The Tragedy of the Commons - Arms Race Within Peer-to-Peer Tools

Bengt Carlsson

Blekinge Institute of Technology, 371 25 Ronneby, Sweden

e-mail: **bengt.carlsson@bth.se**

Abstract. The two major concerns about peer-to-peer are anonymity and non-censorship of documents. Music industry has highlighted these questions by forcing Napster to filter out copyright protected MP3 files and taking legal actions against local users by monitoring their stored MP3 files. Our investigation shows that when copyright protected files are filtered out, users stop downloading public music as well. The success of a distributed peer-to-peer system is dependent on both cooperating coalitions and an antagonistic arms race. An individual will benefit from cooperation if it is possible to identify other users and the cost for doing services is negligible. An arms race between antagonistic participants using more and more refined agents is a plausible outcome. Instead of "the tragedy of the common" we are witnessing "the tragedy of arms race within the common". Arms race does not need to be a tragedy because these new tools developed or actions taken against too selfish agents may improve the P2P society.

1 Background

The Internet as originally conceived back in the late 1960s was fundamentally designed as a peer-to-peer (P2P) system (see [7] for a historical overview). The early Internet was more open and free than today's network. Generally any two machines could send packets to each other. Early client/server applications like FTP and Telnet had a symmetric usage pattern. Every host on the Internet could FTP or Telnet to any other host with servers usually acting as clients as well.

The Domain Name System (DNS), originally from the early 1980s, is an example of a system that blends P2P networking with a hierarchical model of information ownership. A DNS queries higher authorities about unknown names getting answers as well as new queries back. Name servers operate both as clients and as servers.

The explosion of the Internet in 1994 radically changed the shape of Internet into a commercial mass cultural phenomenon. People were connected to the Internet using modems, companies installed firewalls, and the initial structures broke down.

Uncooperative people use the Internet in their own interest without looking at the interests of the common. In the first half of the 1990s this was a surprising experience on the Internet. The "Green Card spam" 1994 appeared on the Usenet as an

advertisement posted individually to every Usenet newsgroup. The advertisers did not pay for the transmission of the advertisement; the costs were born by the Usenet as a whole. Today we have to assume that users behave selfishly and/or have commercial interests. This is a fundamental transition of the Internet and the main topic of this article.

With slow speed modem connections (and large phone bills), user patterns normally involved downloading data, not publishing or uploading information. Companies on the other hand hid their data behind firewalls making it hard to upload data from outside the firewall. By default, any host that can access the Internet can also be accessed on the Internet. Behind the firewalls this was no longer true making the need for a permanent IP address unnecessary for the end-user when IP addresses became in short supply. With dynamic IP addresses the single user is hard to find outside the local network.

Users were getting better computer performance and more applications, but with less authorities than in the early days of the computers. In the late 1990s programs started to bypass DNS in favor of creating independent directories of protocol-specific addresses. Examples are ICQ and Napster, the latter a tremendous success with over 80 million non-DNS addresses in less than two years.

A suggested litmus test that determines whether a system is P2P or not is suggested by [10]. If the answer to both questions below is yes, the application is P2P. If the answer to either question is no, it's not P2P:

1. Does it treat variable connectivity and temporary network addresses as the norm?
2. Does it give the nodes at the edges of the network significant autonomy?

P2P systems can be classified [6] into three main categories: hierarchical, centrally coordinated, and decentralized.

1. A hierarchical P2P system organizes peers into hierarchies of groups where communication is coordinated locally or passed upwards to a higher-level coordinator for peers communicating between groups. A DNS fulfills the requirements of the second question but uses permanent IP-addresses
2. In a centrally coordinated system, coordination between peers is controlled and mediated by a central server. SETI@home is a project trying to detect intelligent life outside earth, which distributes necessary data to millions of end-user computers during screen saving periods or as a process. Because of the biased information flow there is little autonomy left for the end-users, i.e. the significant autonomy criterion in the second question is not fulfilled. Napster stores pointers and resolves addresses of MP3 files and users centrally, but leaves the contents and sharing of the files at the users' machines. This is a true P2P system.
3. Completely decentralized P2P systems have no notion of global coordination at all. Communication is handled entirely by peers operating at a local level, where messages may be forwarded on behalf of other peers. Freenet is mainly focusing on preventing censorship of documents and providing anonymity for users on the Internet. An example is Gnutella which has been used for distributing MP3 music as well as picture and video files among end users.

We will examine the present development of centrally coordinated and decentralized P2P distribution of MP3 files within Internet using models taken from evolutionary biology. In section 2 the concept of the tragedy of the commons is discussed, followed by a description of the different P2P systems investigated. The

research results are described in section 4. P2P systems are further discussed in section 5, and finally some concluding remarks are made in section 6.

2 The tragedy of the commons

In the background section we have seen the transformation of the Internet from a typical cooperative platform to a highly competitive network. Deeper studies of the concept of human nature is outside the scope of this article but let us make some comprehensive statements about humans as biological beings and part of natural ecosystems.

Garret Hardin [5], using a game theoretic model of explanation, described the conflict between the individual and the common in "the tragedy of the commons" as follows:

"Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons. Freedom in a commons brings ruin to all."

Within the P2P field this metaphor is used by several researchers (e.g. [1,8] for explaining overexploitation of the resources.

So are we destined for being either definite controlled or vulnerable to a chaotic Internet? To answer this question we may look at other distributed, open systems capable of evolving robust behaviors based on autonomous selfish agents. Robustness is the balance between efficiency and efficacy necessary for survival in many different environments. A bio ecosystem exactly corresponds to these conditions. The main principle of a biological ecosystem is natural selection [12,13]. This selection, the survival of the fittest, happens among individuals, or agents, with opposed competing skills. A dynamic process, where the action of one agent is retorted by counter-actions taken by another agent, is starting an arms race. In the end one group of agents may form coalitions against another group, based on the needs of the individuals but dependent upon the success of the coalition (see also [3]).

Instead of looking for a central coordinator, the ecosystem emerges by the dynamics of the autonomous agents. This vision is shared by the recent FET (Future and Emerging Technologies) initiative "Universal Information System (UIE)" within the Information Society Technologies (IST) program of the European Commission[1] and by Internet Ecologies Area's[2] which focuses on the relation between the local actions and the global behavior of large distributed systems, both social and computational.

The global information infrastructure may be regarded as an emerging information ecosystem of infohabitants, or agents. Within information ecosystems infohabitants who may have opposite interests, perform the activities. This dynamic process may be compared to a biological view of describing ecosystems, where skills and interactions determine the success of the infohabitants. A biological system does explain the advantage of having cooperating agents within well performing

---

1 http://www.cordis.lu/ist/fetuie.htm**.**

2 http://www.parc.xerox.com/istl/groups/iea/

ecosystems, by its intrinsic dynamics. Such a robust ecosystem will eliminate the advantage for infohabitants of being too disloyal against the community.

Multi-agent system (MAS) has so far paid little attention to the ideas surrounding P2P computing although agent techniques have been applied to the design and implementation of interesting decentralized applications. It is intuitive to think of MAS as P2P systems, since many agents and/or hosts in MAS have been thought of as networks of equal peers. Similarly many existing P2P system can be thought of in terms of concepts developed by the MAS community, e.g., Napster can be thought of as a matchmaker

In our investigation, agents (and the users behind) are autonomous and selfish. Instead of focusing on normative agents, the emphasis is on the dynamics of a competitive system. The tragedy of the commons includes autonomous and selfish agents violating norms and starting an arms race.

3 Four different peer-to-peer systems for file sharing

We investigated four different P2P tools that range from centrally coordinated to completely decentralized systems. Napster and MusicCity represent centrally coordinated system while BearShare represents a decentralized system. The fourth tool, CatNap, encrypts MP3 files in order to bypass the filtering function of Napster.

3.1 Napster

Napster is connecting users using file registers. MP3 files are stored in the computers of the users, but Napster keeps a track of all the filenames. Originally Napster did not separate free and copyright protected music, which made the Recording Industry Association of America (RIAA) take legislative counter-measures. After a court order Napster must provide for songs to be blocked, by filtering out all copyright protected

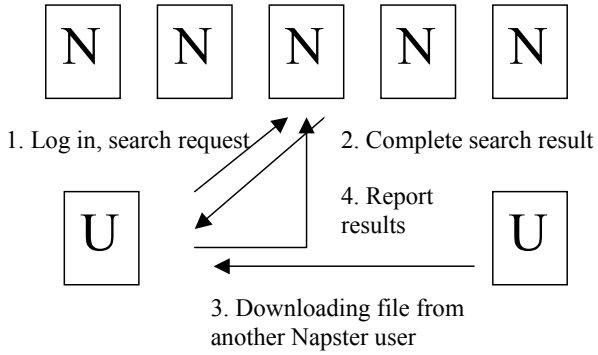

Fig. 1. Downloading files using Napster where N is the Napster server and U denotes the user.

songs from their file register. Downloaded music files both successful and interrupted are locally logged together with IP addresses in this investigation.

Using Napster for finding MP3 files is basically a client – service task finding the requested file and a client – client task transferring the file. As can be seen in Fig. 1 the protocol for doing this in principle involves only four steps. The user is doing a login and search request followed by a search result answer from the Napster server. The file is downloaded from another user and the result is reported back to the Napster server. It is possible for the Napster user to stop other users from downloading the locally stored files, i.e. a user may be selfishly.

3.2 BearShare

BearShare, a Gnutella client, is a distributed P2P tool connecting to at most seven other peers. It has a monitoring tool, which registers the download as before but also downloading time and original country for IP addresses.

A Gnutella P2P-tool uses a huge amount of communication compared to e.g. Napster. After an initial connection to a known Gnutella server a network of Gnutella servers are established. Unlike Napster there is no division into clients and servers at any stage of the service. A representative network includes connecting to four other servers and seven steps of message duration (time to live, TTL equal to 7). In all a server connects to over 4000 other servers.

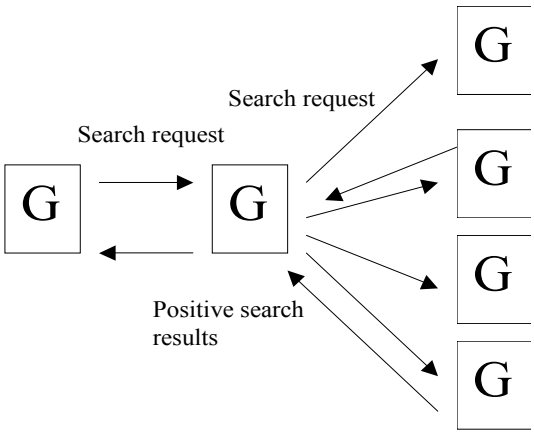

Fig. 2. Downloading files using Gnutella where G is the Gnutella server. Only a small fraction of the actual search space is shown.

In Fig. 2 the original Gnutella user is sending a search request to four other users (only one is shown in Fig. 2), which in turn send the request to four other users. With TTL = 7 the message passes five more steps. It is possible to broadcast across firewalls or to drop messages when connected to low-bandwidth networks. Positive

search results are sent back to the requester. The user is allowed to alter the settings of the protocol by changing the number of servers connected or changing the value of TTL. A remote P2P tool distributor may use agents inside the program to monitor and distribute the activities of a local peer. This so-called spyware is actually used by BearShare. A selfish user may enlarge the search area and prevent uploading local files. This subject will be further analyzed in the discussion section.

Gnutella may be seen as an information ecosystem of agents. Interactions among agents in both natural and information ecosystems may be regarded as a network of dynamically connected agents. In a small world model [11] the ecosystem is represented as a graph with edges connecting different vertices. The amount of interaction within the ecosystem is dependent on the amount of clustering between agents and the path length for reaching an arbitrary agent. Neither a graph with few neighbor connections nor a fully connected graph will do, because of high path length and low clustering respectively. A small world graph with the combination of high local clustering and short global path lengths will do better. Recently Albert et al [2] have shown that two randomly chosen documents on the web are on average 19 clicks away from each other

3.3 MusicCity

Like BearShare but unlike Napster, MusicCity does not maintain a central content index and is not currently subject to content filtering. A file may be downloaded using more than one source file. Like Napster but unlike BearShare, MusicCity is formally a closed system, requiring centralized user registration and logon.

3.4 CatNap

We also investigated CatNap, a program working within Napster encrypting MP3 files. CatNap users must convert their files before entering Napster in an attempt to fool the Napster filter. A user inside the CatNap mode has no possibility to participate in the ordinary Napster community, s/he will act as a parasite agent.

Filtering agents and encrypting agents supplement the user-controlled behavior Fig. 3 shows the essential agent interaction. The goal for the filtering agent is to stop copyright protected MP3 filenames to enter the file register. If other free MP3 files are also stopped, the filter has become too efficient. The CatNap files may pass the filter by encrypting the file names. We shall in the investigation part compare the filtered Napster society with a similar unfiltered one.

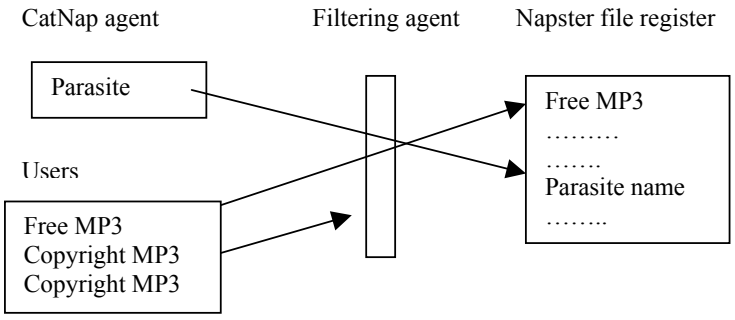

Fig. 3. The filtering function of Napster affected by a parasite agent.

4 Empirical Study

Three identically equipped computers were used during March to May 2001 to investigate Napster, MusicCity and BearShare. During the period MusicCity changed locations making it impossible to reach during several weeks. Also, there was no measurement available for the downloading via BearShare in the first half of the investigation period.

Napster and MusicCity both have centralized distribution of connecting different peers. This fact makes traffic analysis somewhat unnecessary at the end-user level, because much better predictions are done at central servers. BearShare's distributed propagation makes a local investigation necessary because only directly connected peers are involved in the file sharing. We concentrate our efforts on measuring the substantial contents instead of measuring the actual traffic. With Napster the network consists of 5.000 – 10.000 users (out of a population exceeding 1.000.000) and with MusicCity 15.000 – 35.000 users constitute the total number of logged in users for MusicCity.

The investigation of CatNap was done during a ten-day period, at the end of March 2001. Later on, Napster banned CatNap and other encryption programs by identifying encrypted files and blocking these users from Napster.

4.1 Average number of files

When Napster started to use filtering tools, the average number of files made available per user not surprisingly went down. In Fig. 4 bars represent this where the initial, non-filtered files amounted to about 200 per user. At the end of the investigation less than 50 files are left.

.

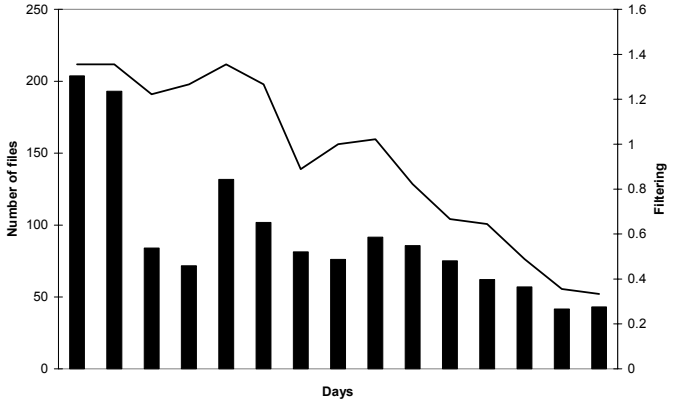

Fig. 4. Mean number of user files and filtering efficiency within Napster.

The measurring lasted for a month and a half, so every single day is not represented in the diagram. During the first month the efficiency of the filter varied due to a leaking filter. This is shown by the varying number of files in the middle section of the diagram.

During a ten-day period when the Napster filter was still leaking the number of files per user was compared for Napster, MusicCity and CatNap as can be seen in Fig. 5. Roughly MusicCity users twice the number of Napster users and CatNap twice the number of MusicCity users. CatNap files were measured by manually counting the number of files per user (totally 125 users). The MusicCity number of files per user is about the same Napster had before the discussion of filtering files started.

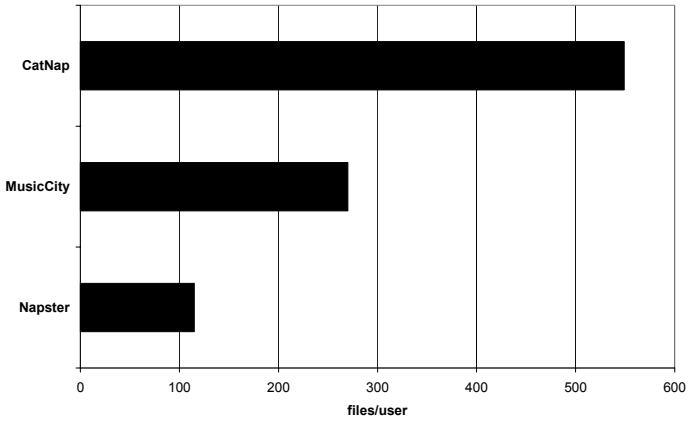

Fig. 5 Files per user for Napster, MusicCity and CatNap

A possible alternative explanation of the decreasing number of files would be that users with a lot of MP3 files were leaving Napster because of difficulties finding new

songs for downloading. To measure this a fixed number (n=61) of both public and copyright protected songs were monitored on a local site. The number of songs passing the filter was measured and an estimated number of songs supposed not to be filtered out are indicated as a filtering efficiency scale in Fig. 4. A filtering effiency close to 1 indicates a well functioning filter neither failing to filter out songs nor overreacting. As can be seen in Fig. 4 the filtering capacity pretty well follows the variation of the number of files. There is no indication of changing file-sharing behavior because of the filter.

4.2 Filtering efficiency

In Fig. 6 we investigated the proportion of files not filtered out by Napster (15 out of 61 files) compared to the filtered files. These filtered or public files are represented as the white parts of the bars for Napster, MusicCity and BearShare.

The investigation was done during on average 77 hours each period. After a peak in the beginning of April Napster almost disappeared. This decline expresses both the loss of filtered files and a decreased interest for remaining public files (a decrease to 1/8 of the public files peak value). MusicCity users had a 31 % and BearShare a 28 % increase of their downloading rate between the measurements, but no increase at all for Napster´s public files. Users are downloading proportionally more copyright protected files from BearShare and MusicCity.

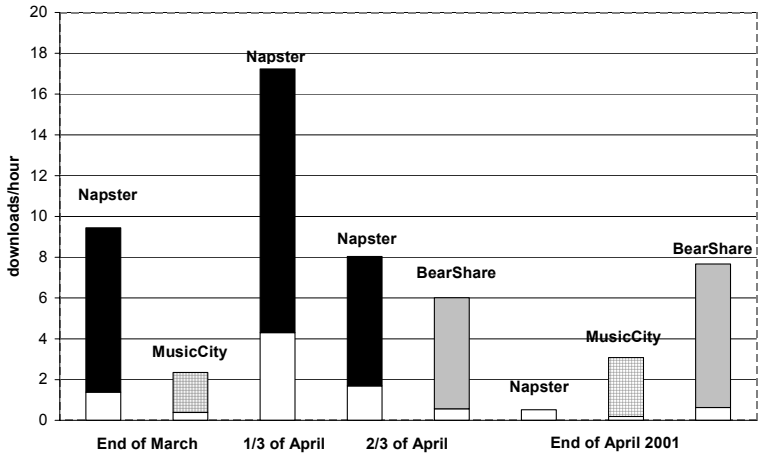

Fig. 6. Average number of downloads per hour for Napster, MusicCity and BearShare. White part of the bar represents files not filtered out by Napster.

4.3 Error rate

Next we compared the rate of errors when trying to download files. The measurements were done during a ten days period lasting for on average 125 hours for each tool.

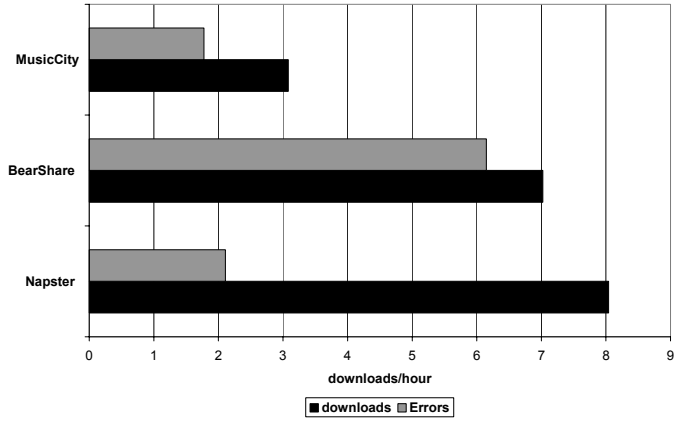

Fig. 7. Download and error rate for Napster, BearShare and MusicCity.

Fig. 7 shows that Napster has the lowest rate of errors. This is probably because Napster only allows one-to-one connections when uploading a file. MusicCity allows multiple sources and BearShare distributes a user´s uploads based on the capacity of the remote connection. Because of BearShare´s increased use of communication between peers the download rates are probably near the capacity limit for this connection.

On average it took 20 minutes and 32 seconds (average for 450 files) for downloading a file using BearShare with variations from several hours to a few seconds. For each file there was a mean transfer speed of 48 kbit/s. Napster and most of MusicCity downloading time for files were directly reflecting the speed of the remote connection.

4.4 User reactions

Users do react against Napster´s filtering function by misspelling artist names and songs. This is possible to do because it is the users naming both songs and artists for a certain MP3 file Fig. 8 below shows an example of that. Searching for artist name or full title returned no results, but searching for “Oops” did. Besides finding misspellings of the actual file, all other files withholding “Oops” will be found.

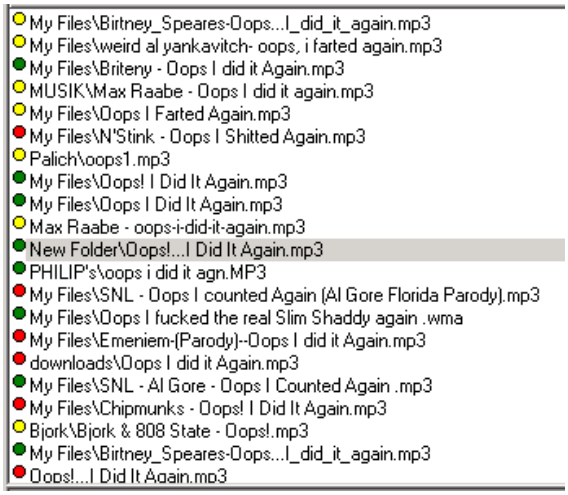

Fig. 8. An example of misspelling Britney Spears´Oops I did it again. Screen dump from Napster 05.10. 2001.

5 Discussion

Recently there has been a dispute about what the standards of a P2P file sharing MP3 music may look like. During the last year Napster has become the main tool for downloading MP3 music files, making it a candidate for being the standard within the P2P file sharing community. Its weakness is a lot of unsolved conflicts both towards the record industry and towards other P2P tools. The record industry wants to create a pay-for tool for downloading MP3 files. Napster uses centralized servers for connecting users.

5.1 File sharing

The basic P2P assumption was about cooperating, equal users sharing network resources. According to a recent report [1] almost 70 % of Gnutella users share no files, and nearly 50% of all responses are returned by the top 1% of sharing hosts showing that free riding is frequent. This may lead to degradation of the system performance. There is a risk for P2P systems being dependent on a few enthusiasts. The increased number of files for CatNap users probably shows this tendency. Such a system may be vulnerable because of lost interest or threats coming from the outside against these main contributors.

5.2 Copy-right protection

Napster will probably meet the demands from RIAA but at the cost of losing the vast majority of the users. As have been shown in Fig. 4 and 5 users leave Napster because there are very few sharing files left. More importantly, those public files left are to a less degree downloaded by users. The difficulties to calibrate the filter made it too efficient. A considerable large proportion of public files did not pass the filter. If the selection of files is reduced, the public or promotional files will be rejected as well. Our guess is that users will use other unfiltered tools rather than a pay-for tool partly because of financial issues and partly because of desires for unlimited search choices.

5.3 Agent interaction

In the presented work the focus is on investigating the behavior of users downloading MP3-files and to discuss present and future agent interactions. For both the filtering and parasite agents there is a risk of overreacting when trying to optimize MP3 file handling. This is partly due to insufficient calibration and partly to built-in constraints.

Facing the alternatives of joining a pay-for site or participate in collaborative behavior with other Napster users, they may behave more actively in keeping current possibilities for downloading files. Unfortunately this was not possible to prove within Napster because of a too efficient and too unpredictable filter. The Napster filter was tested by changing all filtered filenames by misspelling them within the test set of MP3 files. All filenames passed the filter but within two days they were found and filtered out again.

So, CatNap did not succeed very well in our investigation because the Napster filtering agent detected its strategy early. More fundamentally, there is a twofold risk for CatNap of being too small or too big. Why should a user keep her/his CatNap files if no one else does, or why should Napster keep its server if all users join the CatNap? To avoid disclosure, CatNap should hide from the filtering agent, but that means hiding from everybody else.

The Napster filtering agent aims at satisfying both the record companies and the users sharing MP3 files. At most the filtering agent should strictly filter out all copyrighted files but nothing else. This was not the case in our investigation. It was possible to find a lot of copyright protected music at the same time as all files (both copyright protected and public) at a single file sharer site were filtered out. The filtering agent has a mission impossible, making it a target for both the record companies' pay-for music sites and for other P2P freeloading sites.

5.4 Bandwidth sharing

When users are shifting from Napster to MusicCity or BearShare, bandwidth sharing will be the next subject of free riding. Both systems exploit faster connections for directing more traffic through these peers. The basic structure of BearShare also causes enlarged overhead because a lot more communication is necessary in a fully

distributed system. Both MusicCity and especially BearShare, as shown in Fig. 6, abort more transfers than Napster. A user may waste more and more bandwidth and processor capacity without getting anything back when joining these Napster alternatives. For the Internet as a whole it may end up even worse. Ritter [9] made an arithmetical problem of the Gnutella example presented in Fig. 2. He supposed a user sending an 18 bytes search string, ending up with a total data transmission of over 3 Mb[3]. If a user were allowed to send a request covering a society as big as Napster (we suppose 1 million users) the total data transmission generated would exceed 800 Mb.

5.5 Global access

File sharing needs global access because a single user does not normally choose who to connect to. The legal actions taken against Napster and in the future probably MusicCity may cause them to close down. There are also possible reactions against BearShare. It is possible to trace IP numbers to a specific BearShare user, since Internet-service providers store the information. Legal notices have already been sent to operators and users are informed they may be threatened legally by the RIAA.

Global access to the core Internet backbone is controlled by Internet backbone providers (IBP). These IBP consist of a few firms[4] mostly located in the US that secure access to the core routing structure, and access to all Internet addresses in the world [4]. Smaller regional Internet service providers are already charged for access to their global infrastructure and core routing services. The problem is also that, as more bandwidth is needed, the strategic importance of those countries that provide it also increases.

5.6 Future

In "the tragedy of the commons" an individual is always supposed to behave selfishly. But individuals within a natural ecosystem have relatives (kin selection within biology) and a possibility to pay and retort a favor from an unrelated neighbor. The success of the ecosystem is dependent on cooperating coalitions. An individual being part of a file-sharing ecosystem will benefit from cooperation if it is possible to identify (real names or pseudonymous) users and/or the cost for doing services is negligible. We found a few such behaviors with users changing file names and joining encrypting programs. In the future, agents may be designed to find other cooperating users or to avoid controlling IBP's, resulting in more or less locally connected groups with their own norms.

A possible future scenario includes but is not restricted to:

- Pay-for music sites are visited by a restricted number of users because people are used to getting downloadable material for free on the Internet.

---

[3] An 83 byte data packet sent to 4372 users. The mean number of responses (12%) and the amount of data sent back must also be calculated.

[4] MCI WorldCom, Sprint, GTE, AT&T and Cable & Wireless control between 85% and 95% of the total backbone traffic in the US (Cremer et al 1999).

- The P2P tools providers increasingly get their profit from advertising banners and spywares.
- Users have to invest more in bandwidth and technical upgrading.
- New file protection systems like watermarking makes it harder to copy music files but may also reduce the audio quality.

None of the issues above will result in a better-organized file sharing system. RIAA will still have problems getting money out of freeloading users. The new P2P tools will include features not desired by the users. Users have to invest more in technical resources without getting a better audio quality.

6 Conclusions

The two major concerns about P2P are: anonymity and non-censorship of documents. The music industry has highlighted these questions by:

- Forcing Napster to filter out copyright protected MP3 files
- Taking legal actions against local users by monitoring their stored MP3 files

Our investigation shows that when copyright protected files are filtered out, users stop downloading public music as well. When MusicCity and BearShare are replacing Napster, there is an increase in downloading copyright protected files compared to downloading public files. This alteration is contrary to the purpose of introducing a filtering function.

When former Napster users are leaving for other P2P tools, this causes higher bandwidth usage for these users and thus increases the communication needs over the Internet. The Napster alternatives MusicCity and especially BearShare consume more resources both by default and, as shown in our investigation, by having a higher rate of aborted file transfers.

Basically a P2P system consists of a society of equal peers. With central content index, centralized user registration, logon and introduced spywares this is no longer true. There is one group of peers supplying the tools and one group using the tools. Within and between the groups conflicting interests should be expected. The view introduced in this paper treat peers as similar to an (information or biological) ecosystem of agents controlled by Machiavellian beings behind.

The success of a distributed peer-to-peer system is dependent on both cooperating coalitions and an antagonistic arms race. Users may cooperate, i.e. allowing uploading from other users and/or bypass Napster´s filtering function by misspelling or encrypting files. Adar and Huberman [1] have shown the unwillingness for a majority of users to share files and our investigation shows no major tendencies for systematically bypassing Napster´s filtering function. More in general; an individual within the user group will benefit from cooperation if it is possible to identify other users and the cost for doing services towards other users are negligible. In practice it is sufficient to have a fraction of the users cooperating to maintain a well performing system. In Napster there is still some incentive for being cooperating because such a user is not anonymous. In BearShare and MusicCity other users are more anonymous because one MP3 file may be downloaded from multipe sources.

An arms race between antagonistic participants using more and more refined agents is a plausible outcome. Napster´s filtering agent and Catnap, a parasitic agent, are examples of such agents. They fulfill some temporary needs and may probably be replaced by other agents. A possible future agent may be a "bandwidth stealing" agent or a "bandwidth protecting" agent. Users getting used to downloading everything for free has to decide about joining a pay-for service or accepting more power consuming P2P tools with an increased personal effort. Despite legal actions, performance deficits and the strength of commercial forces an uncensored P2P community will probably survive because there are too many new tools developed with innovative new solutions. Instead of "the tragedy of the commons" we are witnessing "the arms race within the commons". Arms race does not need to be a tragedy because these new tools developed or actions taken against too selfish agents may improve the P2P society.

Acknowledgements
I would like to thank Paul Davidsson, Magnus Boman, Ingemar Jönsson and the anonymous reviewers for their comments on various drafts of this work and Martin Hylerstedt for proof reading.

References

1. Adar, A. and Huberman, B.A., Free riding on Gnutella, FirstMonday peer-reviewed journal on the Internet http://firstmonday.org/issues/issue5_10/adar/index.html (2000)
2. Albert, R., Jeong, H., and Barabási, A.-L. Diameter of the World-Wide Web, Nature vol. 401 pp. 130-131 (1999)
3. Carlsson, B. and Davidsson, P., A Biological View of Information Ecosystem, to be presented at IAT'2001, (2001)
4. Foros, Ø., and Kind, H.J., National and Global Regulation of the Market for Internet Connectivity http://www.berlecon.de/services/en/iew3/papers/kind.pdf (2001)
5. Hardin, G. The tragedy of the commons, Science vol. 162 pp. 1243-1248 (1968)
6. Hong, T. Performance in Oram A., ed., Peer-to-peer Harnessing the Power of Disruptive Technologies O'Reilly Sepastopol CA (2001)
7. Minar, N., and Hedlund, M., A Network of Peers in Oram A., ed., Peer-to-peer Harnessing the Power of Disruptive Technologies O'Reilly Sepastopol CA (2001)
8. Oram A., ed., Peer-to-peer Harnessing the Power of Disruptive Technologies O'Reilly Sepastopol CA (2001)
9. Ritter, J., Why Gnutella can't Scale. No, Really. http://www.darkridge.com/~jpr5/doc/ gnutella.html 05.31.2001 (2001)
10. Shirky, C., Listening to Napster in Oram A., ed., Peer-to-peer Harnessing the Power of Disruptive Technologies O'Reilly Sepastopol CA (2001)
11. Watts, D.J., and Strogatz, S.H., Collective dynamics of "small world" networks. Nature vol. 393 pp. 440-442 (1998)
12. Williams, G. C., Adaptation and natural selection, Princeton University Press (1966)
13. Wilson, E.O. Sociobiology - The abridged edition. Belknap Press, Cambridge (1980)