



BITTORRENT SYNC

Informe de Redes de Computadores ELO-322

MARCO BENZI
2803054-1

EDUARDO GONZÁLEZ
2921001-2

MATÍAS MÜLLER
2803026-6

2 de septiembre de 2013

Índice

1. Resumen	2
2. Introducción	2
2.1. Motivación	2
3. BitTorrent Sync	2
3.1. ¿Qué es BitTorrent Sync?	2
3.2. Características y Tecnología	2
3.3. ¿Cómo sabe BitTorrent Sync con quién puede compartir archivos y con quién no?	3
3.4. Ubicación de pares (peers)	4
3.5. Ventajas y Desventajas	4
4. Resultados Prácticos	5
5. Conclusiones	6
5.1. Aplicaciones	6
6. Referencias	6

1. Resumen

En el presente informe daremos a conocer la nueva tecnología que es *BitTorrent Sync*. Hija del mismo grupo de desarrolladores del popular protocolo de comunicación *peer-to-peer* (P2P) *Torrent*, *Sync* promete ofrecer una nueva alternativa al almacenamiento en la nube, usando una metodología distribuida P2P. Bajo esta perspectiva se pretende garantizar mayor seguridad y control sobre los datos guardados, manteniendo la conveniencia de poder sincronizarlos entre varios lugares simultáneamente.

La tecnología resulta altamente escalable y confiable debido a su naturaleza distribuida.

2. Introducción

2.1. Motivación

En un mundo globalizado se vuelve fundamental la necesidad de compartir información, ya sea subiendo o descargando archivos. Hoy, no sólo buscamos subir o descargar archivos, sino que hemos introducido un nuevo concepto: compartirlos. Este problema es solucionado por el paradigma de *Cloud Computing*, utilizando servidores para sincronizar archivos entre varios usuarios. Entre los más conocidos se encuentran Dropbox, Google Drive y Sky Drive. Sin embargo, esta solución requiere tener un servidor online 24/7 para poder mantener la sincronización activa. BitTorrent Sync ofrece este mismo servicio sin la necesidad de mantener la información en un servidor centralizado, y por supuesto, sin todas las desventajas que ello implica.

3. BitTorrent Sync

3.1. ¿Qué es BitTorrent Sync?

Es un software gratis disponible para todos los sistemas operativos, el cual permite una sincronización de archivos sin necesidad de un servidor central, utilizando el protocolo BitTorrent *peer-to-peer* (P2P). No sólo se puede prescindir de un servidor disponible las 24 horas del día, sino que además la calidad del servicio mejora con la cantidad de personas que comparten un mismo archivo.

3.2. Características y Tecnología

Sync se basa principalmente en utilizar el protocolo BitTorrent. Dado que existe un grupo que disertará sobre este tema, no ahondaremos mucho más en él.

El protocolo BitTorrent funciona sin clientes ni servidores fijos, esto es, todos los usuarios pueden ser servidores de descarga o clientes en cualquier instante. Aplicaciones de este protocolo nacieron a finales de los años 90, donde *Napster* y *Gnutella* lideraban la expansión de

esta forma de compartir archivos. Otros softwares P2P que se popularizaron durante los comienzos de este milenio fueron *KaZaA*, *Ares*, etc...

La aplicación fundamental que se le otorga a este protocolo en la actualidad es la transferencia de archivos mediante Torrent. En éste, usuarios que dispongan del archivo que se desea compartir colaboran con un fragmento de éste. Las ventajas de este sistema son evidentes y serán tratadas más adelante, pero cabe destacar que la velocidad de descarga de los archivos se incrementa notablemente si la cantidad de usuarios con el mismo es grande.

BitTorrent Sync es una expansión de este sistema orientado a la sincronización de archivos. Los dispositivos se conectan directamente utilizando *UDP*, *NAT traversal* y *Mapeo de puertos UPnP*. Estos últimos son protocolos y servicios dedicados a permitir la comunicación entre dos dispositivos ubicados detrás de un NAT. La decisión de optar por UDP es básicamente para mejorar las tasas de envío de datos. Usar UDP permite minimizar la cantidad de mensajes enviados, de manera que afecten menos los tiempos de propagación entre usuarios. Los archivos se fragmentan, y diferentes usuarios comparten sus fragmentos con quien requiera el archivo compartido. Éste último reensambla los fragmentos al final del proceso, y por lo tanto no requiere que sus partes siguiera lleguen en orden, lo que hace ideal el uso de UDP por sobre TCP en la mayoría de las situaciones (muchos usuarios, o *seeds*).

Provee además servidores de *relay* (relevos) y rastreo, es decir, cuando dos usuarios no pueden conversar directamente (por ejemplo, un cortafuegos no lo permite), BitTorrent Sync provee un servidor relay para rutear tráfico entre ambos, por supuesto, en forma encriptada. Utilizar servidores de relay es opcional.

Finalmente, al igual que Dropbox, permite versionado de archivos, almacenándolos en una carpeta oculta.

3.3. ¿Cómo sabe BitTorrent Sync con quién puede compartir archivos y con quién no?

Resulta lógico pensar que personas ajenas al archivo que se desea compartir no puedan verlo, y por supuesto que los demás si lo puedan hacer. Pero ¿cómo hacerlo sin necesidad de un sistema login/password?

El *secreto* es una clave de 20 bytes generada aleatoriamente, codificada en base 32, por el usuario que desea compartir por primera vez algún archivo o carpeta. Esta clave debe hacerse llegar a los pares que deseen pertenecer a la sincronización. Una de las novedades es que BitTorrent Sync permite obtener la clave mediante un *código QR*, lo cual es más sencillo y seguro a la hora de trabajar con dispositivos móviles como celulares.

Existen distintos niveles de secretos, los cuales otorgan distintas atribuciones a quienes posean esta clave. Al compartir algún archivo, BitTorrent Sync pregunta acerca de qué tipo de secreto desea compartir.

Master Secret Es una clave con acceso completo. Quienes posean esta clave tendrán derechos de lectura y escritura libres sobre los archivos que se compartan.

Read Only Secret Resulta necesario mantener archivos compartidos, pero sin que estos puedan ser alterada su versión original. Este tipo de clave es justamente la solución que se necesita cuando sólo se le desea otorgar derechos de lectura a algún usuario.

One-time Secret Como su nombre lo indica, sólo otorga acceso a la carpeta compartida 1 vez.

3.4. Ubicación de pares (peers)

Búsqueda Local Peers en LAN responden a un paquete enviado por broadcast en caso de coincidir con el secreto.

Intercambio de Peers Cuando un Peer está conectado, éste comparte con los demás usuarios su lista de pares detectados.

Hosts conocidos Si un host tiene una dirección IP y un puerto estáticos, entonces es posible conectarse remotamente a él utilizando esta información.

DHT (Distributed Hash Table) Utiliza DHT para distribuir y obtener información de otros peers con un secreto dado. Sync envía $\text{SHA2}(\text{secreto})\text{-ip-puerto}$ al DHT para anunciarse, y recibe una lista de peers al preguntarle a la DHT por la clave $\text{SHA2}(\text{secreto})$. SHA2 corresponde a *Secure Hash Algorithm 2* y es una serie de funciones hash criptográficas diseñadas por la agencia nacional de seguridad de los EEUU. En esta estructura, la tabla hash se distribuye en todos los computadores de la red (con redundancia). Existe una red superpuesta que agrupa claves similares de manera de aumentar la rapidez para encontrar la combinación deseada (desde $O(n)$, sin red superpuesta, a $O(\log(n))$).

BitTorrent Tracker Servidor de rastreo específico para facilitar descubrimiento de peers. El tracker ve la combinación $\text{SHA2}(\text{secreto})\text{-ip-puerto}$ y ayuda a los pares a conectarse directamente. Actúa como servidor *STUN* y ayuda a realizar *NAT traversal* (su uso es recomendado por los diseñadores del sistema). Los servidores *STUN* permiten a los computadores conocer su IP vista desde afuera de una red NAT, permitiendo compartir su ubicación con el resto de los usuarios del sistema.

3.5. Ventajas y Desventajas

- Ventajas

1. Alta escalabilidad y el servicio mejora con la cantidad de usuarios: Dado que BitTorrent Sync utiliza el protocolo BitTorrent, si mucho usuarios poseen un archivo

que algún nuevo usuario desee descargar, todos ellos contribuirán con un fragmento de este archivo al nuevo usuario limitando el ancho de banda de descarga sólo al de bajada del nuevo usuario. En cambio, en un esquema centralizado, el ancho de banda estaría limitado probablemente por el ancho de banda del servidor.

2. El tamaño de la carpeta/archivo a compartir es ilimitado: Sólo se restringe a la capacidad del hardware de un computador (HDD/SSD). En los servicios que utilizan servidores centrales para sincronizar, se debe restringir usualmente al tamaño máximo asignado por cada compañía. A modo de ejemplo, Dropbox sólo entrega 2 GB de forma gratuita.
 3. Ideal para compartir grandes archivos: Como se explicó con anterioridad, cada par que tenga el archivo en su máquina compartirá un fragmento del archivo a algún nuevo usuario. De esta forma, si un paquete se corrompe o se pierde, no se debe descargar nuevamente el archivo, el cual probablemente hubiese demorado una eternidad si se descarga desde un servidor central. El fragmento faltante simplemente se reenvía desde el mismo peer o de algún otro disponible.
 4. Transferencias Seguras: La transferencia de archivos es encriptada (AES), y los archivos nunca son almacenados en ningún servidor.
 5. Servidores Privados: Si alguien lo desea, puede establecer su máquina como servidor para todos los demás usuarios, manteniéndolo en línea las 24 horas del día (equivalente a tener un servidor Dropbox administrado en forma personal).
- Desventajas
1. No permite transferencia de archivos entre 2 usuarios si alguno de ellos se encuentra desconectado.
 2. La tasa de descarga puede ser muy lenta si hay pocos usuarios para una misma carpeta compartida: Esto sucede porque la transferencia se realiza entre pares, por lo que la descarga estará limitada al ancho de banda de subida de alguno de los usuarios, el cual suele ser muy bajo, o al menos más bajo que el ancho de banda de bajada.

4. Resultados Prácticos

Se procedió a instalar BitTorrent Sync en un computador portátil y en un dispositivo móvil. Su potencial fue directamente presentado en clases, donde se generó un código QR el cual fue descifrado por el dispositivo móvil. Este último capturó en el momento una fotografía con su cámara, la cual almacenó en memoria y automáticamente procedió a compartir con todos los usuarios que estuviesen compartiendo la carpeta donde se encuentra la imagen. Unos instantes después, la fotografía apareció en el computador portátil y fue exhibida al público.

5. Conclusiones

El servicio funciona a la perfección. Sync no sólo han incursionado en otorgar un nuevo servicio, sino que también a logrado entregar un servicio de calidad. Lo novedoso y simple que resulta compartir archivos es excepcional. El usuario no necesita crear cuentas ni recordar claves. Sólo elige la opción de compartir una carpeta y entrega el código QR o bien el secreto en sí, para que algún usuario acceda a la información.

5.1. Aplicaciones

Algunas de las aplicaciones que creemos útiles son las siguientes.

Manejo de archivos sensibles Gracias a la seguridad que otorga Sync, resulta muy sencillo transferir archivos sensibles y poder manejarlos de forma segura. Mediante los distintos tipos de secretos, se pueden distribuir guardando la discreción deseada.

Sincronización de almacenamiento masivo Sin dudas, es una de las aplicaciones más útiles, dado que Sync posee todos los atributos para hacer de este servicio uno de los mejores. Si un nuevo usuario posee un ancho de banda de bajada relativamente alto, y hay muchos usuarios compartiendo un gran archivo, éste se descargará probablemente a la máxima tasa posible.

Solución de bajo costo para PYMEs Un servicio de Cloud Computing de alta capacidad de almacenamiento resulta muy caro. Por ejemplo, 1 año de 500 GB de capacidad en Dropbox cuesta US\$500. Sin embargo, con esta nueva solución, basta tener un dispositivo de almacenamiento con 500 GB, el cual cuesta alrededor de US\$50, y se paga sólo una vez, pues recuerde que Sync es gratis.

6. Referencias

- BitTorrent Labs, <http://labs.bittorrent.com/experiments/sync/technology.html>
- Dropbox <http://dropbox.com>
- Peer-to-Peer, Wikipedia
- Apuntes del ramo ELO-322