Aretusa, reputation system for BitTorrent

Jaime Prez Crespo
Middleware Engineer
RedIRIS / Red.es
Edificio Bronce, Plaza de Manuel Gomez Moreno, s/n
28020 Madrid, Spain
jaime.perez@rediris.es

Keywords

Aretusa, BitTorrent, reputation, eduGAIN, Public Key Infrastructure

Abstract

Peer to peer applications are a powerful way to share contents within a network, scalable and efficient. At least theoretically, due to a problem that peer to peer protocols have, known as free-riding. *That means any peer is able to download at the maximum rate without even sharing a single byte with other peers in the network. This paper proposes an extension to BitTorrent protocol to try to avoid this problem and enhance the BitTorrent protocol to allow its massive usage.*

1. Introduction

While the federation of applications has become widespread, its usage has gone far away than the usual *single sign on* use case. Nowadays, federation is an useful tool to provide ubiquitous identity for everyone, everywhere. Architectures such as eduGAIN make possible to interconnect federations themselves, so it can be considered a further step on the concept of federation. The JRA5 team from Geant2 works hard to develop a stable and feature rich confederation infrastructure to build higher level applications on top of it. Aretusa is one of those next generation, higher level applications. It uses the capabilities of eduGAIN and the concept of confederation to build an extension to BitTorrent protocol which will take care of the reputation of all the peers on a confederated peer to peer network. Using this as our starting point, we have the basis to do further research on peer behavior analysis and reputation assignment.

It's easy to imagine multiple use cases for the proposed architecture, from the usage on educational networks to share data, to secure, private sharing networks.

2. eduGAIN

eduGAIN is an AAI architecture developed by the JRA5 team from Geant2 to provide a common authentication and authorization infrastructure, unifying the existent ones, like *Shibboleth*, *PAPI*, *A-Select* among others. It makes use of the SAML (*Security Assertion Markup Language*) language, XML based, to allow federations exchange information on what we call a *confederation*. As it is a decentralized, open architecture that uses a well known standard like XML, it is virtually possible to connect any AAI software to it.

3. The free riding problem

Free riding is a common problem of peer to peer networks, and BitTorrent protocol is not free from it. It is basically the selfish behavior of peers downloading contents at full speed from other peers without even sharing a single byte with them. This kind of behavior makes the peer to peer concept break itself, as if no one shares, no one will obtain any benefit at all. Free riding makes peer to peer networks inefficient and results in a waste of resources and a lack of confidence from the user's point of view.

To solve such a problem we must follow two single steps:

1. First of all, identify univocally any peer on the network. Note that here *network* stands for a whole bunch of peer to peer networks, consisting on BitTorrent trackers and their peers.
2. Once we have identified peers, follow their behavior every time they use the network, and keep track on it. This is done by means of *reputation*, which can be seen as a single value describing the behavior of the peer in the past.

4. A solution: Aretusa

Given some indications to solve the free riding problem, Aretusa is our implementation approach. It consists on an extension to BitTorrent protocol, adding several new interactions between peers, trackers and new components, to identify them, query and notify their reputation and act in consequence.

Identification Peer authentication is achieved by means of a Public Key Infrastructure that guarantees the identity of peers and trackers in the system with X509 certificates. Peers must exchange their certificates so that they can authenticate and even authorize (based on their known reputation) each other and then share data across the network.

A very simple protocol, built on top of Azureus Messaging Protocol, is the key to exchange certificates between peers. Just two messages carrying their respective certificates will be enough.

Reputation querying Peers will be able to query the reputation of other peers willing to download from them by finding and asking the trackers *responsible* for them. As we want to provide ubiquity, we need to associate each peer to a single tracker on our confederated network, which will track their reputation throughout the time they use it. That's why we talk about a tracker being *responsible* for a peer.

Reputation notifying Just like reputation querying, we'll need to find the tracker responsible for a peer to tell it our experience with that peer (whether if it was good or not). Obviously, this can be used with malicious purposes, so our own reputation must be used to weight the values we are notifying.

Searching for federations As our approach takes each tracker and its peers as a single federation, we need a way to search for peers or trackers across networks. This is done by means of a Meta Data Service, provided by eduGAIN. This allows peers to move between trackers and keep track of their reputation over the whole network.

5 Author Biographies

Jaime Perez works as a Middleware Engineer at RedIRIS since November 2006. He got a Computer Science Management Technical Engineering Bachelor's degree at the Rey Juan Carlos University of Madrid in 2004. Currently he is finishing his Computer Science Engineering degree at the same University, where he was working for more than two years before joining RedIRIS.

6 Full Paper

The author plans to submit a full paper for the TERENA Networking Conference 2008.