Desenvolvimento de um sistema descentralizado de envio de mensagens

Uma análise de dificuldades e limitações

Aluno: João Renner Rudge | Orientador: Daniel Macêdo Batista

Bacharelado em Ciência da Computação

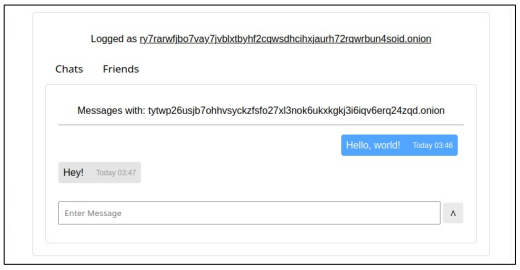
Instituto de Matemática e Estatística – Universidade de São Paulo

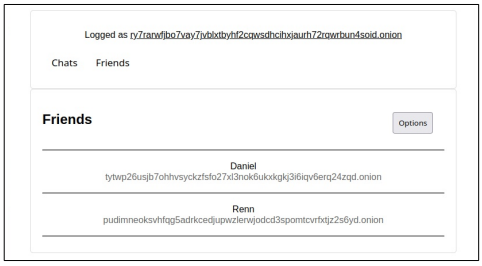
Proposta de trabalho

Este Trabalho de Conclusão de Curso tem como objetivo a análise das características positivas e negativas de sistemas descentralizados de envio de mensagens pela internet, e posteriormente buscando a implementação de um protótipo funcional.

Esta monografia se insere no contexto da crescente centralização da internet moderna, que pode ser observada tanto no mercado de hospedagem web, na distribuição de *Content Delivery Networks* (CDNs), ou até mesmo na propagação da versão mais recente do protocolo de segurança *Transport Layer Security* (TLS), . Nos últimos 20 anos, a adoção de sistemas descentralizados caiu significativamente. **O objetivo deste trabalho é discutir as vantagens e limitações de protocolos distribuídos para envio de mensagens em redes de computadores.**

A arquitetura híbrida proposta para o projeto de protocolo utiliza serviços ocultos do *Tor* na comunicação entre usuários. Cada usuário hospeda seu próprio serviço oculto com um par de chaves público-privadas e expõe uma API acessível por outros usuários, permitindo funcionalidades como envio de mensagens, verificação de status de amizade e estabelecimento de conexões P2P diretas. A comunicação padrão esconde o IP, mas, para reduzir latência, usuários podem optar por conexões diretas ao adicionarem outros como "amigos". Nesse modelo, a conexão P2P é estabelecida apenas quando ambos os usuários estão online, possuem o chat aberto e confiam um no outro.

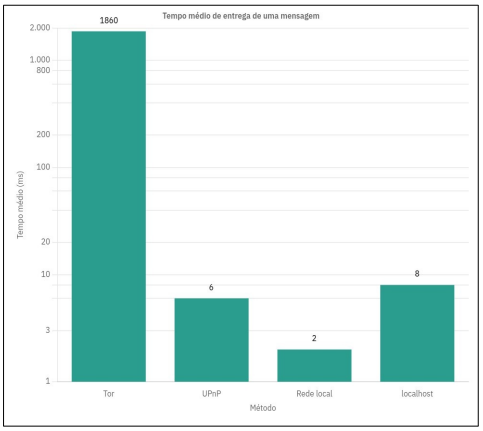




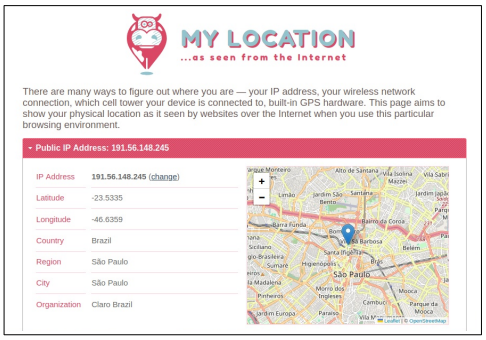
Capturas de tela de uma conversa e da interface de amigos

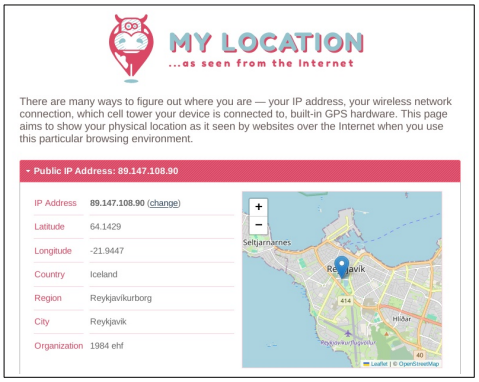
Resultados

O protótipo desenvolvido cumpre os requisitos que foram estabelecidos, permitindo comunicação entre usuários por meio da rede do *Tor*, por meio de conexão P2P por UPnP, por meio de conexão pela rede local entre dois usuários, e por conexão via *localhost*. A latência de envio de mensagens via cada uma dessas vias foi medida e analisada, com resultados a seguir:



Tempo de entrega de uma mensagem para cada método de conexão, em milissegundos





Capturas de tela de um site de localicação realizadas usando um navegador comum (acima), e o Tor (abaixo). Note que mesmo sendo acessados do mesmo lugar, o site acessado pelo tor não consegue determinar corretamente a localicalização do usuário.