Fundamentos de Redes

Redes anónimas: I2P

Alberto Jesús Durán López
Antonio Coín Castro

Grupo 5

30 de noviembre de 2017

Privacidad en la red

"[Privacy] can be defined as an individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed, and used."

Anonimato en el acceso corriente a Internet

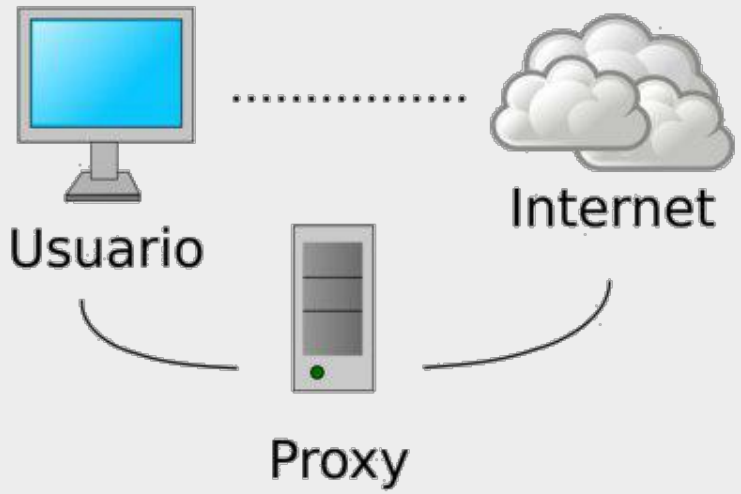
- Identificación de forma unívoca por la **dirección IP**
- Geolocalización
- Rastreo de datos personales (*tracking*)
- Cookies
- Anuncios dirigidos

Métodos para mantener el anonimato

- Proxy
- VPN
- Redes anónimas
- Otros

Proxy

Servidor intermediario entre las conexiones de un cliente y un servidor.



- Dirección IP camuflada
- Acceso a contenido bloqueados en algunos países

VPN

VPN

Acrónimo de *Virtual Private Network*. Es un medio de extender una red privada a través de una red pública.

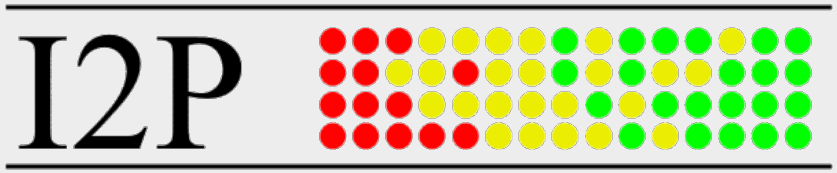
- Acceso remoto a una red privada (UGR)
- Dirección IP camuflada
- Confidencialidad garantizada: paquetes encriptados
- Sistema de autentificación para conectarse
- Mecanismos para mantener integridad de mensajes

Otros. . .

- Buscadores que no te rastrean (e.g. DuckDuckGo)
- Sistemas operativos específicos (e.g. Tails)

Redes anónimas

Invisible Internet Project



I2P es una herramienta de **software libre** que ofrece una capa de red de abstracción distribuida para comunicaciones entre ordenadores, la cual permite a las aplicaciones que la utilizan transmitir mensajes de forma anónima y segura.

Invisible Internet Project

Estructura

Se trata de una red superpuesta (*overlay network*) basada en el intercambio de paquetes.

- Los paquetes están dirigidos a direcciones criptográficas.
- Emisor y receptor no pueden identificarse mutuamente.
- Comunicaciones ocultas a terceros (encriptadas).
- Funcionamiento P2P.

Invisible Internet Project

Estructura

- Un **router** es un ordenador conectado a I2P. En general, nos referiremos a ellos también como **nodos** de la red.
- Un **túnel** es una secuencia de nodos que forman camino temporal, unidireccional y seguro por el que viajan los mensajes.

Invisible Internet Project

Funcionamiento

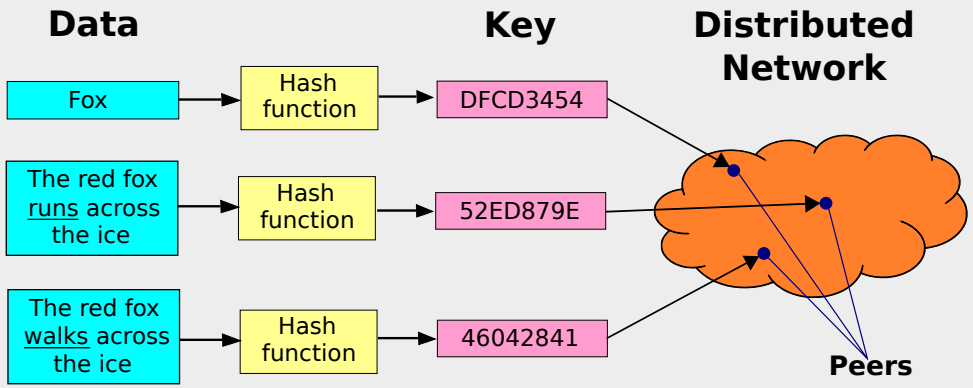
Cada cliente construye una serie de túneles de entrada (*inbound*) y de salida (*outbound*). El primer nodo de un túnel se denomina *gateway*.

Se elige la longitud del túnel para encontrar un equilibrio entre el anonimato, la latencia y el *throughput*.

Invisible Internet Project

netDB

La base de datos en red está completamente distribuida. En cada instante, hay un subconjunto de nodos especiales (*floodfill nodes*) encargados de mantenerla.



Cuando se envía un mensaje, se buscan en la tabla los túneles de entrada del nodo destino (*LeaseSet*).

Invisible Internet Project
netDB

La información que se almacena en la tabla es la siguiente:

- **RouterInfo:** estructura que contiene información para contactar a un router concreto.
- **LeaseSet:** información para establecer comunicación con un destino concreto (otro nodo, un servidor de correo, un sitio web. . .).

Invisible Internet Project

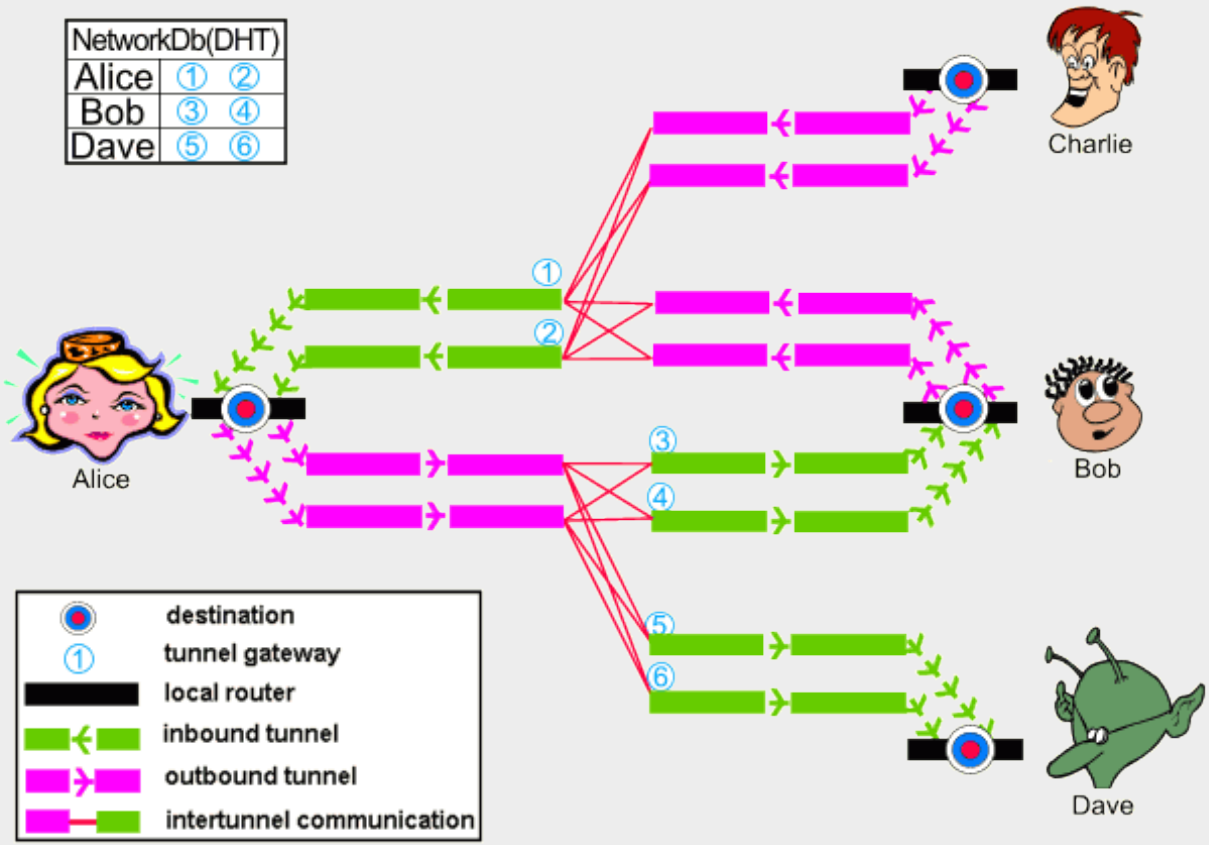
Algoritmo Kademlia

Los accesos y consultas a la base de datos se realizan al nodo *floodfill* más cercano. La medida de cercanía se computa utilizando la métrica XOR sobre el ID de los nodos.

- $A \oplus B \geq 0$, y $A \oplus B = 0 \iff A = B$
- $A \oplus B = B \oplus A$.
- $A \oplus B \leq (A \oplus C) + (C \oplus B)$

Invisible Internet Project

Ejemplo de comunicación



Garlic routing

Enrutamiento tipo garlic:

- Cifrado por capas
- Agregación de múltiples mensajes juntos
- Cifrado ElGamal/AES

Garlic routing
Cifrado por capas

- Comunicación de dos usuarios mediante túneles
- La información viaja desde el primer nodo del túnel hasta el último
- El *gateway* fragmenta mensajes I2P en mensajes de túnel
- En cada salto se envía una tupla (mensaje del túnel)

Garlic routing
Cifrado por capas

Los mensajes del túnel están formados por:

- ID del túnel
- Vector de inicialización (*IV*)
- Instrucciones de envío/enrutamiento
- Mensaje (encriptado) que se quiere enviar
- Relleno

Garlic routing

Agregación de mensajes

Agregación de múltiples mensajes juntos juntos para aumentar velocidad de transferencia de datos y aumentar seguridad.

Garlic routing
Encriptación de la información

Tipos de cifrado:

- Cifrado ElGamal
- AES: Cifrado simétrico por bloques de 128 bits

Procedimiento aplicado a los mensajes:

- Se cifra el IV recibido con AES
- Usa el IV obtenido para cifrar los datos
- Cifra de nuevo el IV usando AES
- Envía {ID del túnel, IV, mensaje del túnel} al siguiente nodo

I2P vs Tor

- *Onion routing* vs *Garlic routing*
- *Túneles bidireccionales vs túneles unidireccionales*
- Directorio distribuido vs centralizado. Peer selection.
- Outproxies

Software I2P

- Susimail: Interfaz web para emails
- Syndie: blogs, noticias y foros para I2P
- I2P Messenger: Cliente de mensajería instantánea
- Navegación web mediante webs anónimas
- Compartición de archivos mediante el uso de BitTorrent dentro de la red I2P
- (Android) Nightweb, aplicación que usa I2P y BitTorrent para compartir entradas de blogs, fotos y otros contenidos similares

I2P
Demo

Acceso a la red I2P. Configuración, panel de control y ejemplo de navegación.

El software se puede descargar en el siguiente enlace:
`https://geti2p.net/en/download`