, who knew more about distributed systems, knew better; Usenet and some email systems used the same decentralization concept back in the 1980's.

Over the last years, the number of services that p2p systems provide has grown rapidly. Nowadays, p2p networking is also used in for example IPTV, VoIP and distributed data storage. There is however a distinction between p2p systems and distributed systems in general. Grid computing for example are distributed systems, but not p2p systems, because grids are often managed at a single location or at multiple ones in a

978-1-4244-5626-0/09/$26.00 ©2009 IEEE

federated manner [4]. The definition of p2p systems used in this paper is:

"Peer-to-peer systems are distributed systems consisting of interconnected nodes able to self organize into network topologies with the purpose of sharing resources such as content, CPU cycles, storage and bandwidth, capable of adapting to failures and accommodating transient populations of nodes while maintaining acceptable connectivity and performance, without requiring the intermediation or support of a global centralized server or authority", from [5].

Old and recent p2p applications are grouped below by the service they provide. Because of the large number of p2p applications available, only the most popular are listed.

A. File Sharing

File sharing applications are probably the most popular p2p applications available, although in recent years other p2p services, like VoIP and IPTV, are catching up on them. The most famous file sharing application is probably Napster [7], especially because it was shut down in 2001 due to legal issues. Napster had a number of successors which offered more or less the same service but tried to avoid the legal issues.

File sharing applications are often part of a network with a number of different applications connecting to it. For example, BitTorrent [8] is a well known p2p file sharing network and applications like uTorrent [9], Vuze [10] and BitTornado [11] are all connecting to the network. Table 1 contains a list of popular p2p file sharing networks and applications running on them.

TABLE 1. P2P FILE SHARING NETWORKS AND APPLICATIONS RUNNING ON IT

P2p network	Popular Applications
Ares	Ares Galaxy [12]
BitTorrent	BitTorrent [8], uTorrent [9], Vuze [10], BitTornado [11]
DirectConnect	DC++ [13]
eDonkey2000[1]	eDonkey2000 [14], eMule [15]
FastTrack	KaZaa [16], Kazaa Lite [17]
Gnutella	LimeWire [18], Shareaza [19]
Gnutella2 (G2)	Morpheus [20], Gnucleus [21], Shareaza [19]
Kad Network	aMule [22], eMule [15], MLDonkey [23]
OpenNap	Napster [7]
WPNP	WinMX [24]

Not all applications connecting to each network are listed, because some networks have a large amount of applications running on it. BitTorrent, for example, has over fifty applications, called clients, using the network. All these clients have some different properties, but all of them are part of the same community using the BitTorrent protocol. There are several p2p file sharing applications that support multiple file sharing networks. For example eMule originally runs on the eDonkey2000 network, but now also connects to the Kad network. Another example is that a lot of Gnutella2 (G2) clients also connect to the original Gnutella network.

B. Content Publishing and Storage Systems

These systems create a distributed storage medium, where users are able to publish, store and distribute content in a secure and persistent manner [5]. In some aspects this looks similar to p2p file sharing systems received earlier, but there is however a major difference. "Where p2p file sharing systems are most of the time light weight applications that adopt a best-effort approach without addressing security, availability and persistence, p2p content publishing and storage systems focus on security and persistence", from [5]. Other aspects these systems frequently feature are incorporated provisions for accountability, anonymity and censorship resistance, as well as persistent content management (updating, removing and version control) facilities. Table 2 contains a list of the most popular p2p content publishing and storage systems with a brief description of their purpose.

TABLE 2. POPULAR P2P CONTENT PUBLISHING AND STORAGE SYSTEMS

P2p application	Brief Description
Freehaven [25]	A system for distributed, anonymous, persistent data storage which is robust against attempts by powerful adversaries to find and destroy any stored data [25].
Freenet [26]	A system which lets you publish and obtain information on the Internet without fear of censorship [26].
Groove [27]	A collaboration software program that helps teams work together dynamically and effectively [27].
Mnet [28]	A shared virtual space onto which you can put, and from which you can retrieve, files. (created from the source code of MojoNation [32]) [28].
OceanStore [29]	An architecture for global scale persistent storage. Scalable, provides security and access control [29].

These systems or projects are still in ongoing use. In the past there have been a number of other projects concerning p2p-based content publishing and data storage, but these remained scientific or are not deployed anymore. Examples of such projects are Intermemory [30], Mnemosyne [31], MojoNation [32], PAST [33], Publius [34], SCAN [35] and Tangler [36].

C. Voice over IP

Something which has become very popular in recent years is Voice over IP (VoIP). Many ISPs offer VoIP services to let people call over the internet instead of over the "old" Public Switched Telephone Network (PSTN). Many of these VoIP-networks use standardized protocols like SIP [37], H.323 [38] and IAX [39], but do not run over a peer-to-peer network. Recent work from the P2PSIP Workgroup (P2PSIP WG) [6], part of the IETF, involved p2p-based VoIP communication based on the Session Initiation Protocol (SIP) [41]. The main motivation behind p2p-based SIP is to support ad hoc communication, to simplify the configuration of SIP networks, to make SIP networks more scalable and to provide services independently of other network components such as DNS [42].

[1] The eDonkey2000 application and its website were shut down on September, 28 2005 due to legal issues. Nevertheless, the eDonkey2000 network is still available through other clients like eMule [15]

Skype [40] is currently without doubt the most popular VoIP application available. Skype was developed in 2002 by the creators of KaZaa [16], it recently reached over 170 million users, and it accounts for more than 4.4% of total VoIP traffic [43]. Skype also relies on a p2p infrastructure to exchange signaling information in a distributed fashion, with a twofold benefit of making the system both highly scalable and robust [43]. Skype uses a proprietary protocol that is difficult to reverse engineer and which unlike SIP, for example, is not standardized. The service Skype offers, is not limited to VoIP, but also includes video communication, file transfer and chat services. Voice calls made by Skype can also be directed toward the PSTN using SkypeIn/SkypeOut services, in which case a fee is applied [43].

The target of P2PSIP WG [6] is to develop a peer-to-peer version of the SIP protocol called P2PSIP [41], which can use any DHT-based peer-to-peer overlay network to locate resources, services and users in a decentralized way. The motivation of this work comes from the necessity of having a standard for developing Skype-like decentralized multimedia applications [44]. The P2PSIP protocol should re-implement the proxy and registrar functionality of SIP in a distributed fashion, but should also support other functionalities like file-sharing. Besides that, it should be compatible with signaling protocols other than SIP.

Based on the requirements of the P2PSIP protocol the P2PSIP WG is also working on another draft called the RELOAD protocol [45]. This protocol is binary based instead of the character based P2PSIP protocol, which makes it more light weighted. The RELOAD protocol also offers the possibility of implementing TLS or DTLS secure connection.

D. IPTV

One of the newest services offered by p2p networking is IPTV. Although the first p2p-based IPTV systems have only been recently deployed, the service is gaining popularity. Compared to client/server solutions, the main advantage of p2p streaming for ISPs is an increased cost-effectiveness, since the network capacity costs are shared among the participating peers. Another advantage is self-scalability, since the more peers take part of the network, the more resources are available for exchanging the media data [46]. P2p IPTV offers two different services, namely Video on Demand (VOD) and Real Time (RT) streaming. Most p2p IPTV applications only offer the first service. The p2p streaming concept has now lead to a number of trial p2p IPTV systems such as PPlive [47], PPStream [48], Joost [49] and Sopcast [50]. There is now clear commercial interest in these new technologies which are revolutionizing the online broadcasting arena. Despite the numerous advantages of p2p streaming in general and p2p IPTV in particular, their characteristics in terms of signaling overheads and network efficiency are not well known. Unfortunately, the majority of above described systems are proprietary, and thus their protocols, architectures and algorithms are inaccessible [51]. Some of the IPTV applications are only regionally deployed, like PPlive and PPStream which are only available in China. According to [46], Joost is a p2p video streaming application with the potential of becoming one of the most contributors to traffic over the Internet in the near future.

III. MAIN CHARACTERISTICS OF P2P APPLICATIONS

Some important characteristics of p2p applications are scalability, transience, manageability and single point of failure. A network is said to be scalable when it operates efficiently in a large population of participating nodes. A transient network is network where nodes connect and disconnect at a high rate [5]. Manageability of the network includes removing or updating content; maintaining previous versions of updated content; managing storage space; and setting bandwidth limits [5]. When a single node can cause the network to malfunction, the node is considered as a single point of failure.

All these characteristics are to a great extent determined by what is called, the overlay network. The overlay network consists of a network of peer computers (nodes) and connections (edges) between them. This network is built on top of, and independently from, the underlying physical computer network (typically IP) [5]. A lot of the characteristics of KaZaa [16], for example, are deductable to the characteristics of the underlying FastTrack network because all applications which are running on the same overlay network have more or less the same properties. So, it is sensible to first look at the characteristics of the overlay networks and then to the characteristics of the applications of the networks. The two main characteristics of an overlay network are *structure* and *centralization*. Both will be discussed below. Scalability and ability to handle transient node populations are largely dependent on the structure of the overlay network. The centralization of the network determines whether the network is manageable and if it has a single point of failure.

A. Structure of the Overlay Network

The structure of the overlay network determines the type of routing algorithm used. The overlay network can be either structured or unstructured.

Unstructured p2p networks, also called 1st generation networks, are formed when the overlay links are established arbitrarily. The placement of content is completely unrelated to the overlay topology. The routing is mainly based on broadcasting and the search is based on keywords. Some routing algorithms used in unstructured networks are blind flooding, random walks, probabilistic flooding, breadth first flooding (used in Gnutella v0.4.), dept-first search (used in Freenet [26]) and JXTA search. This makes unstructured networks operate effectively in highly transient node populations, which can be considered as a major advantage [5]. Because the routing is mainly based on broadcasting, users have to accept a best effort search and the scalability (number of peers) of the network is limited. An approach to make unstructured networks more scalable is the use of a Time To Live (TTL) field for queries, which can reduce the network load. Of course, this reduces the chances for successful query hits [5]. Examples of unstructured systems

are Napster [7], Publius [34], Gnutella v0.4, FastTrack and Freehaven [25].

Structured p2p networks, also called 2nd generation networks, employ a globally consistent protocol to ensure that any node can efficiently route a search to some peer that has the desired file, even if the file is extremely rare [5]. Structured networks mainly use deterministic search based on Distributed Hash Tables (DHT). Often structured p2p networks are built on top of an existing routing algorithm, like PRR [52], Pastry [53], Tapestry [54], Kademlia [55], Chord [56] or CAN [57]. All these routing algorithms use DHTs. There are however routing algorithms in structured p2p networks, which are not based on DHTs, but these are rare. An example of such a routing algorithm is Mercury [58], which organizes nodes in a circular overlay and places data contiguously on this ring [3].

Structured networks have a number of advantages over unstructured networks. The most important is that they are more scalable, because they do not use broadcasting. Besides that structured networks are efficient in searching for rare data. Unlike unstructured networks, structured networks are not efficient in highly transient node populations, because the management costs of the DHTs are high [5]. Examples of p2p systems with a structured architecture are: OceanStore [29], Mnemosyne [31], Scan [35], PAST [33] and Freenet [26].

B. Centralization of the Overlay Network

Another aspect of the overlay network is centralization. The centralization of a p2p network can be expressed in terms of the location of the index. Index can be described as a collection of pointers to places where information can be found [4]. The index of a p2p network can be either centralized, distributed or hybrid. Each of these types is discussed below.

Centralized p2p networks have a single indexing server that keeps references to data on many peers in the network. Examples of networks using a centralized index are Napster [7], Publius [34] and BitTorrent [8]. The centralized indexing servers, which are often websites, are referred to as trackers. Famous trackers for the BitTorrent network are ThePirateBay [59] and Mininova [60]. Centralized networks are easy to implement, provide quick and efficient search and are simple to manage. Major disadvantages are the single point of failure (the centralized servers) and the fact that these networks are vulnerable to censorship and legal surveillance.

Most of the recently deployed p2p IPTV applications also adopt a centralized architecture, which is similar to the one in the BitTorrent network [8]. In this architecture data is divided into chucks in such a way which allows a peer to receive portions of the stream from different peers and assemble them locally [61]. When a new node registers to the system it receives the addresses of a number of trackers. A tracker is a central node that tracks the nodes that are downloading or have downloaded a file. When the node contacts the peers advertised by the tracker, the node receives from each of them a buffer map, that is, a map of the chunks of data they own and are able to share. At this point, based on various heuristics (e.g. bandwidth, delay), the node selects a subset of those peers and requests chunks from them [62]. Examples of p2p IPTV applications using this architecture are GNuStream [64], PPLive [47], Coolstreaming [65], SopCast [50] and Joost [49]. Due to the fact that each node relies on multiple peers to retrieve content, these mesh-based systems offer good resilience to node failures [62].

Distributed p2p networks, also called pure p2p networks, are completely decentralized. In these networks there is no central coordination of activities, which makes them difficult to manage, but also excludes the single point of failure. Users communicate directly to each other through a software application that acts both as a client a server. Pure p2p networks are not scalable, because the Time To Live (TTL) field of queries effectively segments the network into sub-networks [5]. Because of this, these networks are not widely used. Examples of distributed p2p networks are Gnutella v0.4, Freehaven [25], Freenet [26], PAST [33] and OceanStore [29].

Hybrid p2p networks, also called partially centralized networks, are similar to distributed p2p networks, but some nodes have a more important role in the network. These super-nodes act as local indexes for files shared by local peers, often called leaf-nodes (see Fig. 1).

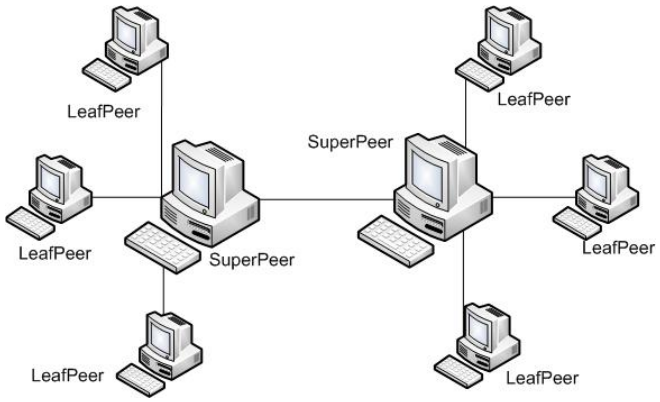

Figure. 1. A hybrid p2p network

In these networks there is a hierarchical structure, where the super-nodes become heavily loaded and the leaf-nodes are lightly loaded. The network structure of hybrid networks is a combination of structured and unstructured. The communication between super-nodes and leaf-nodes is still unstructured by means of query flooding, but the interconnection of super-nodes is structured. In this way these networks are more scalable than distributed networks, because the amount of query flooding is reduced [5]. In comparison to distributed networks discovery times are lowered because of the hierarchical structure. A disadvantage of these hybrid networks is that the dependability of the system is sensitive to the query success of the super-peers, which form the single points of failure. Nowadays a lot of p2p networks implement this hybrid structure, especially file sharing networks. Examples of file sharing networks using a hybrid architecture are Gnutella v0.6, FastTrack and DirectConnect.

Skype [40] is also an example of a hybrid network. This is not surprising when considering that Skype is based on the FastTrack network, which is also hybrid. Skype distinguishes normal users (leaf-nodes) and super-nodes. The super nodes

are selected among peers with large computational power and good connectivity (considering bandwidth, uptime and absence of firewalls) [43]. Skype uses the super-nodes for maintaining presence information of their users and locating other users by communicating with other super-nodes. In this way the Skype super-nodes are similar to the SIP registrar, proxy and presence server [63]. The communication between the super-nodes is based on DHT and the communication between users and super-nodes is based on some sort of flooding, similar to the FastTrack architecture [63]. Skype's user information (e.g. contact lists, status and preferences) is completely distributed among nodes [63].

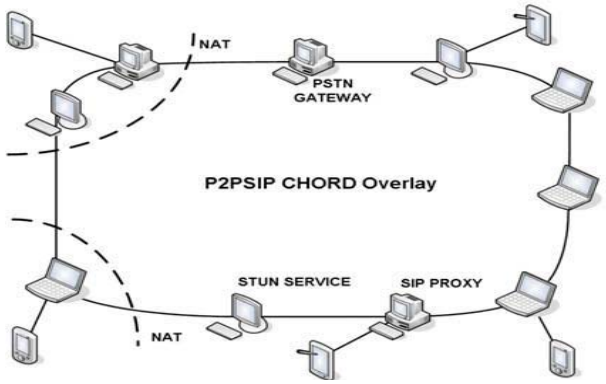

Figure. 2. example of P2PSIP network using a Chord overlay. The peers (e.g. the computers and laptops) form the overlay and the users (e.g. handheld devices) are connected to the peers, from [44]

P2PSIP shows many similarities with Skype. P2PSIP also uses a hybrid architecture in which it differentiates super-nodes, called peers, and leaf-nodes, called clients. The peers in P2PSIP are designed to override the SIP proxy and registrar functionality [44]. Together they form the active participants in the overlay network. This overlay network can be any DHT-based infrastructure, like Kademlia [55], CAN [57] or Chord [56]. The clients are nodes that use the resources offered by the peers, but they do not participate in network maintenance. This role is reserved to and should be used only by devices with very limited capabilities, such as the handheld devices [44]. In this way the number of clients is kept to a minimum and the number of peers participating in the DHT overlay remains as high as possible. An example of a P2PSIP network is shown in Fig. 2.

C. Security

A major drawback for p2p networks is their lack of security. The decentralization comes at a cost of less control over what is happening in the network. P2p networks lack a central control element, what makes them vulnerable to a wide range of attacks [42]. A number of common attacks on p2p networks is: Denial of Service (DoS) attacks; Eavesdropping; Eclipse attack; Forging messages; Free riders (defection attacks); Impersonation; Insertion of viruses to carried data; Invalid lookups; Filtering; Identity attacks; Malware in the peer-to-peer network software itself; Partition attacks; Propagating wrong routing tables; Spamming and Sybil attacks. Because of the difficulty to create safe p2p networks, security has become an important issue. This is especially the case for content publishing and storage systems, which are targeted towards creating a distributed storage medium in-and through-which users will be able to publish, store and distribute content in a secure and persistent manner [66]. They often aim to incorporate provisions for accountability, anonymity and censorship resistance, as well as persistent content management (updating, removing, version control) facilities [66]. Also for real time services like VoIP and IPTV, security is an important aspect. To lower the risks of the security attacks listed above, p2p networks can implement the following security services:

- **Authentication**: The process of determining whether or not some entity is in fact who or what that entity declares itself to be and not a malicious node with several identities (Sybil attacks) [5].
- **Authorization**: The process of giving an authenticated entity permission to do some action or access some resource [66]. In a p2p application, a peer might be authenticated to access some subset of the resources on another peer.
- **Access control**: Protects against unauthorized use of the network or its resources. This can be done by the use of signed certificates [5].
- **Encryption**: various cryptographic algorithms and protocols are employed to provide security for content published and stored in and routed through the p2p networks [5].
- **Anonymity**: there are several mechanisms to provide either anonymity to the author of the content; to the node storing the content; to the content itself and to the queries retrieving the content.
- **Accountability/Deniability**: mechanisms for a node being accountable for the data stored or transferred by the node. One way to deny accountability is to break the content into blocks and store them at different nodes.

It has been proven to be practically impossible to provide these security services in a fully distributed network. Because of that, a lot of p2p networks use central elements to provide security related tasks. Skype [40] for example use central login servers for authentication [42]. Because most p2p applications have a proprietary protocol it is difficult to say what security measures they implement. At the same time, the proprietary protocol makes it more difficult to build malicious software that can communicate with it.

D. Standardization

Up until now there are few p2p networks which use standardized protocols. Most of the p2p file sharing networks and content publishing and storage systems have their own protocol. A lot of these applications implements a DHT overlay network, like Chord [56], CAN [57] or Pastry [53]. None of these overlay networks is however considered as a standard.

After standardizing the Session Initiation Protocol (SIP) [37] for VoIP, the P2PSIP WG is now looking to develop a p2p-based VoIP communication protocol based on SIP. The

P2PSIP WG currently has two drafts describing the P2PSIP [41] and the RELOAD [45] protocol. Exactly when one of these protocols will be standardized is not known. The first p2p-based IPTV applications have only recently been deployed, so there are currently no standardized protocols.

E. Deployment

Not every application that has been developed is actually deployed. A lot of applications are scientific projects, which only run in test environments, but are never used in public. Especially with distributed storage & content publishing systems there are a lot of systems, like Intermemory [30] and Publius [34], which remain scientific projects. Also a lot of p2p TV applications are (yet) underutilized. The reason is that researchers are still searching for suitable architectures and protocols. Besides that p2p-based TV is a new service, so the impact on the market is not yet known.

IV. TAXONOMY BASED ON THE P2P CHARACTERISTICS

After analyzing what p2p applications are available and what their main characteristics are, it is now time to put them in some sort of framework. This framework, shown in Fig. 3, will help classifying p2p applications in relation to other p2p applications by distinguishing them by their main properties. What follows is a brief explanation of the proposed framework

The framework has a tree-based structure, where each level represents a property of a p2p application. The tree contains seven levels:

0. P2p application (the root of the tree)
1. Main type of service
2. Centralization of the index
3. Structure of the network
4. Deployment
5. Standardization
6. Security mechanisms used

The starting point is always the root (level zero). From the root a path downwards will be formed by making choices at each level of the tree. Because of space limitations not the entire tree is drawn; redundant braches are left out. For example, looking at level one there are four types of services to choose from. Each of these types has the same three possibilities for level two (type of centralization). So at level two there are four identical groups of three possible values. The groups can be identified by the dotted line around it. Because the properties below level two are exactly the same for each group, the remainder of the three has been drawn for only one group. In Fig. 3, this was done for the group below VoIP. In level three, four and five the same grouping structure is used to save space. For all of these levels, the groups from which the remainder is not drawn continue in the same way as the drawn group. At each level of the framework a unique choice has to be made. This means that for each property that the framework discusses, all p2p applications have a unique value. In this way every p2p application will form a single path in the tree. There is however one exception: namely level six, "security mechanisms used". A p2p application can implement multiple security mechanisms. So this is the only property that possibly has multiple values.

The framework shown in Fig. 3 does not list all properties of p2p applications. For example, pay mechanisms in p2p applications are not discussed. Many properties though are implied by the overlay network, as described in section two. The main properties of the overlay network are centralization of the index and structure of the network. This makes them important properties for classifying a p2p application. Both of these properties are taken into account in the framework.

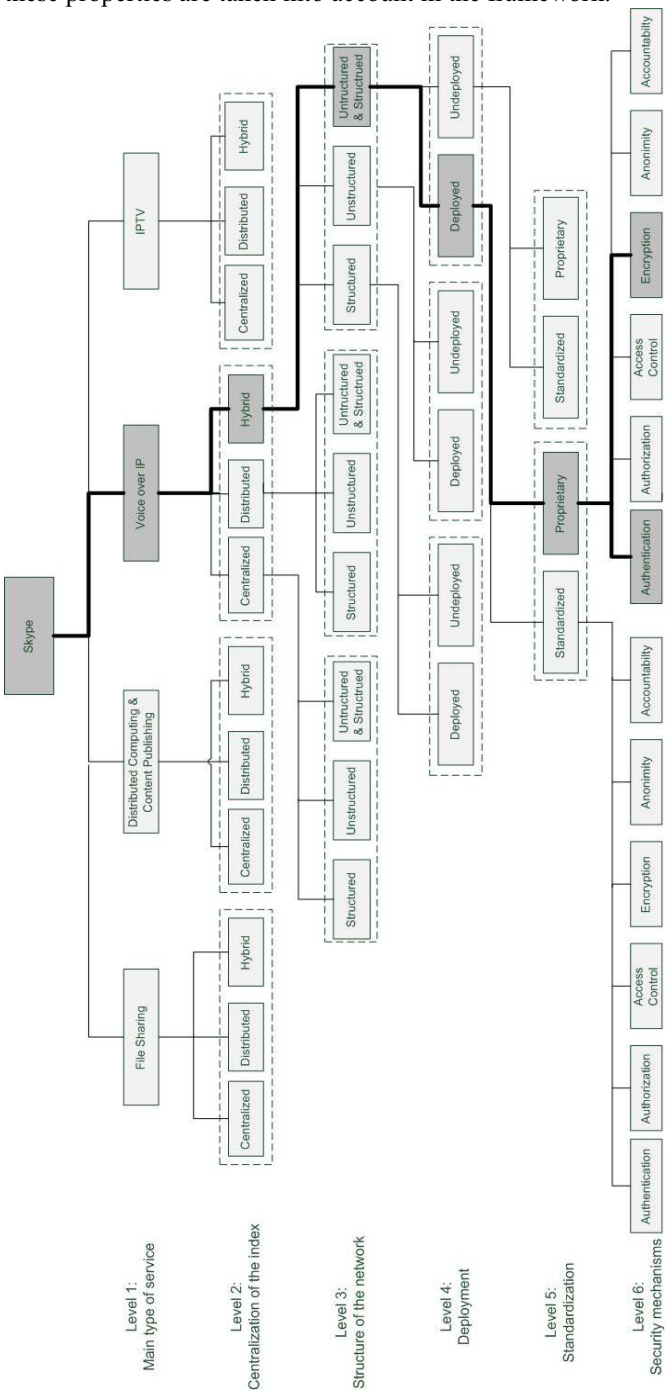

Figure. 3: Taxonomy framework. The highlighted path are the components of the application Skype [40]

V. CATEGORIZING P2P APPLICATIONS IN THE TAXONOMY

In order to explain how this framework can be applied, its use will be discussed by the popular p2p-based VoIP application Skype [40].

Skype

- **Main type of service:** The service offered by Skype is not limited to VoIP, but also includes video communication, file transfer and chat services. Skype's main service however remains VoIP.
- **Centralization of the index:** Skype uses a hybrid architecture, based on the FastTrack network. Skype distinguishes super-nodes and leaf-nodes.
- **Structure of the network*:*** The communication between super-nodes is structured, based on DHT. The communication between leaf-nodes and super-nodes is unstructured based on some sort of flooding, similar to FastTrack.
- **Deployment:** Skype is one of the most popular and widely deployed VoIP applications.
- **Standardization:** Skype uses a proprietary protocol.
- **Security mechanisms used:** Skype is based on a proprietary protocol, what makes it difficult to judge what security mechanisms it uses. It is known however that Skype uses a central server for authentication and uses some sort of encryption [42].

Table 3 summarizes the properties of Skype discussed above. Fig. 3, shows how Skype fits in the taxonomy framework. The properties of Skype form the highlighted path in the tree.

TABLE 3: PROPERTIES OF SKYPE

Skype	
Main type of service	VOIP
Centralization of the index	Hybrid
Structure of the network	Structured and Unstructured
Standardization	Proprietary
Deployment	Deployed
Security mechanisms used	Authentication control, Encryption. Rest is unknown

VI. CONCLUSIONS AND FUTURE WORK

In this paper a framework for classifying p2p applications has been presented. The framework is capable of classifying both old and recent p2p applications. The classification is based on (1) properties of the overlay network, (2) the service the application offers and (3) the security mechanisms it provides. Standardization and deployment have also been taken into account. The taxonomy framework can help classifying p2p applications by identifying the most important characteristics of the application. After classifying an application the hierarchical framework can also be used for indentifying sub- and super classes of the application.

Not all properties of p2p applications are discussed in the framework. However, the framework still provides enough properties to distinguish most of the available p2p applications. In this paper, attention is given to the overlay network of p2p applications. The introduced framework provides an accurate analysis of both available overlay networks and their properties.

In order to make the framework more complete a number of other properties have to be added to the framework. Performance issues, such as latency and congestion control, are not analyzed in this paper, because they require a quantitative comparison. This paper is based on a literature study and no quantitative measurements were done. Another aspect which requires future work is security. This paper provided a clear overview of the possible attacks on p2p networks and security mechanisms available. However, it is difficult to assess what security mechanisms are actually used, since most of the applications use proprietary protocols. The implementation of various payment mechanisms is also an issue that requires further research. Payment mechanisms are an interesting property of p2p applications and could be a useful addition to the framework.

REFERENCES

[1] Internet Research Task Force - Peer-to-Peer Research Group. [Online]. Available: http://www.irtf.org/charter?gtype=rg&group=p2prg (visited 2009, March 28)

[2] D. Bricklin (2001, June) "A Taxonomy of Computer Systems and Different Topologies: Standalone to P2P". [Online]. Available: http://www.bricklin.com/p2ptaxonomy.htm (visited: 2009, February 18).

[3] R. Ranjan, A. Harwood and R. Buyya. "Peer-to-peer-based resource discovery in global grids: a tutorial," Communications Surveys & Tutorials, IEEE , vol.10, no.2, pp.6-33, Second Quarter 2008.

[4] J. Risson and T. Moors. "Survey of Research towards Robust Peer-to-Peer Networks: search methods" *Computer Networks,* vol. 50, pp. 3485-3521, 2006.

[5] S. Androutsellis-Theotokis and D. Spinellis. "A survey of peer-to-peer content distribution technologies". ACM Comput. Surv. 36, 4 (Dec. 2004), 335-371

[6] IRTF, Peer-to-Peer Research Group (P2PRG) Home Page and Charter. [Online]. Available: http://trac.tools.ietf.org/group/irtf/trac/wiki/PeerToPeerResearchGroup (visited: 2009, March 28)

[7] Napster. [Online]. Available: http://free.napster.com/ (visited: 2009, May 27)

[8] BitTorrent. [Online]. Available: http://www.bittorrent.com/ (visited: 2009, May 27)

[9] uTorrent [Online]. Available: http://www.utorrent.com/ (visited: 2009, May 27)

[10] Vuze. [Online]. Available: http://www.azureus.com/ (visited: 2009, May 27)

[11] BitTornado. [Online]. Available: http://www.bittornado.com/ (visited: 2009, May 27)

[12] AresGalaxy. [Online]. Available: http://aresgalaxy.sourceforge.net/ (visited: 2009, May 27)

[13] DC++. [Online]. Available: http://dcplusplus.sourceforge.net/ (visited: 2009, May 27)

[14] eDonkey2000. [Online]. Available: http://www.edonkey2000.com/ (visited: 2009, May 27)

[15] eMule. [Online]. Available: http://www.emule-project.net/ (visited: 2009, May 27)

[16] KaZaa. [Online]. Available: http://www.kazaa.com/ (visited: 2009, May 27)

[17] Kazaa Lite. [Online]. Available: http://www.kazaa-lite-info.nl/index.php (visited: 2009, May 27)

[18] Limewire. [Online]. Available: http://www.limewire.com/ (visited: 2009, May 27)

[19] Shareaza. [Online]. Available: http://www.shareaza.com/ (visited: 2009, May 27)

[20] B. Mitchell. (2009, January). Morpheus P2P Application - Free Downloads. *About.com*. [Online]. Available:

http://compnetworking.about.com/od/p2ppeertopeer/qt/morpheusp2papp.htm (visited: 2009, May 27)
[21] Gnucleus. [Online]. Available: http://www.gnucleus.com/Gnucleus/ (visited: 2009, May 27)
[22] aMule. [Online]. Available: http://www.amule.org/ (visited: 2009, May 27)
[23] MLDonkey. [Online]. Available: http://mldonkey.sourceforge.net/ (visited: 2009, May 27)
[24] B. Mitchell. (2008, April). What Happened to the WinMX P2P Network? *About.com*. [Online]. Available: http://compnetworking.about.com/od/winmx/f/winmxstatus.htm (visited: 2009, May 27)
[25] Freehaven. [Online]. Available: http://www.freehaven.net (visited: 2009, May 27)
[26] Freenet. [Online]. Available: http://freenetproject.org/whatis.html (visited: 2009, May 27)
[27] Microsoft Groove. [Online]. Available: http://office.microsoft.com/en-s/groove/HA101656331033.aspx (visited: 2009, May 27)
[28] Mnet. Intro. [Online]. Available: http://mnetproject.org/intro (visited: 2009, May 27)
[29] The OceanStore Project. [Online]. Available: http://oceanstore.cs.berkeley.edu/info/overview.html (visited: 2009, May 27)
[30] Y. Chen, J. Edler, A. Goldberg, A. Gottlieb, S. Sobti and P. Yianilos. 1999. A prototype implementation of archival Intermemory. In *Proceedings of the Fourth ACM Conference on Digital Libraries* (Berkeley, California, United States, August 11 - 14, 1999). DL '99. ACM, New York, NY, 28-37. DOI= http://doi.acm.org/10.1145/313238.313249
[31] Mnemosyne Project. [Online]. Available: http://www.mnemosyne-proj.org/ (visited: 2009, May 27)
[32] MojoNation. [Online]. Available: http://sourceforge.net/projects/mojonation (visited: 2009, May 27)
[33] PAST: A large-scale, peer-to-peer archival storage facility. [Online]. Available: http://freepastry.org/PAST/default.htm (visited: 2009, May 27)
[34] Publius Censorship Resistant Publishing System. [Online]. Available: http://cs1.cs.nyu.edu/~waldman/publius/ (visited: 2009, May 27)
[35] Y. Chen, Y.H. Katz and J.D. Kubiatowicz. "SCAN: A Dynamic, Scalable, and Efficient Content Distribution Network" (2002). [Online]. Available: http://oceanstore.cs.berkeley.edu/publications/papers/pdf/pervasive_dtree.pdf (visited: 2009, May 27)
[36] M. Waldman and D. Mazières. 2001. Tangler: a censorship-resistant publishing system based on document entanglements. In *Proceedings of the 8th ACM Conference on Computer and Communications Security* (Philadelphia, PA, USA, November 05 - 08, 2001). P. Samarati, Ed. CCS '01. ACM, New York, NY, 126-135. DOI= http://doi.acm.org/10.1145/501983.502002
[37] Session Initiation Protocol (SIP). [Online]. Available: http://www.cs.columbia.edu/sip/ (visited: 2009, May 27)
[38] H.323. [Online]. Available: http://www.h323.org/ (visited: 2009, May 27)
[39] IAX: Inter-Asterisk eXchange Version 2. [Online]. Available: http://www.rfc-editor.org/authors/rfc5456.txt (visited: 2009, May 27)
[40] Skype. [Online]. Available: http://www.skype.com/ (visited: 2009, May 27)
[41] D. Bryan, P. Matthews, E. Shim, D. Willis. Concepts and terminology for peer to peer sip, Internet Draft draft-ietf-p2psip-concepts-02.txt, July 2008.
[42] A. Fessi, H. Niedermayer, H. Kinkelin and G. Carle. 2007. A cooperative SIP infrastructure for highly reliable telecommunication services. In *Proceedings of the 1st international Conference on Principles, Systems and Applications of IP Telecommunications* (New York City, New York, July 19 - 20, 2007). IPTComm '07. ACM, New York, NY, 29-38. DOI= http://doi.acm.org/10.1145/1326304.1326310
[43] D. Rossi, M. Mellia and M. Meo. "Understanding Skype signaling". (2009) Computer Networks, 53 (2), pp. 130-140.
[44] I. Martinez-Yelmo, A. Bikfalvi, R. Cuevas, C. Guerrero and J. Garcia. "H-P2PSIP: Interconnection of P2PSIP domains for global multimedia services based on a hierarchical DHT overlay network" (2009) Computer Networks, 53 (4), pp. 556-568.
[45] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, H. Schulzrinne. Resource location and discovery (reload), Internet Draft draft-ietfp2psip-reload-00.txt, July 2008.
[46] J. Moreira, R. Antonello, S. Fernandes, C. Kamienski and D. Sadok. "A step towards understanding Joost IPTV," Network Operations and Management Symposium, 2008. NOMS 2008. IEEE , vol., no., pp.911-914, 7-11 April 2008.
[47] PPlive. [Online]. Available: http://www.pplive.com/ (visited: 2009, May 27)
[48] PPStream. [Online]. Available: http://www.ppstream.com/ (visited: 2009, May 27)
[49] Joost. [Online]. Available: http://www.joost.com/ (visited: 2009, May 27)
[50] Sopcast. [Online]. Available: http://www.sopcast.com/ (visited: 2009, May 27)
[51] D. Ciullo, M. Mellia, M. Meo and E. Leonardi. "Understanding P2P-TV Systems Through Real Measurements," Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE , vol., no., pp.1-6, Nov. 30 2008-Dec. 4 2008.
[52] X. Li and C.G. Plaxton. 2002. On name resolution in peer-to-peer networks. In Proceedings of the Second ACM international Workshop on Principles of Mobile Computing (Toulouse, France, October 30 - 31, 2002). POMC '02. ACM, New York, NY, 82-89. DOI= http://doi.acm.org/10.1145/584490.584507
[53] Pastry. [Online]. Available: http://freepastry.org/ (visited: 2009, May 27)
[54] Tapestry. [Online]. Available: http://current.cs.ucsb.edu/projects/chimera/ (visited: 2009, May 27)
[55] Kademlia: a design specification. [Online]. Available: http://xlattice.sourceforge.net/components/protocol/kademlia/specs.html (visited: 2009, May 27)
[56] Chord. [Online]. Available: http://pdos.csail.mit.edu/chord/ (visited: 2009, May 27)
[57] S. Ratnasamy, P. Francis, M. Handley, R. Karp and S. Schenker. 2001. A scalable content-addressable network. In Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications (San Diego, California, United States). SIGCOMM '01. ACM, New York, NY, 161-172. DOI= http://doi.acm.org/10.1145/383059.383072
[58] A.R. Bharambe, M. Agrawal and S. Seshan. 2004. Mercury: supporting scalable multi-attribute range queries. *SIGCOMM Comput. Commun. Rev.* 34, 4 (Aug. 2004), 353-366. DOI= http://doi.acm.org/10.1145/1030194.1015507
[59] ThePirateBay. [Online]. Available: http://thepiratebay.org/ (visited: 2009, May 27)
[60] Mininova. [Online]. Available: http://www.mininova.org/ (visited: 2009, May 27)
[61] M. Alhaisoni and A. Liotta. "Characterization of signaling and traffic in Joost" (2009) Peer-to-Peer Networking and Applications, 2 (1), pp. 75-83.
[62] A. Sentinelli, G. Marfia, M. Gerla, L. Kleinrock and S. Tewari. "Will IPTV ride the peer-to-peer stream? [Peer-to-Peer Multimedia Streaming]," Communications Magazine, IEEE, vol.45, no.6, pp.86-92, June 2007.
[63] K. Singh and H. Schulzrinne. 2005. Peer-to-peer internet telephony using SIP. In *Proceedings of the international Workshop on Network and Operating Systems Support For Digital Audio and Video* (Stevenson, Washington, USA, June 13 - 14, 2005). NOSSDAV '05. ACM, New York, NY, 63-68. DOI= http://doi.acm.org/10.1145/1065983.1065999
[64] J. Xuxian, D. Yu, X. Dongyan and B. Bhargava. "GnuStream: a P2P media streaming system prototype," Multimedia and Expo, 2003. ICME '03. Proceedings. 2003 International Conference on, vol.2, no., pp. II-325-8 vol.2, 6-9 July 2003.
[65] CoolStreaming. [Online]. Available: http://www.coolstreaming.us/ (visited: 2009, May 27)
[66] A.A. Economides and A.A. Pomportsis. 2005. "Security in p2p networks". [Online]. Available: conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2006/security%20in%20P2P%20networks.pdf