Shadow Peer-to-Peer Networks

Luke Murray, supervised by Dr. Simon Hollis

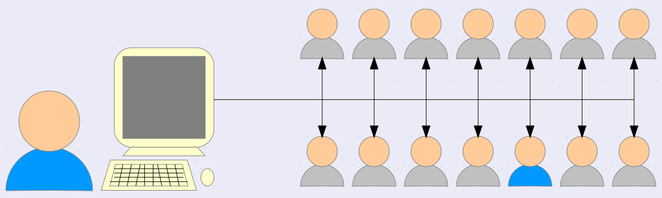
University of Bristol, Department of Computer Science

Introduction

Shadow P2P is a network designed to provide a level of anonymity that has never been provided before. On existing networks, it is very hard to tell what a communication is about or who is talking with who. My network aims to provide these anonymity features and it also 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

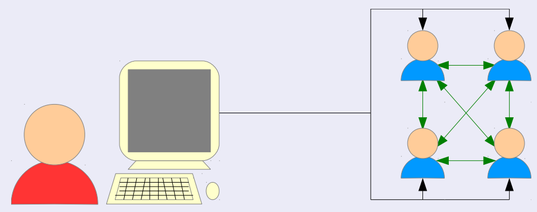
A shout is essentially a multicast. This is where a message is sent to a known list of IP addresses. In my network, the receiver provides a list of IP addresses, only one of which is the receiver's true IP address. This list is called a 'shout list'. The sender "shouts" by sending a message to every IP address in the shout list whilst also spoofing their own IP address. This anonymises the receiver's IP address amongst those in the shout list and the sender's identity has been removed the message. This method of communication reveals very little about who is talking to who and is the communication primitive that the network depends on.



The communication is unreliable, so how do we make sure the receiver gets the message? How do we prevent a hostile sender from searching the shout list to find the receiver's real IP address? Isn't this method of sending messages not incredibly inefficient?

2. Shout Groups

Shout groups are a defence mechanism against hostile parties searching through the IP addresses on 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 have been shouted to the entire shout list.



The peers need to be careful which messages they do or do not respond to; the different search methods used by a hostile sender can reveal information about the peers in the shout group. The aim of the shout group is to minimise the amount of information that a hostile sender can gain about the peers' IP addresses. What if the members of the shout group are hostile? How do the shout group members communicate amongst themselves? How are repeated attacks hindered?

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 such that it can still be used for encryption. In ElGamal, this can be done as follows:

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

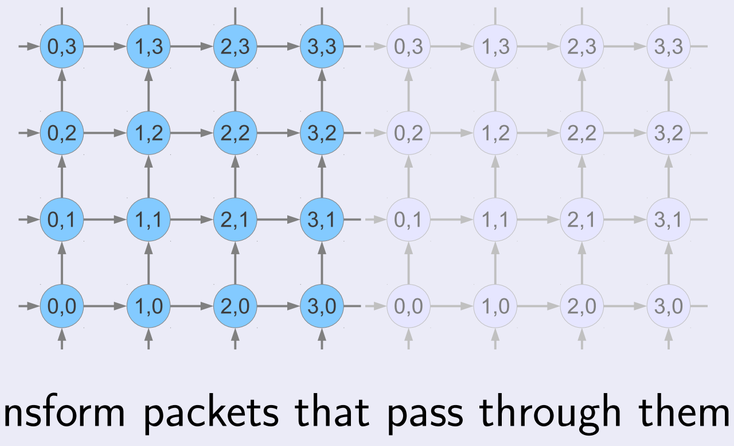
```
Function encrypt(G, g', q, h', m) {
    select y randomly from {1 … q}
    c1 = g'^y
    s = h'^y
    m' = m converted to a member of G
    c2 = m'.s = m'.h'^y = m'.g^xry
    return (c1, c2)
}
```

```
Function decrypt(G, x, c1, c2) {
    s = (c1)^x
    m' = c2.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