UNIVERSIDADE FEDERAL DE MINAS GERAIS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
REDES DE COMPUTADORES - Prof. Aldri Luiz dos Santos

Sistema de Controle de Acesso aos Prédios Universitários

Trabalho prático

Júlio Guerra Domingues

2022431280

Introdução

O presente trabalho prático tem como objetivo o desenvolvimento de um sistema distribuído destinado ao controle de acesso em prédios universitários. A arquitetura proposta é composta por dois tipos distintos de servidores—Servidor de Usuários (SU) e Servidor de Localização (SL)—e múltiplos clientes denominados Interfaces de Controle (IC). O foco principal reside na implementação de um modelo funcional de comunicação cliente-servidor e servidor-servidor, utilizando sockets com suporte a IPv4 e IPv6. O sistema foi concebido para realizar operações essenciais, tais como o cadastro de usuários, controle de acessos, consultas de localizações e a gestão de desconexões controladas. Além disso, o sistema suporta a troca de mensagens entre pares de servidores (peer-to-peer), assegurando a integridade e consistência dos dados compartilhados.

Mensagens

A comunicação entre os componentes do sistema é estabelecida por meio de um conjunto predefinido de mensagens, conforme detalhado na seção de especificações. Estas mensagens são categorizadas em Mensagens de Controle, Mensagens de Dados e Mensagens de Erro ou Confirmação, cada uma desempenhando um papel específico na gestão das operações do sistema.

Mensagens de Controle são responsáveis por gerenciar as conexões tanto entre clientes e servidores quanto entre os próprios servidores. Exemplos incluem solicitações de conexão entre peers, entrada e saída de clientes na rede, e encerramento de conexões.

Mensagens de Dados facilitam operações como o cadastro, consulta e controle de acessos dos usuários, além de gerenciar registros de localização e autenticação de permissões especiais.

Mensagens de Erro e Confirmação sinalizam o sucesso ou falha das operações realizadas, garantindo a robustez e confiabilidade do sistema.

A implementação cuidadosa dessas mensagens, de acordo com a especificação, foi fundamental para assegurar a compatibilidade e a comunicação eficaz entre os diferentes componentes do sistema.

Arquitetura

O sistema foi projetado com uma arquitetura distribuída baseada no modelo cliente-servidor, integrando também uma interação peer-to-peer entre os servidores. Os três componentes principais do sistema são:

3.1. Servidor de Usuários (SU)
O SU é responsável pelo gerenciamento do cadastro de usuários e pelo controle de seus acessos. Além disso, atua como intermediário ao encaminhar mensagens de registro de localização para o Servidor de Localização (SL), facilitando operações que envolvem múltiplos servidores.

3.2. Servidor de Localização (SL)
O SL armazena informações relativas às localizações dos usuários e gerencia consultas associadas. Possui um mecanismo de pendência para operações de inspeção (inspect), garantindo que apenas uma operação seja processada por vez, o que previne conflitos em consultas simultâneas.

3.3. Cliente (Interface de Controle - IC)
As ICs servem como interfaces de interação com os servidores SU e SL, permitindo a execução de comandos como add, find, in, out, inspect e kill. Esses comandos facilitam o cadastro, consulta e controle de acessos, bem como a desconexão controlada do sistema.

A comunicação entre os componentes foi implementada utilizando sockets TCP com suporte a IPv4 e IPv6, o que proporciona escalabilidade e compatibilidade com as especificações. A interação peer-to-peer entre os servidores foi cuidadosamente projetada para manter a integridade dos dados e evitar conflitos durante operações simultâneas.

Servidores

Os servidores SU e SL compartilham uma base de código comum, porém desempenham funções distintas dentro do sistema. Ambos utilizam arrays estáticos para armazenar informações críticas, como usuários cadastrados no SU e registros de localização no SL. Cada servidor possui mecanismos próprios para gerenciar conexões de clientes e mensagens de peers, assegurando uma operação eficiente e organizada.

No SU, as operações de controle de acesso—especificamente os comandos in e out—envolvem verificações locais dos usuários e comunicação com o SL para registrar ou remover localizações. Por outro lado, no SL, a operação inspect é gerenciada por um sistema de pendência que garante que apenas um comando seja processado por vez, prevenindo conflitos em consultas simultâneas.

Além disso, ambos os servidores implementam mecanismos para gerenciar desconexões controladas, tanto de clientes quanto de peers, utilizando mensagens como REQ_DISC e REQ_DISCPEER. Isso é fundamental para manter a consistência e integridade da rede, assegurando que todas as conexões sejam devidamente encerradas e os recursos sejam liberados de maneira apropriada.

4.1. Comunicação Peer-to-Peer

A comunicação entre os servidores SU e SL foi implementada utilizando uma abordagem peer-to-peer, onde ambos os servidores podem atuar de forma ativa ou passiva na conexão. Essa interação permite a troca direta de informações e comandos, garantindo a sincronização e consistência dos dados armazenados em cada servidor.

4.2. Suporte a IPv4 e IPv6

Para garantir a compatibilidade e flexibilidade nas conexões de rede, os servidores foram desenvolvidos com suporte a ambos os protocolos IPv4 e IPv6. Essa implementação permite que o sistema seja utilizado em diferentes ambientes de rede, ampliando sua aplicabilidade e facilitando futuras expansões.

Clientes

As Interfaces de Controle (IC) foram concebidas como interfaces simples e funcionais para interação com os servidores SU e SL. Elas suportam uma variedade de comandos que permitem a realização de operações essenciais dentro do sistema:

- add <UID> <0|1>: Solicita ao SU o cadastro de um novo usuário, indicando se ele possui permissões especiais.
- find <UID>: Consulta a localização atual de um usuário no SL.
- in <UID>: Registra a entrada de um usuário em uma determinada localização.
- out <UID>: Registra a saída de um usuário de uma determinada localização.

- inspect <UID> <Loc>: Lista todos os usuários presentes em uma localização específica, validando a permissão do usuário informado.
- kill: Solicita a desconexão da IC e encerra a comunicação com os servidores.

A implementação das ICs foi estruturada de maneira a estabelecer conexões ativas com os servidores SU e SL, enviar comandos e processar as respostas de forma clara e concisa. Um mecanismo de leitura foi desenvolvido para garantir que todas as mensagens sejam recebidas e processadas adequadamente, evitando problemas de buffer e assegurando a robustez da comunicação.

Discussão

O desenvolvimento deste sistema apresentou uma série de desafios que demandaram soluções criativas e meticulosas. Um dos principais obstáculos enfrentados foi a necessidade de garantir que todas as mensagens trocadas entre os componentes do sistema seguissem exatamente a especificação predefinida. A diversidade e complexidade das mensagens, juntamente com suas variações, exigiram um alto nível de atenção aos detalhes para assegurar a compatibilidade e funcionalidade desejadas.

Adicionalmente, a ausência de ferramentas automatizadas para testes representou uma barreira significativa, obrigando o uso de múltiplos terminais para simular os diferentes componentes do sistema. Este método manual de testes foi não apenas demorado, mas também propenso a erros, especialmente em cenários que envolviam interações peer-to-peer complexas e comandos como inspect. A implementação de suporte aos protocolos IPv4 e IPv6 também constituiu um desafio considerável, necessitando de consultas e orientações adicionais para resolver questões técnicas específicas relacionadas aos protocolos.

Outro aspecto crítico foi a implementação da comunicação peer-to-peer entre os servidores, que exigiu a criação de mecanismos robustos para lidar com comandos de handshake e garantir a consistência nas operações. A correta gestão dos identificadores de peers (PidSi e PidSj) foi essencial para evitar conflitos e assegurar a integridade das conexões estabelecidas.

O trabalho também evidenciou a importância de uma documentação clara e detalhada, tanto para a implementação das mensagens quanto para a estrutura geral do sistema. A complexidade das interações peer-to-peer ressaltou a necessidade de um design modular e bem estruturado, facilitando futuras manutenções e expansões do sistema.

Por fim, o projeto ressaltou a relevância da comunicação clara e precisa entre os componentes distribuídos, essencial para manter a consistência e a integridade do sistema como um todo. A integração eficaz dos protocolos IPv4 e IPv6 demonstrou a importância de considerar a flexibilidade e a compatibilidade em projetos de redes, garantindo que o sistema possa operar em diversas infraestruturas de rede.

Conclusão

O presente trabalho proporcionou uma oportunidade para explorar e implementar conceitos fundamentais de sistemas distribuídos, tais como comunicação cliente-servidor, interação peer-to-peer e gerenciamento de conexões em redes IPv4 e IPv6. Apesar dos desafios técnicos e operacionais enfrentados durante o desenvolvimento, o sistema desenvolvido atende às especificações estabelecidas e demonstra um modelo distribuído funcional para o controle de acesso em ambientes universitários.

Os principais aprendizados extraídos deste projeto incluem o manuseio eficiente de sockets em ambos os protocolos IPv4 e IPv6, a importância de aderir a especificações rigorosas para garantir a compatibilidade e a necessidade de desenvolver sistemas de teste robustos para validar funcionalidades complexas. Além disso, o trabalho destacou a relevância de uma comunicação clara e precisa entre os componentes distribuídos, essencial para manter a consistência e a integridade do sistema como um todo.