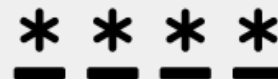




Computação Distribuída

Projeto Final

Distributed Password Cracker



Andreia de Sá Portela, 97953
Diana E. Siso Oliveira, 98607

Arquitetura



Cada slave tem um ID próprio, isto é um número aleatório entre 0 e 10000. Como só vamos ter no máximo 3-4 slaves (quando temos 4, o 4º é expulso), é pouco provável que haja colisão de IDs.

A comunicação entre slaves é feita unicamente em multicast seguindo o protocolo explicado a seguir.

Para dividir o trabalho, temos um slave coordenador (denominado “boss”), que é escolhido automaticamente de acordo com o tempo de registo. Se este falhar, o primeiro slave a reparar torna-se no novo boss. O coordenador é responsável por distribuir o trabalho entre os slaves. Se um slave (que não seja coordenador) falhar, é função do coordenador redistribuir o trabalho novamente.

Os slaves mandam periodicamente mensagens “try” (“I’m alive”). Sempre que um slave receber uma mensagem deste tipo de um dos outros slaves, ele regista o ID do slave e o momento da receção da mensagem. Se um slave não tiver recebido um “try” de um outro slave nos últimos 60 segundos, ele assume que este falhou e age de acordo.

Criamos também um gerador de passwords possíveis de acordo com o tamanho da password gerada pelo server.

Para evitar ficar no estado banned, fazemos um sleep de 1s (superior ao tempo do cooldown) de 9 em 9 tentativas consecutivas.

Assim que um slave receber uma mensagem de confirmação do server, ele avisa os restantes slaves e todos fecham a conexão com o servidor.

Protocolo



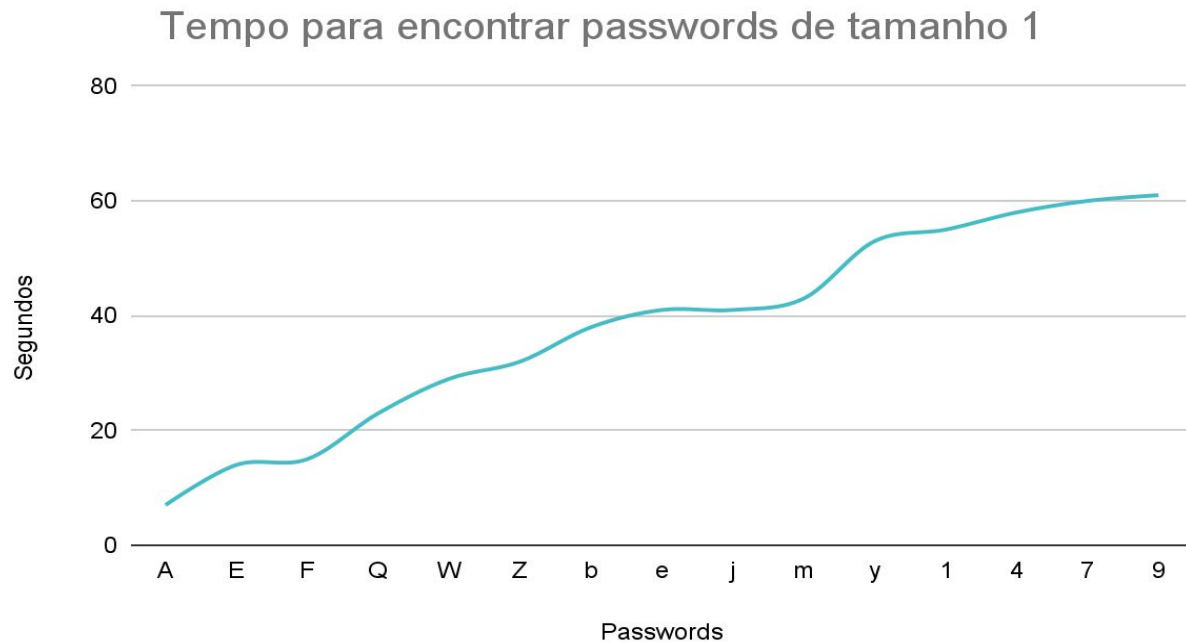
Temos 6 tipos de mensagens entre slaves:

- register: mensagem enviada por um slave ao entrar, incluindo o seu id, o numSlaves (1 por default) e o proxPass (0 no início)
- update: mensagem enviada pelo slave “boss” para os slaves restantes já funcionais, onde diz o numSlaves e o proxPass
- correct: mensagem enviada por um dos slaves assim que encontrar a password certa
- boss: mensagem a informar os outros slaves que é ele o “boss”
- bye: mensagem a expulsar um 4º slave
- try: mensagem periódica onde indica qual foi a última password tentada, utilizada como message “I’m alive”

Temos 1 tipo de mensagem entre slave e servidor:

- request: pedido incluindo a password a tentar

Resultados



Resultados

