CSC573 - Spring20
Project proposal

CHAT ROOM COMMUNICATION WITH ENCRYPTION

Submitted on: 02/20/2020

Team:
Abhishek Gadireddy - agadire
Lakshmi Aishwarya Nellutla - lnellut
Lokesh Reddy Police - lpolice
Unith Mallavaram - ukmallav

Introduction:

We are planning to implement a chat room with the support of file transfer and socket programming. To achieve low latency, we intend to use UDP as our transport layer protocol and reliability is implemented in the application using GoBack-N or Selective Repeat algorithm.

Problem Statement:

Implement a chat room with the capabilities of exchanging encrypted messages as well as files among the peers in the room. The application should also let the users in the room to send encrypted data to selected peers.

Project Objectives:

- Broadcast messages *(Sending a message to all the other clients in the chat room)*
- Broadcast files *(Sending file to all the other clients in the chat room)*
- Unicast messages *(Sending a message to a specific client in the chat room)*
- Unicast files *(Sending a file to a specific client in the chat room)*
- Blockcast messages *(Sending a message to all the clients excluding the client id's which is provided)*
- Blockcast files *(Sending a file to all the clients excluding the client id's which is provided)*
- Multicast messages *(Sending a message to multiple clients)*
- Multicast files *(Sending a file to multiple clients)*
- Encrypt all the communication.
- Ensure reliable delivery using GoBack-N or Selective Repeat algorithm in the application.

How we plan to carry out your project:

We plan to code the application in Python3. Python libraries will be used for socket based programming. We might also have to use some software like maven for dependency management and GIT for version management.

How we evaluate our project:

- Test the connectivity of the chat system
    - All the peers that are present in the chat system should be connected to the server.
- All the messages and files that are being sent should be in encrypted format.
- Should support broadcasting messages and files to all the clients in the chat room.
- Should support unicasting messages or files to a particular client in the chat room
- While broadcasting data, blocked peers shouldn’t receive the data.
- Should support multicasting messages and files to several selected peers in the chat system.
- Reliably exchanging messages and files.

What exactly will be shown during the demo:

- Test the connectivity of all the peers.
    - Broadcast a ping message from the server to all the clients and get the response back.
- Send encrypted messages to the clients.
    - To test encryption, don't decrypt the messages at the receiver end and check if the messages are encrypted.
- Broadcast a message to all the peers and get the response back.
    - If there is a packet loss to a particular peer during the transmission, retransmit that packet.
    - Should receive acknowledgments from all the peers.
- Broadcast a file to all the peers in the chat room.
    - Retransmit packets in case of packet loss.
- Multicast a message and a file to the selected multiple peers.
- Unicast a message and a file to a particular client.
    - Should get an acknowledgment from only that particular client.
    - Drop a packet and only that packet has to be retransmitted.
- Blockast a message and file:
    - The clients that are being blocked shouldn't receive the message or file.