

# Anonymous Communication Tools

Govind Kumar  
210050058

Khushang Singla  
210050085

March - April 2023

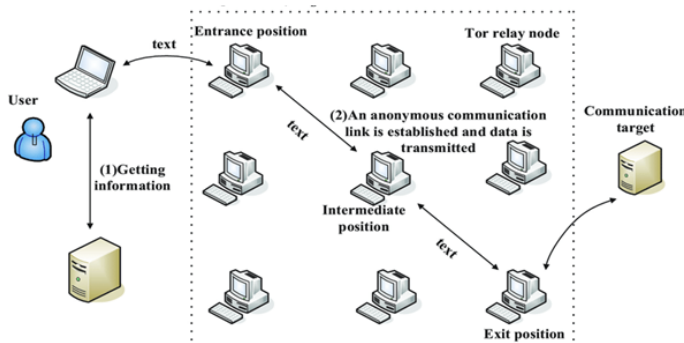
## 1 Overview

Anonymity describes situations where the acting person's identity is unknown. The important idea here is that a person be non-identifiable, unreachable, or untrackable. Anonymous online services allow people to communicate and share content without revealing their name or true identity. The benefits of these tools include promoting free criticism, security to whistle blowers, prevention of individual data collection, privacy among individuals, etc. Nowadays, there are many tools being built for anonymous communications. Onion routing and Garlic Routing are two of the most famous routing protocols for communicating anonymously on internet. These routing protocols route the data through various nodes so that the path cannot be traced by someone looking the network. VPN (Virtual Private Network) also provide some level of anonymity but in VPNs, user's privacy is in hands of a single person with access to the VPN servers. There also exist remailers and rewebbers to provide anonymous e-mailing service(eg. ProtonMail) and browsing services.

## 2 Tor - Onion Routing

Tor has been one of the most famous and widely used anonymous communication tool. Tor, The onion Routing Browser is simply an Internet Browser based on Firefox, with modifications to hide the user's IP address. Although Tor was initially developed by the US government in 2002, it is not presently controlled by any one entity.

### 2.1 Onion Routing



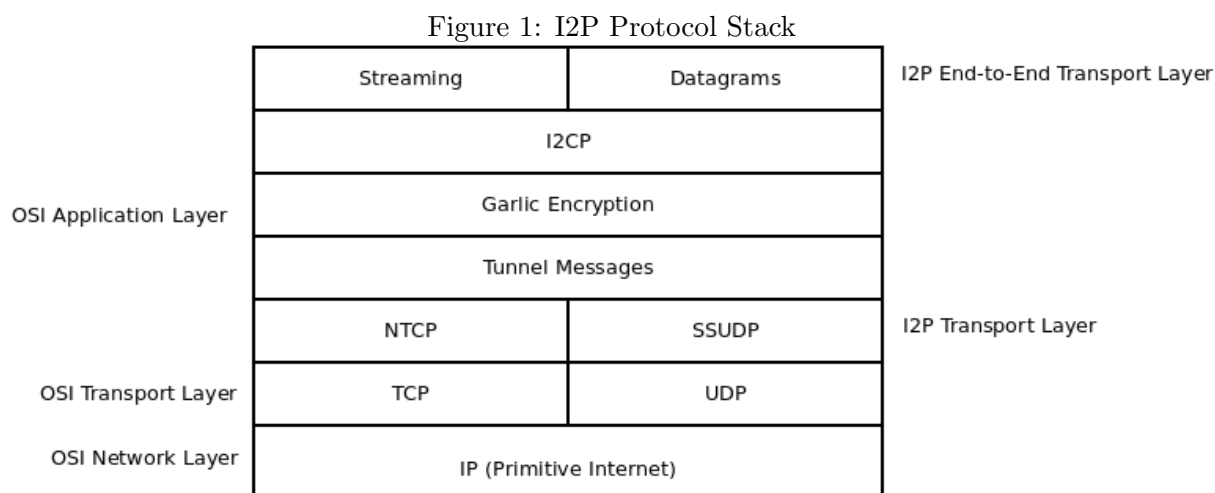
In a nutshell, onion routing refers to encapsulating message under layers of encryption at different nodes before it reaches the final destination. All the nodes only know about the previous node and the next node. In this way, no single node knows the entire path of the message. Clients choose these path randomly and build a circuit. These circuits change every few minutes preventing any snooping attempts.

### 3 Invisible Internet Project - I2P

This is a project trying to implement **Garlic Routing** - A Routing protocol built over onion routing. It is not used widely as of today because it needs slightly more technical knowledge to set up for the first time for use. Also, the sites outside the network of invisible internet cannot be accessed through the invisible internet. One may access outside internet through proxies (which do exist) but the proxies may be malicious and it may not be safe to do so. This also is a big problem hindering the popularity of i2p.

#### 3.1 I2P Protocol

I2P adds more layers in Application Layer of primitive internet to introduce anonymity. Figure 1 shows the layers in this stack.



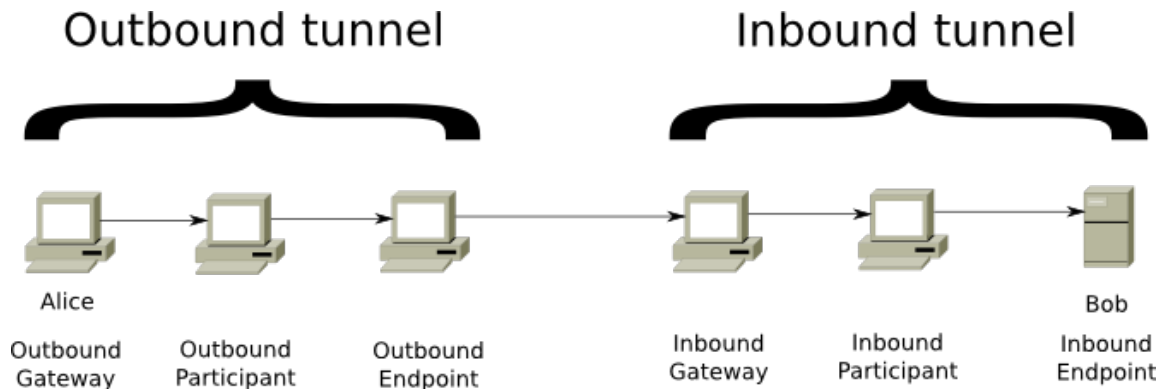
I2P transport layer is built over Transport layer of regular internet. It is strictly for next-hop transfer among I2P routers. This is non-anonymous transfer. This layer has two protocols built over TCP and UDP each.

- NTCP2 - New I/O based TCP
- SSU - Secure and Semi-Reliable UDP

#### 3.2 Structure of I2P: Components

- **Tunnel**

Messages are sent from one node to another through tunnels. There are two tunnels, outbound tunnel and inbound tunnel. This is needed as per Garlic Routing protocol. The sender first builds an outbound tunnel. It gets the details of Inbound tunnel from netDB. In a tunnel a gateway refers to first router and the last router is called endpoint. A user might have multiple such outbound and inbound tunnels. These tunnels used in I2P are **unidirectional** as opposed to bi-directional routes in Tor.



The sender adds routing instructions with the message, encrypts it and sends it through the tunnel. Just like Onion routing, this message is also encrypted using layered encryption. When the endpoint receives the final message, it gets the routing instruction to the inbound gateway of receiver. The inbound gateway then sends this message to inbound endpoint through the tunnel. Except for this difference, if we see tunnels as gateway to endpoint, both work in a similar way.

Gateway accumulates some messages to be sent through the tunnel, adds path to receiver and converts them to **Garlic Message** so that they can be sent through tunnel. When the endpoint of tunnel finally decrypts the message, it separates the messages and forwards them to the required hosts.

- **Network DataBase**

Network Database stores the information about the routers present in the network. It also stores information about the tunnel gateways for inbound tunnels of users. In I2P, routers are identified by their public keys. This Network Database is a decentralized database.

When a user wants to communicate with some other router in the Invisible Internet, he needs to lookup in the network database to find the details of inbound tunnel gateway for receiver. As it is a decentralized database, possibly, a router may not have access to complete database at any given time. As I2P is not widely used, it is possible to find these details in a few tries but if the usage increases, it might become difficult to access this information.

Network database stores two kinds of data: **leaseSets**(Section 3.3.1) and **routerInfo**(Section 3.3.2)

### 3.3 Network Database

#### 3.3.1 Lease Sets

Lease Sets are used to document tunnel entry points for a particular client destination. The following information is stored in a Lease Set.

**Lease** stores information of the inbound tunnel gateway. A lease stores the following information. It is needed to send messages to the Destination.

**Gateway Router** is specified for the tunnel. It is specified by specifying its identity.

**Tunnel ID** to be used to send message through the tunnel.

**Expiry Date** stores the time till when the tunnel is available.

**Destination** encryption key, signing key and a certificate.

**Additional encryption public key** for use in encrypting garlic messages. It is used for end-to-end ElGamal/AES + Session Tag encryption.

**Signature** of the lease set to ensure that the data is published by the entity mentioned in destination.

There are various types of Lease sets like Unpublished Lease sets, Encrypted LeaseSets etc.

### 3.3.2 Router Info

RouterInfo includes the following details

**Router's Identity** stores an encryption key, a signing key and a certificate to authorize that. The public\_key is used for ElGamal Encryption in next-hop messages. The signing public key and key certificate are used for verifying signatures.

**Contact Addresses** where the router can be reached. It contains mapping of transport protocol (NTCP or SSU) with ip address and port.

**Publish Date** is the time when this info was published.

**Options** is a set of arbitrary options for telling the bandwidth capacities, router version, netId. There are some other stat options also.

**Signature** of all the above data.

Router Info is stored in NetDB. This is required for building tunnels.

## 4 VPN

VPN stands for Virtual Private Network. VPNs provide a set of servers through which the connected clients route their traffic. The cost to maintain VPN services is high as with increase in number of clients, the service provider needs to get more servers to keep up with the load. This reduces scalability of VPNs.

One bigger problem of VPN is that the admin of the VPN servers can see what each user is accessing, thus VPNs can't be considered enough anonymous. VPNs are mostly used to be able to access a private network from anywhere and less popular to be used for privacy or anonymity over internet. But they may well be used to hide from the websites, who is trying to access the content as for the websites see the VPN servers as their clients.

## 5 Resources Used

1. An Analysis of Tools for Online Anonymity
2. Tor Website
3. Tor: The Second-Generation Onion Router
4. I2P Docs