**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. Peers are linked by a central server, and utilize encryption in a method similar to onion routing to hide the contents of messages between users. Messages are sent out to nodes in a broadcast format to obfuscate the intended recipient.

In order to evaluate our success, we assessed two areas that would be crucial to the success of the protocol: security and practicality. To address security, we tested to make sure an adversary could not determine who received a packet based on the difference in successful and unsuccessful decryptions. Our results showed that decryption times were indeed inconsistent enough that we feel an adversary could not identify a user’s identity from them. To address practicality, we tested to see if the protocol was both fast and scalable. To do this we …