

Anonymous Self-organizing Adaptive Peer-to-Peer Publication System (ASAP3)

Steffen Larsen – zool@diku.dk

October 6, 2005

Introduction

This document contains a description of a ongoing project written by Steffen Larsen at Copenhagen University, Department of Computer Science (DIKU). The document is a part of a written project done on a course called “Written projects in data nets”. This written report will be called “Anonymous Self-organizing Adaptive Peer-to-Peer Publication System”, and will be finished winter 2005. Supervisors on the project will be Per Høgh (phoegh@diku.dk) and Klaus Hansen (khan@diku.dk).

Motivation

Our interest became more and more awaken, because of the fast flowing Peer-to-Peer software that were becoming available. Also the Peer-to-Peer software as KaZaa, GnuTella and Bit-torrent has changed the way that the consumers used the Internet for publishing and retrieving documents instead of the old-fashion File Transfer Protocol (FTP) style. Our goal though, is to have some kind of **Freedom of Speech** and be able to use the rights of freedom to allow individuals to speak freely without further persecution. Our project would allow users to publish and retrieve information which should resemble the World Wide Web (WWW), but without the fear of being censored or survailanced by any government or any other organization like in eg. China (see (?)) and some countries in Africa etc (which is often suppressed by their own governments). This will of cause also bring up some moral issues as evil organizations as terror cells, Nazi propaganda etc. also has the potential to use this kind of freedom.

Project Summery

What we will try to design is an anonymous publication system which is adaptive, so that peers can join and leave without harming the infrastructure in the system. With publication system we mean the ability that allow people to publish (send) documents anonymously and other people as well to retrieve the material as an anonymous.

We will of course cover the abilities and frameworks that lies behind the idea of Peer-to-Peer (P2P) technology. In the same context we will try to address the problems and advantages that lies in this area, such as: robustness, scalability and availability. When this is covered, we will try to outline what kind of problems this will emphaze when we are doing an anonymous system instead of a non-anonymous one. Due to our interest, we will try to analyze the current available anonymous P2P systems, and evaluate them and extract the best of practice out of them and use what ever we can based on our design.

We will look at the abilities to keep different types and levels of anonymity and how to keep integrity and robustness of the published material and how to make this kind of secret sharing in an distributed environment. In the same section when we introduce the levels of anonymity, we will try to act as an attacker on the system (advisory) and thereby profile our system and come with some kind of counter-attacks. We will also investigate how we can build up a reputation scheme and maintaining a trust model etc. in this anonymous system if needed.

Design requirements

We will in our design of the anonymous publication system, strive to provide the publisher and the reader/retriever as much as anonymity as possible. Because anonymity is such a wide definition, we will have to explicit try to define, what it means in our context:

Publisher Anonymity To be able to anonymous publish a document into our system, such that it is un-linkable to the publisher.

Recipient Anonymity To be able to anonymous retrieve a document from the system, such that it is un-linkable to the recipient.

Relationship Anonymity A property in which the publisher and recipient can not be linked together.

Location Anonymity When retrieving a document, it should be unable to see which server we get it from or at least satisfy some kind of **deniability**.

Author Anonymity The author can be the same as the publisher or not. Either way the author should be able to deny every kind of linking of the document.

With this terms in mind, we can also add some other requirements:

- To make the system robust to failures and scalable
- To make a system that is adaptive for leaving and joining.
- Allow the users to share a specified area of local disk space with other peers anonymously.
- The material on the disk should probably be encrypted and not known of (deniable).
- Make the published document easily/effectively retrievable
- Make sure of the integrity of the document and validating that it is the original

To make a quick summery, we will strive to:

- Get a fundamental understanding on Adaptive peer-to-peer systems.
- Get a understanding on how we obtain anonymity in a peer-to-peer publication system and evaluate these techniques
- Make a design that will meet the demand of best practice according to our design requirements.
- Implement our design, when it is ready and thereby propose a proof of concept and make a small working network if we got the time(tm).

Deliverables

To make a brief summary; we will in this project deliver a report that will cover an analyze and empirical work on the current platforms of anonymous peer-to-peer systems. Afterwards we will tend to see if we can use some of the current knowledge in these implementations and bring it together and make a better design that will fulfill our requirements. We will look at abilities to keep different types and levels of anonymity and still keep the integrity and robustness of the published material due to our requirements.

References

- [1] www.gnutella.com
- [2] www.freenet.com
- [3] www.jxta.org
- [4] <http://mixminion.net/>
- [5] www.politiken.dk (the 27th. september (15:18))

Signatures

Steffen Larsen Per Høgh Klaus Hansen