Red IRIS

Universidad Rey Juan Carlos

Aretusa
Sistema de reputación para BitTorrent

Jaime Pérez
jaime.perez@rediris.es

Red IRIS

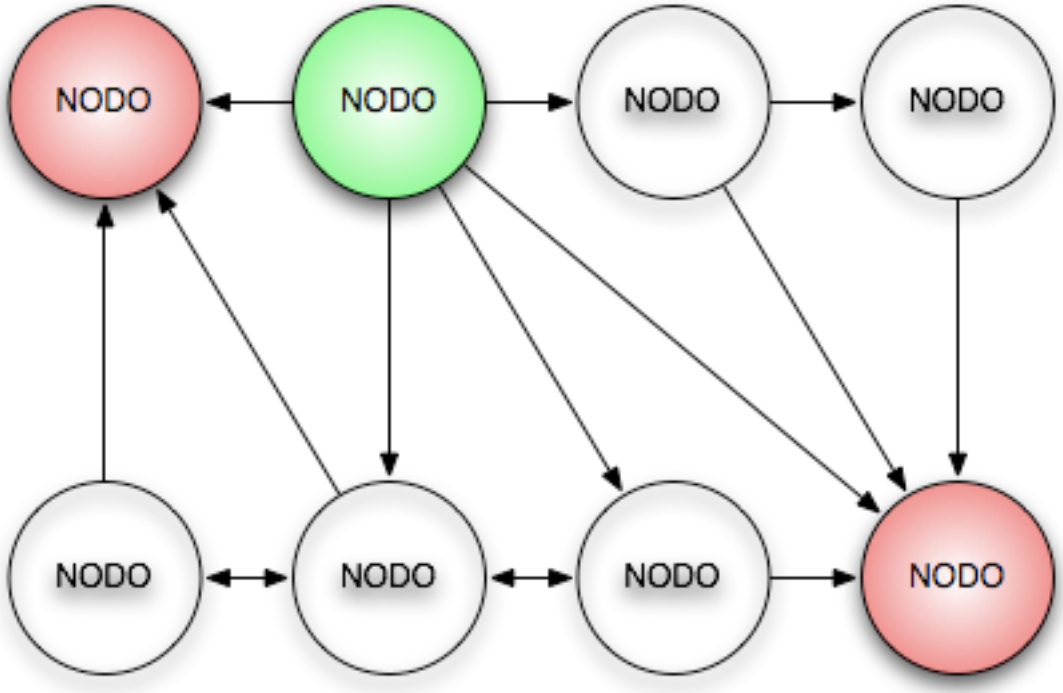
Universidad Rey Juan Carlos

ÍNDICE

- Introducción: *free-riding* y BitTorrent.
- Objetivos.
- Solución propuesta.
- Arquitectura.
- Implementación.
- Conclusiones.
- Trabajo futuro.

INTRODUCCIÓN: P2P

- En una red entre pares, un conjunto de nodos colaboran entre sí para obtener un recurso.



INTRODUCCIÓN: FREE-RIDING

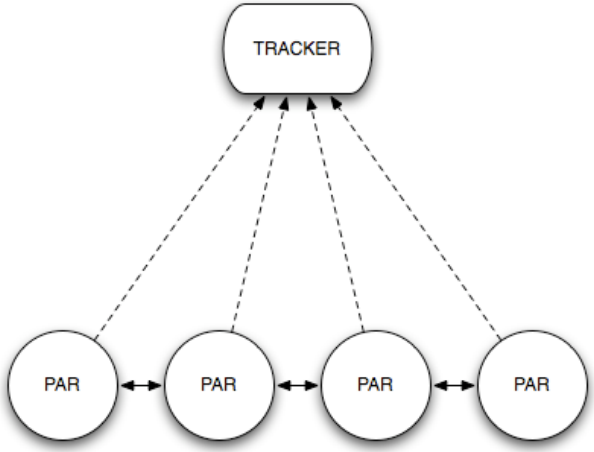
- ¿Qué es el *free-riding*?
- Básicamente: hacer trampas.
- Formalmente: el uso incorrecto de una red entre pares para obtener un recurso sin ofrecer nada a cambio, en contra del paradigma de este tipo de redes.

INTRODUCCIÓN: BITTORRENT

- Red entre pares semi-centralizada.

  Trackers: distribuyen información sobre los nodos interesados en un recurso.

  Pares: comparten esfuerzos para obtener el recurso.



INTRODUCCIÓN: BITTORRENT Y FREE-RIDING

- BitTorrent implementa medidas para evitar el abuso de la red.
- Permite bloquear y desbloquear pares de modo que no se comparte con ellos.
- Es insuficiente: el "*optimistic unchoke*" permite desbloquear pares aleatoriamente cada cierto tiempo.
- Resultado: es posible aprovecharlo para hacer *free-riding*.

INTRODUCCIÓN: BITTORRENT Y FREE-RIDING

- Existe una demostración práctica: BitThief.

  http://dcg.ethz.ch/projects/bitthief/

- Permite descargar contenidos incluso más rápido que el cliente oficial de BitTorrent.
- Nunca comparte nada de lo que obtiene con otros pares.

OBJETIVOS

- Diseñar una solución al problema del *free-riding* en redes BitTorrent.
- Implementar dicha solución sobre algún cliente de BitTorrent ya existente, extendiendo el protocolo original de BitTorrent como sea necesario, pero alterándolo lo menos posible.

SOLUCIÓN PROPUESTA

- No parece posible eliminar por completo el problema...
- Pero sí se puede reducir en gran medida.
- La solución propuesta pasa por construir un sistema de reputación que refleje el comportamiento de los pares de la red.

SOLUCIÓN PROPUESTA

- Dos requisitos para construir el sistema:
  - Identificar a los pares de la red de forma unívoca y persistente.
  - Almacenar un historial de comportamiento en la red asociado a cada identidad única, en forma de reputación.

SOLUCIÓN PROPUESTA

- Identidad digital de los pares:
  - La identidad debe ser única en cualquier red BitTorrent.
  - Cada red BitTorrent debe comportarse de forma “federada” con respecto a las demás.
  - La identidad debe preservarse cuando los pares se mueven de una red a otra.

SOLUCIÓN PROPUESTA

- Mantener la reputación de los pares:
  - Los pares deben notificar el comportamiento de otros pares cada vez que interactúen con ellos.
  - La reputación debe almacenarse en alguna parte: *trackers*.
  - Cada par tendrá una organización responsable de su identidad y su reputación.

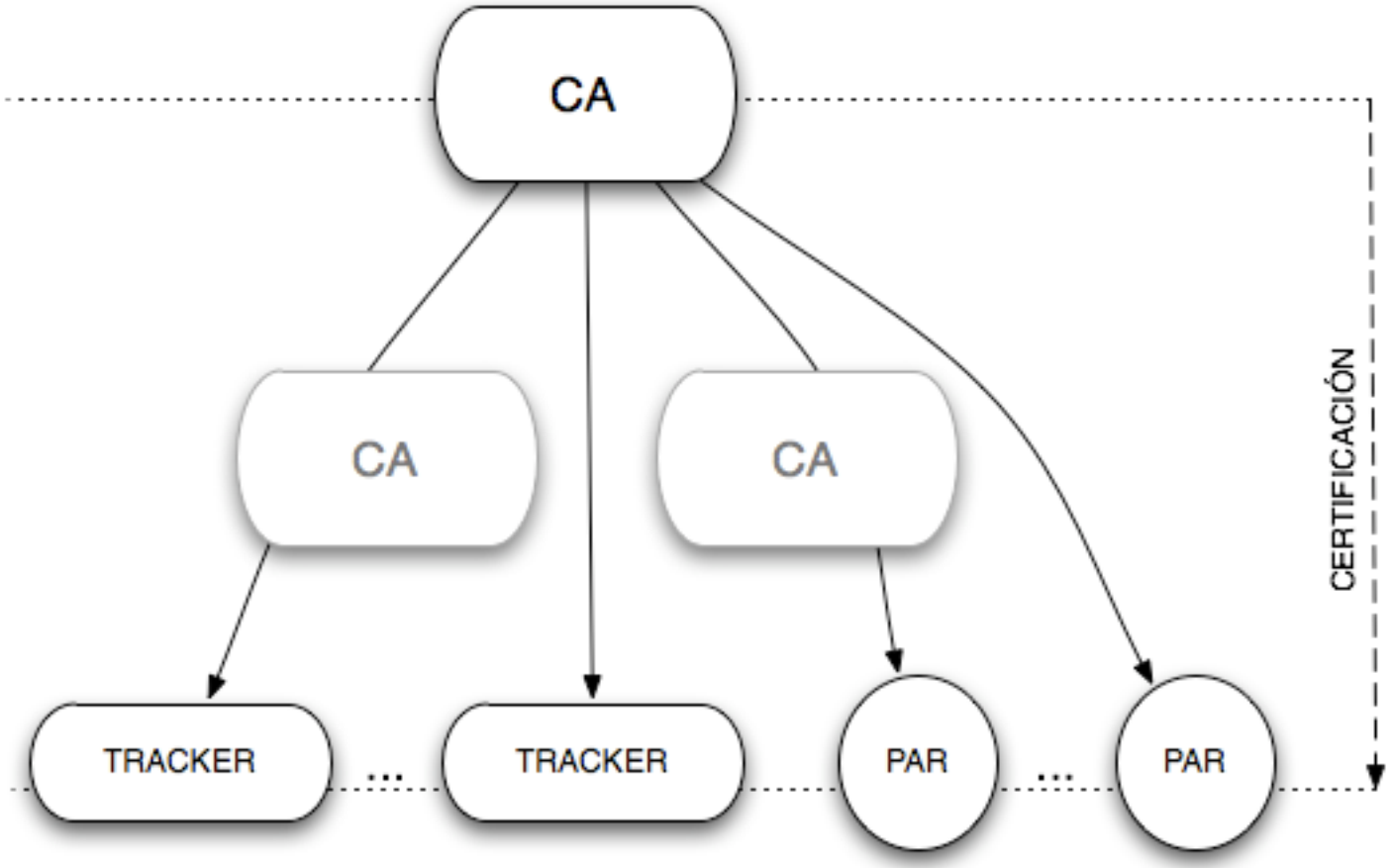
ARQUITECTURA

- Los *trackers* almacenan la reputación.
- Los pares preguntan y notifican a los *trackers* la reputación de otros pares.
- Un par decide si compartir o no con otro en función de la reputación del segundo.
- Todo esto es posible utilizando certificados y una infraestructura de clave pública para garantizar la identidad de pares y *trackers*.

ARQUITECTURA

- Autenticación entre pares:
  - Cuando se abre una conexión entre dos pares, éstos intercambian sus certificados.
  - Los certificados se validan contra la infraestructura de clave pública, para asegurar la identidad.
  - De esta forma los pares se pueden mover de una red a otra.

ARQUITECTURA



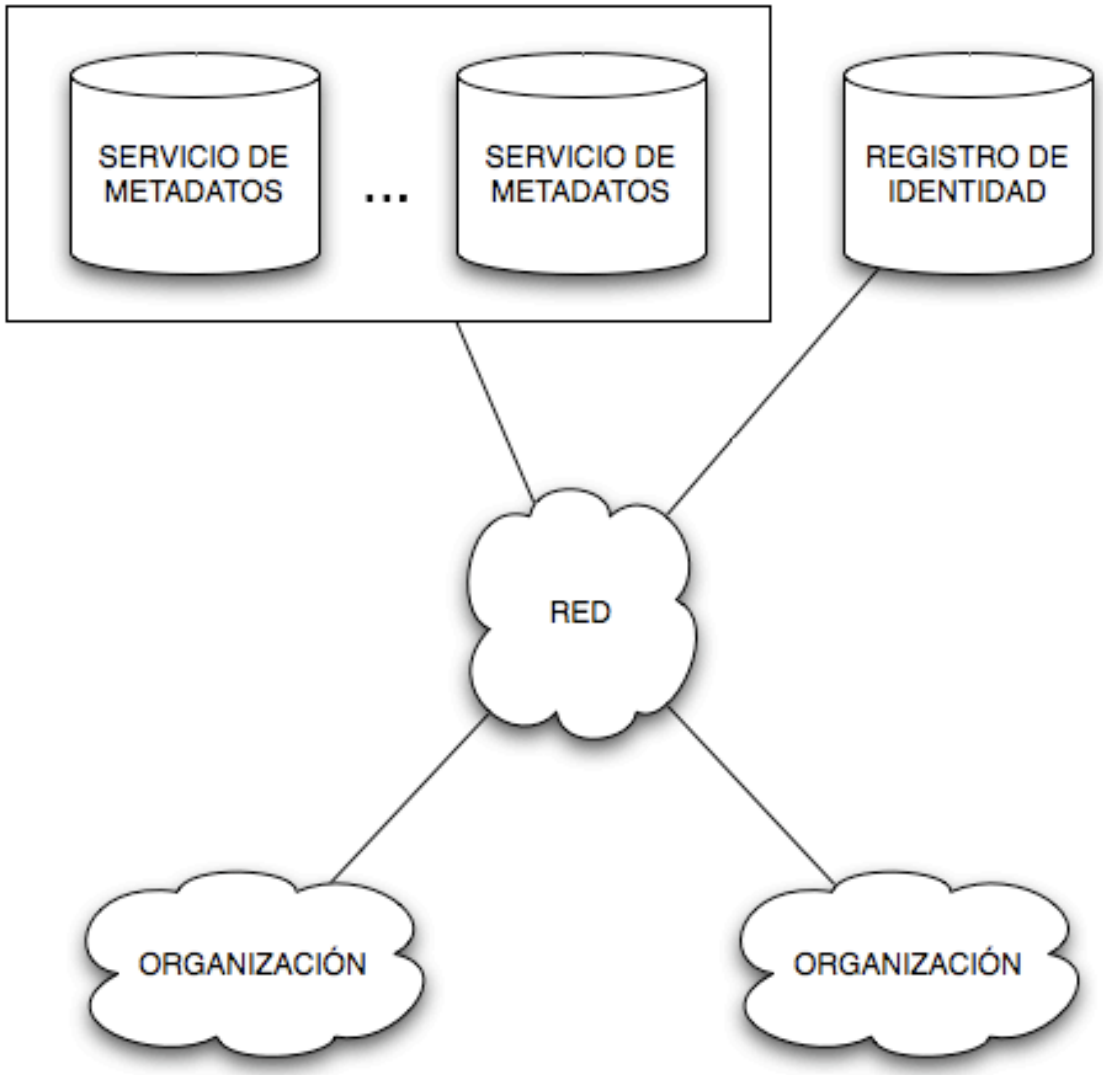
ARQUITECTURA

- Petición/notificación de reputación:
  - Los pares preguntan al *tracker* adecuado por la reputación de otros pares. Si no es positiva, los bloquean.
  - Cada par notifica, tras interactuar con otro par, el comportamiento observado al *tracker* responsable del mismo, ya sea bueno (el esperado) o no.

ARQUITECTURA

- Búsqueda y localización de los *trackers*:
  - Gracias a un servicio de metadatos, cada organización publica información relativa a su red (incluyendo sus *trackers* y cadenas de certificación).
  - Mediante redirecciones web, alcanzamos el *tracker* adecuado.
  - El *tracker* al que nos encontramos conectados será el punto de partida.

ARQUITECTURA



Red IRIS

Universidad Rey Juan Carlos

IMPLEMENTACIÓN

- Lenguaje Java.
- Basada en Vuze (Azureus): cliente + *tracker*.
- Extensión al protocolo de pares para la autenticación.
- *eduGAIN AAI* para la identidad digital y el intercambio de mensajes (SAML).
- Extensión al protocolo de los *trackers* para consultar y notificar reputaciones.

Red IRIS

Universidad Rey Juan Carlos

CONCLUSIONES

- Demostración práctica de solución al problema del *free-riding*.
- Sencilla de desplegar:
  - Usuarios: pedir e instalar un certificado.
  - Organizaciones: instalar un *tracker* de BitTorrent y una fuente para publicar contenidos.
- Especial interés en la privacidad. No es necesario usar información personal.

TRABAJO FUTURO

- Evaluar extensivamente la solución y analizar los resultados.
- Desplegar una plataforma de pruebas:
  - Infraestructura de clave pública.
  - *Trackers*.
  - Clientes.
  - Servidores de metadatos e identidad.
- Mejorar la representación de la reputación y los algoritmos utilizados.

Red IRIS

Universidad Rey Juan Carlos

Aretusa
Sistema de reputación para BitTorrent