**Abstract**

Many internet users desire a means of communication that guarantees privacy so that they can be confident their identities will remain unknown and their messages will be safe from prying eyes. This is especially the case nowadays as public concern increases about organizations spying on users in both foreign and domestic networks. Networks such as TOR already provide such a service; however, do not do so in a peer-to-peer manner. In this paper, we introduce Anonychat, an anonymous peer-to-peer chat protocol designed to keep the identities of its users a secret.

To do this we create an application layer protocol that references a central name server to identify a list of peer connections. Users connect to peers from this list and are able to send and receive messages to each other. In order to keep users’ identities anonymous, messages are broadcast to all peers whenever they are sent or unsuccessfully decrypted, and controlled flooding is used to prevent saturation over the network. We use a slight spin-off of onion routing with two layers of encryption to guarantee that an adversary with a view of the entire network cannot trace packets back to their senders.

In order to evaluate our success, we then assess several areas that would be crucial to the success of the protocol. Among these areas is security. To do this, we tested to make sure an adversary could not determine who received a packet based on the difference in successful and unsuccessful decryptions. In this experiment, we found time differences inconsistent enough to be confident an adversary could not use decryption information to identify who received messages. Another area of testing concerned practicality; the protocol needs to be both fast and scalable to compete with other competition like TOR. We tested packet RTTs on a local network and found overall sending times were feasible for deployment. These results leave us confident that with continued work the Anonychat system could prove successful.