Projeto Final de Computação Distribuída - 2020/2021

Distributed Password Cracker

Camila Fonseca - 97880
Afonso Campos - 100055

Arquitetura

- Arquitetura peer-to-peer
- Comunicação Multicast (UDP) entre slaves
- Comunicação TCP entre slave-server - Http 1.0

Protocolo

Tradução password -> int: BASE62

Exemplos (PW_SIZE = 3):

aaa -> 1; ajj -> 567; bhr -> 4321; j8m -> 38328; 999 -> 238328

Protocolo

Data structures do slave:

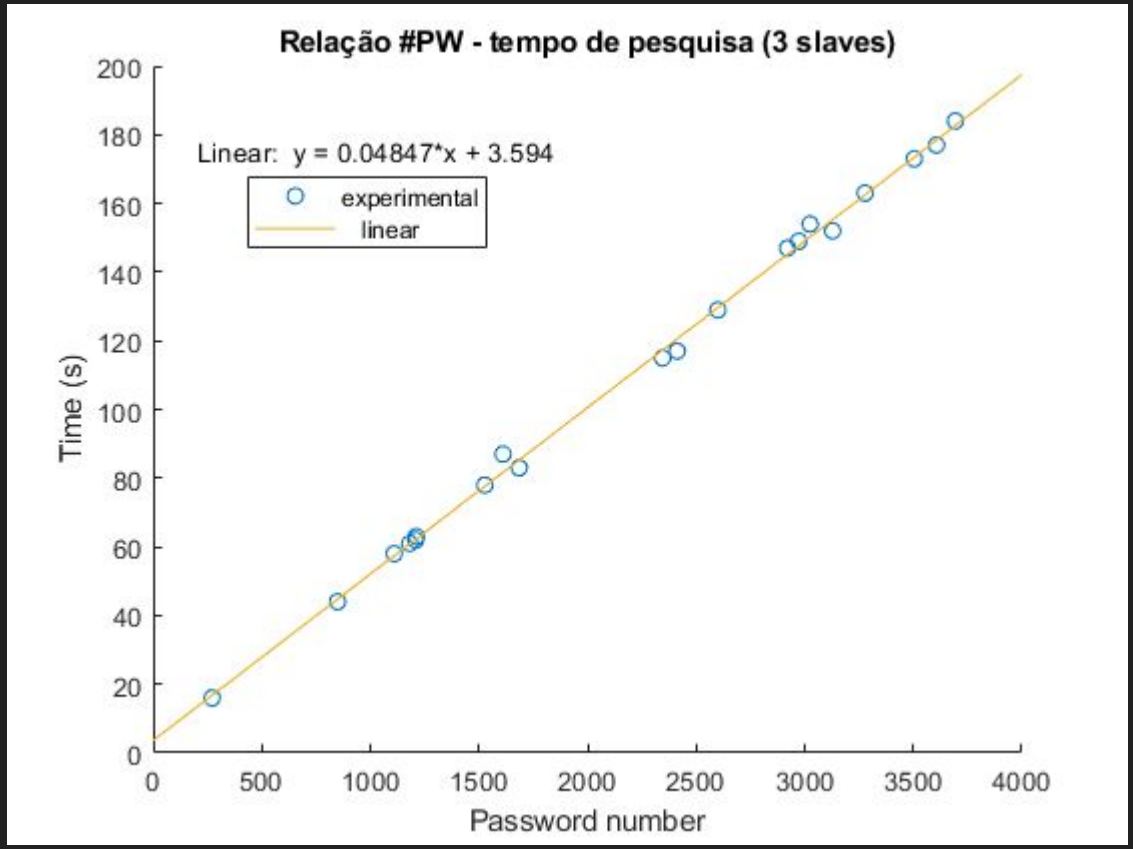
- **Verified:** array de ranges (range: [lower bound, upper bound]). Todos as pw englobadas nos ranges desta lista já foram verificadas;
- **Range:** [lower bound, upper bound]. Range de pws que o slave se encontra, de momento, a verificar;
- **Current:** última pw verificada;
- **Peers:** { peerIP : (latest response timestamp, peer range)}, qualquer peer que não tenha enviado mensagem à mais de 5s é assumido como morto.

Protocolo - Mensagens

- **IMHERE**
  - Serve de mensagem de heartbeat, i.e., ao não receber mensagens durante 5s de um determinado slave, ele é eliminado da lista de peers;
  - Informa periodicamente os outros slaves do trabalho feito (verified) e a sua range atual;
  - No caso de overlap entre o range atual e o range do slave que enviou a mensagem IMHERE, aquele com o menor ID move-se para um novo range;
  - Enviada entre cada 10 tentativas da password (autenticidade das PW verificadas SEMPRE garantida).
- **FOUNDPW**
  - Enviada quando um slave recebe uma resposta OK do servidor -> palavra passe encontrada!;
  - Ao receber, um slave cessa a sua atividade.

Resultados

Relação aparentemente linear!



Resultados

Aparentemente linear, poderá progredir para logarítmico?