**Team 17 Results, Anonychat**

Ben Korza, Mark Fitzgibbon, Mitchell Caisse

The main goal of our project was to create an Anonymous chat program to allow users to communicate with each other anonymously. We have defined several metrics that determine how successful we were in creating this protocol. These metrics include, but are not limited to, the travel time of messages sent, an appropriate encryption scheme, and ensuring that peers are distributed appropriately.

Our implementation uses a central name server to distributed peers. In order to maintain the proper operation of our name server, we need to ensure that the server does not get overloaded and can no longer process requests. To ensure this we tested the load that each additional client added to the server and compared it against our goal of having a linear increase in CPU usage. Our results are as follows.

Number of Nodes Average CPU Usage (Over 5 seconds)

1. 10%
2. 11%
3. 13%
4. 15%
5. 18%
6. 21%
7. 25%
8. 26%
9. 31%
10. 33%

This roughly coheres to our desire for linearity.

As our chat program relies on a distributed approach to send messages between clients, we needed to verify that the algorithm in use by the name server is distributing the peers appropriately. Each client will have a route to each other client and there will be no orphaned clients. We tested the algorithm and compared it against our goal of each client having a path to another, and the clients not being isolated. The following results present connections between clients as Xs in the table. They reflect a successful graphing of a simulation with 10 clients.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Node | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 |  | X | X | X | X |  |  |  |  |  |
| 2 | X |  | X | X | X |  |  |  |  |  |
| 3 | X | X |  | X | X |  |  |  |  |  |
| 4 | X | X | X |  | X |  |  |  |  |  |
| 5 | X | X | X | X |  | X |  |  |  |  |
| 6 |  |  |  |  | X |  | X | X | X | X |
| 7 |  |  |  |  |  | X |  | X | X | X |
| 8 |  |  |  |  |  | X | X |  | X | X |
| 9 |  |  |  |  |  | X | X | X |  | X |
| 10 |  |  |  |  |  | X | X | X | X |  |

We have also tested the transfer time of messages between clients. As this is a chat program it is essential that the time it takes for messages to be sent from one client to another is not drastically increased by the enhanced security and anonymity. We have a set a goal of having the message communication not be more than five times the time it takes for direct communication between clients. Essentially our goal was for every client to be within five hops of other clients. We found that in testing it took an average of 3.89 seconds for a message to propagate in an environment that consisted of 15 peers. In an environment of five peers, it took 1.30 seconds for a message to propagate. This meets our standards for success.

We have also verified the encryption of our messages to ensure that the content of them stays private. To do so we have encrypted the messages with AES and are using public / private keys to encrypt the AES encryption key. This ensures that the messages can only be opened by their intended recipient.