Parallel and Distributed Computing

Momina Atif Dar
P18-0030

Torrent – Tor/Onion Routing

Working of torrents:

Peer to peer communication is used in torrenting. A P2P communication protocol (example: BitTorrent) breaks down the file into many pieces. Torrent tracker knows what piece is on what machine and what's its IP address so it connects peers by forwarding the IP addresses to all clients to make sure all peers are connected. When the peers are connected and the download starts, the tracker is no longer needed. Tracker gets all the necessary information about the peers and their IPs from .torrent file. When the client has downloaded enough data, it also starts to upload the files to aid other peers. This way the circle goes on.

TOR project-onion routing:

Tor is basically another name for onion routing. Just like there are layers in onion, onion routing has layers of encryption as well.
For example there's a client which wants to access Facebook and is using Tor browser or service. Between the client and Facebook server there are three onion routers. Client has three encryption keys for three onion routers. When the client enters login information, the data is encrypted in three layers using Key 1, Key 2 and Key 3. The data is then sent to 1st onion router and that router decrypts the data using its Key 1. It then forwards the data to 2nd onion router which decrypts the data using Key 2 and forwards it to 3rd onion router which decrypts the data using Key 3 and forwards it to Facebook server which verifies the credentials and logs in the user. When the reply is sent from Facebook server to client, encryption takes place. Server sends reply to 3rd onion router which encrypts the message using Key 3 and forwards it to 2nd onion router which encrypts the message using Key 2 and forwards it to 1st onion router which encrypts the message using Key 1 and forwards it to client. Then client using they Keys that it already has, decrypts the message.
Due to layers, Tor is slow. It is also not much safe as packet sniffing can be done at routers but due to onion routing i.e multiple layer encryption, the packets even if sniffed doesn't make much sense to the hacker. Let's say the hacker is sniffing packets between from 3rd onion router, it would know only about 2nd onion router and Facebook server because of 3rd onion router's connection with them. It wouldn't know with whom 2nd onion router connected or from where the data is actually coming from. Another thing that is important is that TLS (Transport Layer Security) or HTTPS is used between 3rd router and Facebook server so the credentials of users or any other sensitive information is not in plain view to hacker. Using TLS or HTTPS would secure the information so hacker can not take advantage of it.