Protecting Free Expression Online with Freenet

(Ian Clarke and Scott G. Miller)

Sistemas Ubicuos
Universidad Rey Juan Carlos

Diego Chaparro González
dchaparro@gsyc.escet.urjc.es

Objetivos

- Crear un sistema de ficheros virtual
- P2P descentralizada
- Privacidad
- Prevenir la censura
- Mantenimiento de los datos
- Alta disponibilidad de datos
- Eficiente, escalable y adaptativo

Arquitectura

GUID (Globally Unique Identifier)

- Content-hash keys (CHK):

  Hash (SHA-1) del contenido del fichero

- Signed-subspace keys (SSK)

  Pequeña descripción concatenada con la clave pública

  El fichero se firma con la clave privada

Arquitectura

Mensajes y privacidad

- Diseñado asumiendo la posibilidad de ataques desde dentro y fuera de la red
- Los datos no se mueven de origen a destino, sino a través de una cadena de nodos
- Un nodo no sabe si el que le envió el mensaje era el emisor original del mensaje
- Un nodo no sabe si el siguiente nodo al que debe enviar un mensaje es el destino final

Arquitectura

Routing (queries)

- Napster usa un servicio centralizado
- Gnutella hace un broadcast a todos
- Freenet elimina los problemas de los anteriores:
  - Cada nodo reenvía las preguntas al nodo que piensa que está más cercano el objetivo final

Arquitectura

Requesting files

- Cada nodo mantiene una tabla de rutas con la dirección de cada nodo y los GUID que piensa que almacena
- Cuando un nodo recibe una query:
  - Si el nodo tiene el fichero lo devuelve con una etiqueta identificando que él lo tiene
  - Si no lo tiene, lo reenvía al nodo que tiene la clave más cercana en la tabla de rutas
- Para ocultar la identidad del que tiene el fichero, los nodos intermedios alteran el mensaje indicando que son ellos los que lo almacenan

Arquitectura

Inserting files

- Sigue el mismo camino que el request
- Se asigna un GUID y se manda un mensaje de inserción con un TTL que indica el número de copias que se guardarán
- Si un nodo recibe el mensaje, comprueba si existe la clave (CHK o SSK), y en caso afirmativo se rechaza (habría que hacer update)

Mantenimiento de la red

Añadir nodos

- Primero debe crear un par de claves
- Las claves no están certificadas
- El nuevo nodo manda un mensaje a un nodo de la red su clave pública y su dirección física
- El nodo que recibe el mensaje lo reenvía a otro elegido de forma aleatoria y así consecutivamente hasta que se llega al TTL

Mantenimiento de la red

Aprendiendo rutas

- Los nodos van aprendiendo nuevas rutas hacia nodos que almacenan una serie de claves
- Los nodos se especializan en almacenar ficheros con claves similares

Claves

- Los ficheros se agrupan por similaridad de claves, no porque el contenido sea sobre el mismo tema

Mantenimiento de la red

Buscar contenido

- Posiblidades:
  - Los autores publican listas de enlaces a ficheros
  - Se puede crear un símil a los buscadores en la web
- Todavía no hay una solución

Gestión del almacenamiento

- A veces hay que decidir qué ficheros mantener
- Actualmente se prioriza la popularidad
- Cuando hay que eliminar un fichero se elije el que ha sido solicitado hace más tiempo

Conclusiones

- Todavía está en desarrollo, cosas importantes que necesitan atención:
  - Desarrollar mecanismos de búsqueda
  - Mayor protección contra ataques de denegación de servicio
  - Caché menos agresiva: hay veces que un fichero desaparece porque no ha habido tiempo a que alguien lo haya solicitado.