Shadow Peer-to-Peer Networks

Luke Murray, supervised by Dr. Simon Hollis

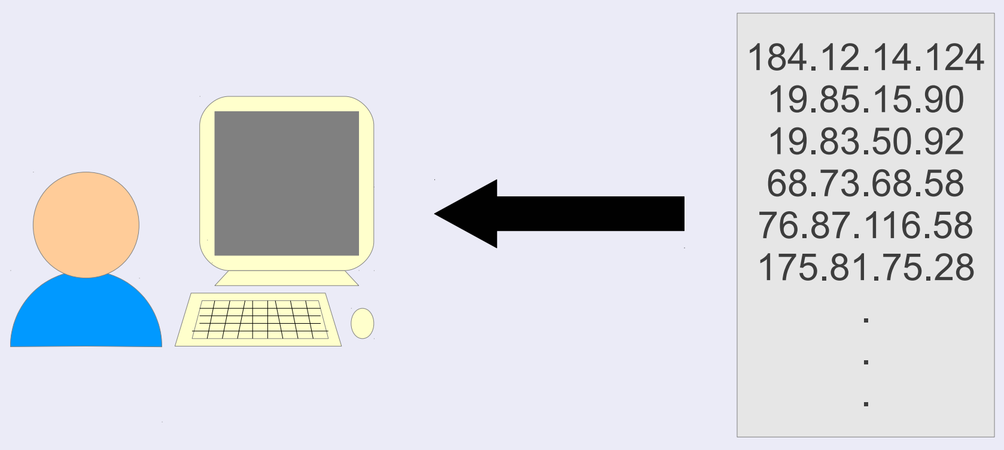
University of Bristol, Department of Computer Science

Introduction

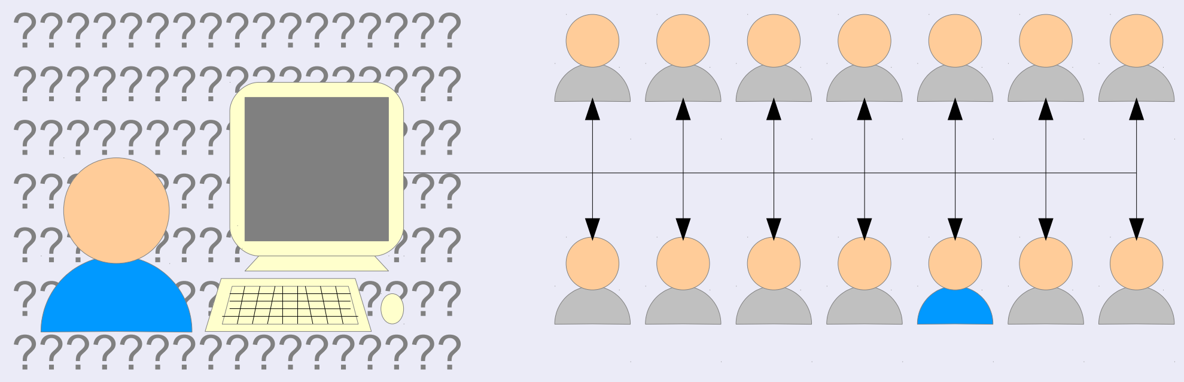
Shadow P2P is a network designed to provide a level of anonymity that has never been provided before. In existing networks, it is very hard to tell who is talking with who and what they are talking about. In additon to these features, my network aims to prevent anyone from being able to tell if a person is participating in the network or not. This is a feature not offered by any other network. This is achieved through the use of several key project components. Among these are: shouts, shout groups, public key hiding and a toroidal network structure.

1. Shouts

A shout is how peers communicate anonymously. To do this, the sender gets the shout list corresponding to the receiver.



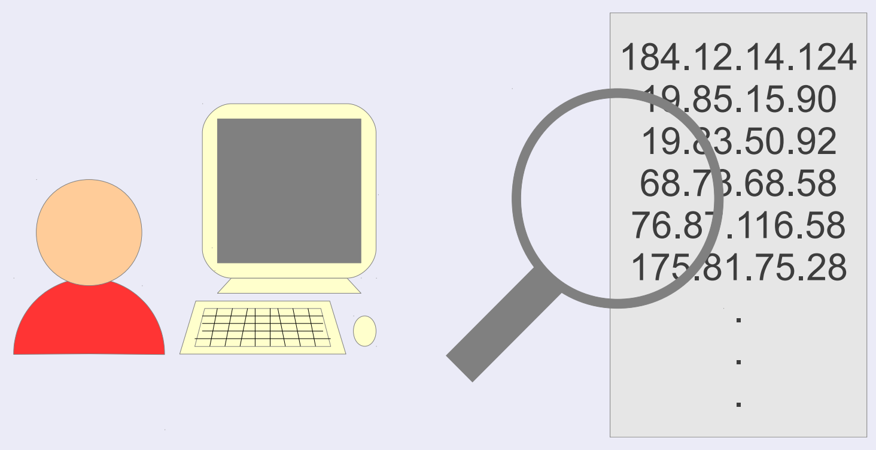
The sender then sends messages to the receiver by sending packets with a spoofed source IP address to every IP address in the shout list.



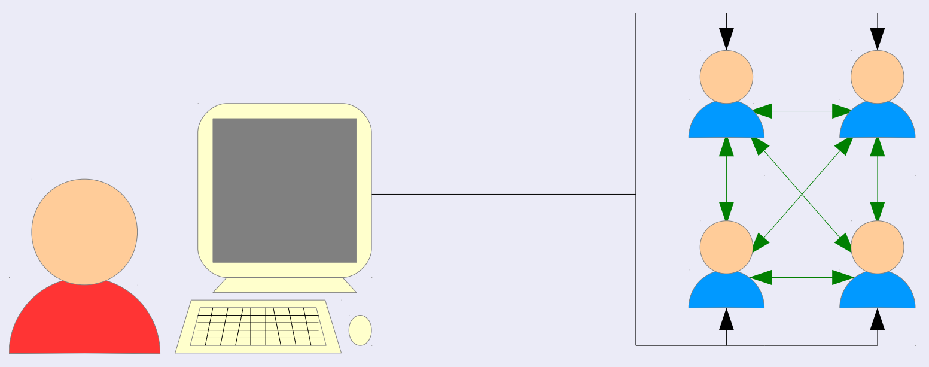
This method of communication is unreliable and very inefficient but it does remove most of the information about the peers' identities. The point of most concern is that some party could search through the IP addresses in the shout list to find the true identity of the peer. For that reason, shout groups have been created.

2. Shout Groups

Shout groups are a defence mechanism that prevents adversaries from searching through the IP addresses in the shout list. A small number of peers work together and create a joint shout list that contains all of their real IP addresses.



These peers work together to ensure that they only respond to messages that do not give their identities away.



The aim of the shout group is to minimise the amount of information that a hostile sender can gain about the peers' IP addresses. Here, we also need to consider the cases where members of the shout group are hostile and how we reduce the frequency of these attacks.

3. Public Key Hiding

Peers are associated with a public key. This can reveal who is communicating with whom, even with anonymous identities. To prevent this I have invented a method of hiding a public key such that it becomes unrecognisable but so that it can still be used for encryption. In ElGamal, this can be done as follows:

To scramble: select r randomly from $\{1 \dots q\}$ and calculate $g' = g^r$ and $h' = h^r = g^{xr}$.

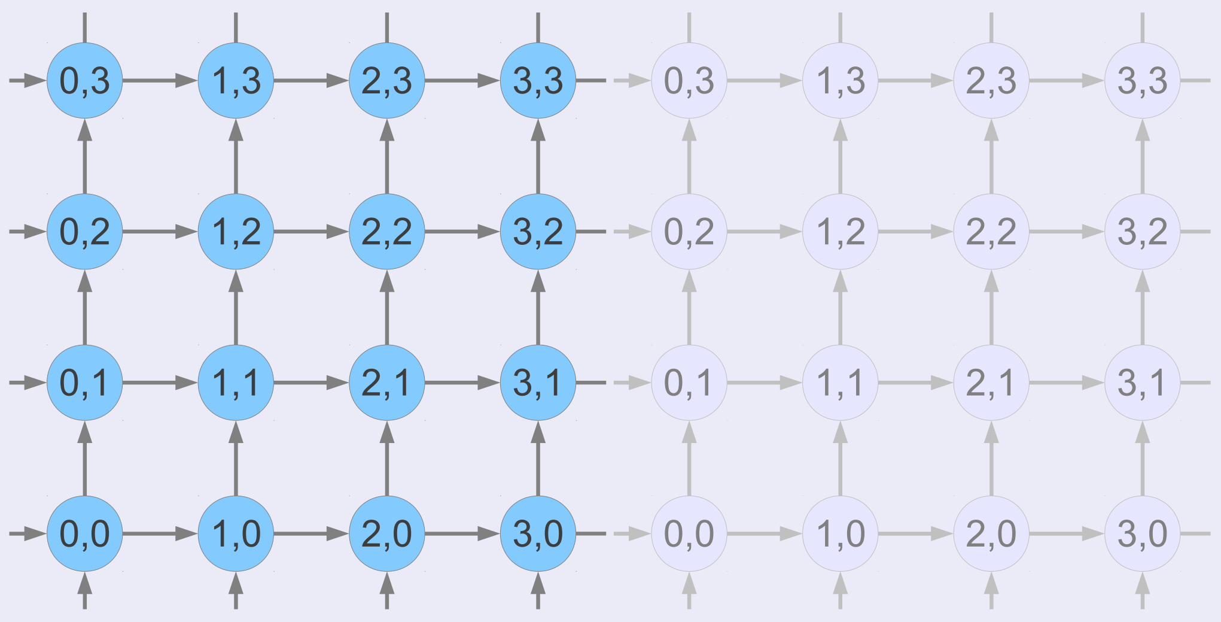
```
Function encrypt(G, g', q, h', m) {
    select y randomly from {1 … q}
    $c_1 = g'^y$
    $s = h'^y$
    m' = m converted to a member of G
    $c_2 = m'.s = m'.h'^y = m'.g^{xry}$
    return $(c_1, c_2)$
}
```

```
Function decrypt(G, x, $c_1$, $c_2$) {
    $s = (c_1)^x$
    $m' = c_2.s^{-1} = m'.g^{xry}.g^{-xry}$
    m = m' de-converted from a member of G
    return m
}
```

This method of public key hiding also works with ECIES (Elliptic Curve Integrated Encryption Scheme).

4. Network Structure

The network uses a uni-directional toroidal structure through which to deliver packets. This regular structure allows packets to be routed in many different ways making it very difficult to perform traffic analysis. The structure also allows easy dynamic expansion and contraction of the network.



Nodes transform packets that pass through them so that packets cannot be traced. By using source routing, the sender can be assured that their packets are routed randomly.

University of Bristol