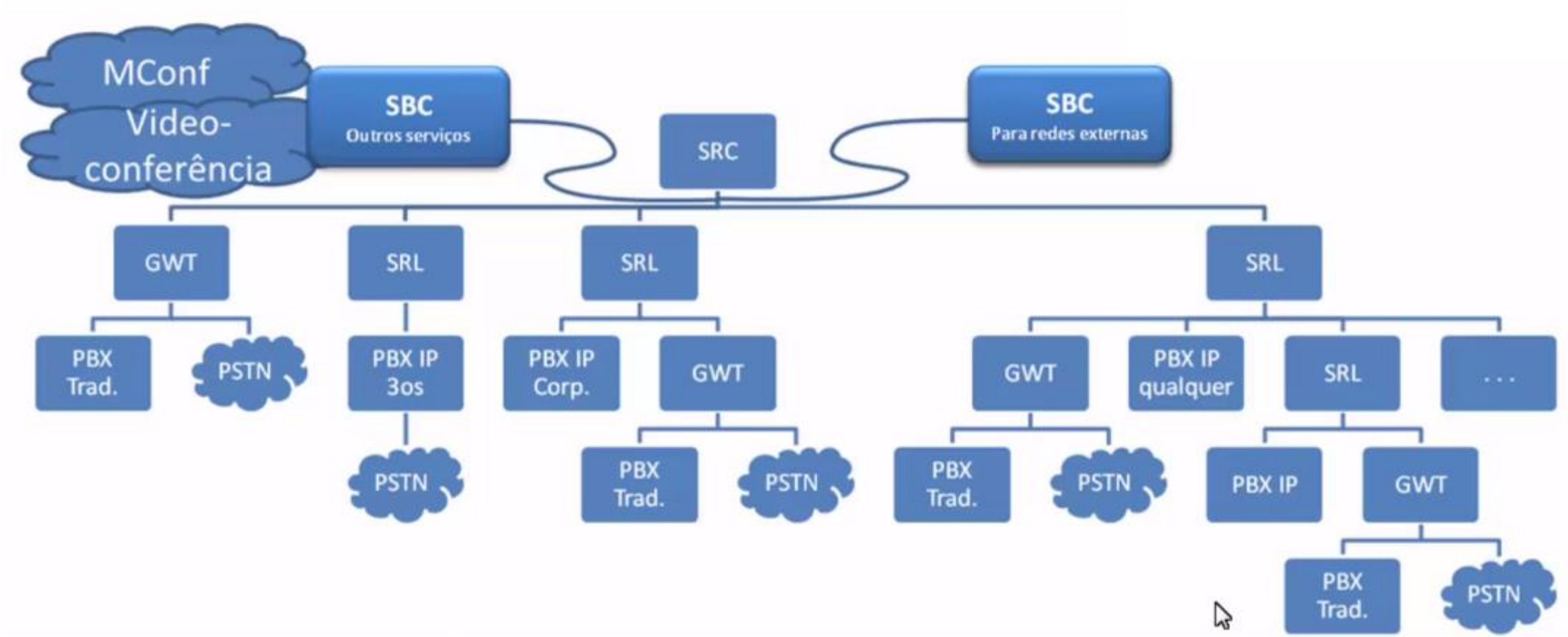
Vulnerabilidades do fone@RNP

GT-ACTIONS

Marcilio Lemos
LaR/UFPB

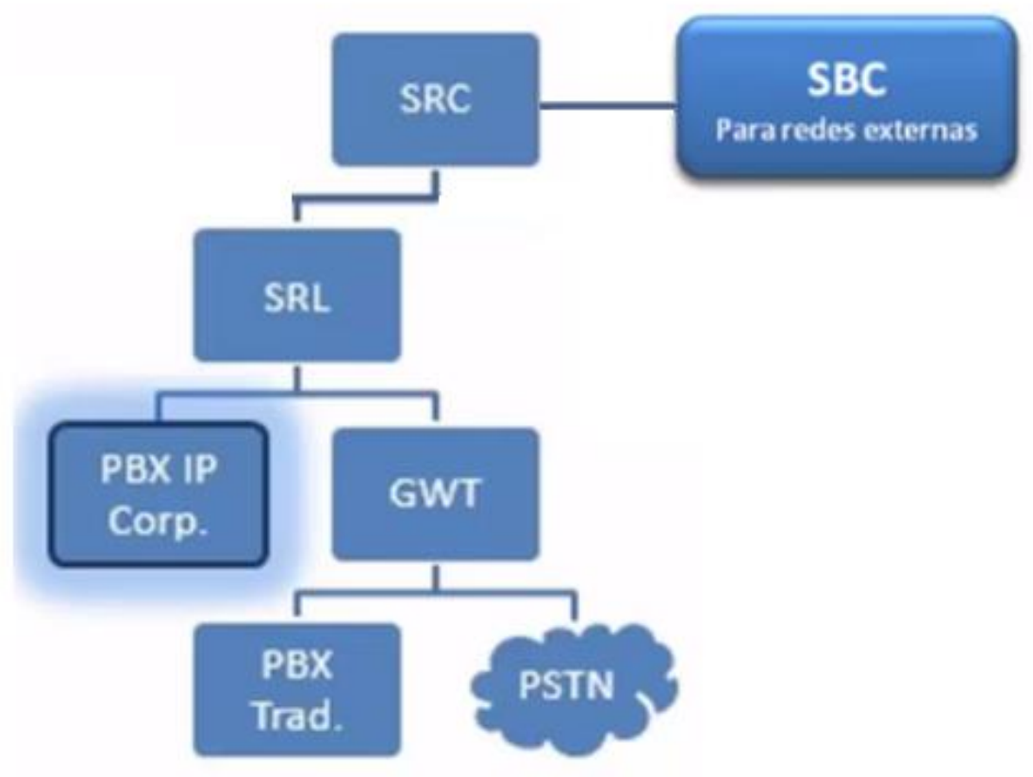
fone@RNP

Arquitetura completa do fone rnp



Módulos Analisados

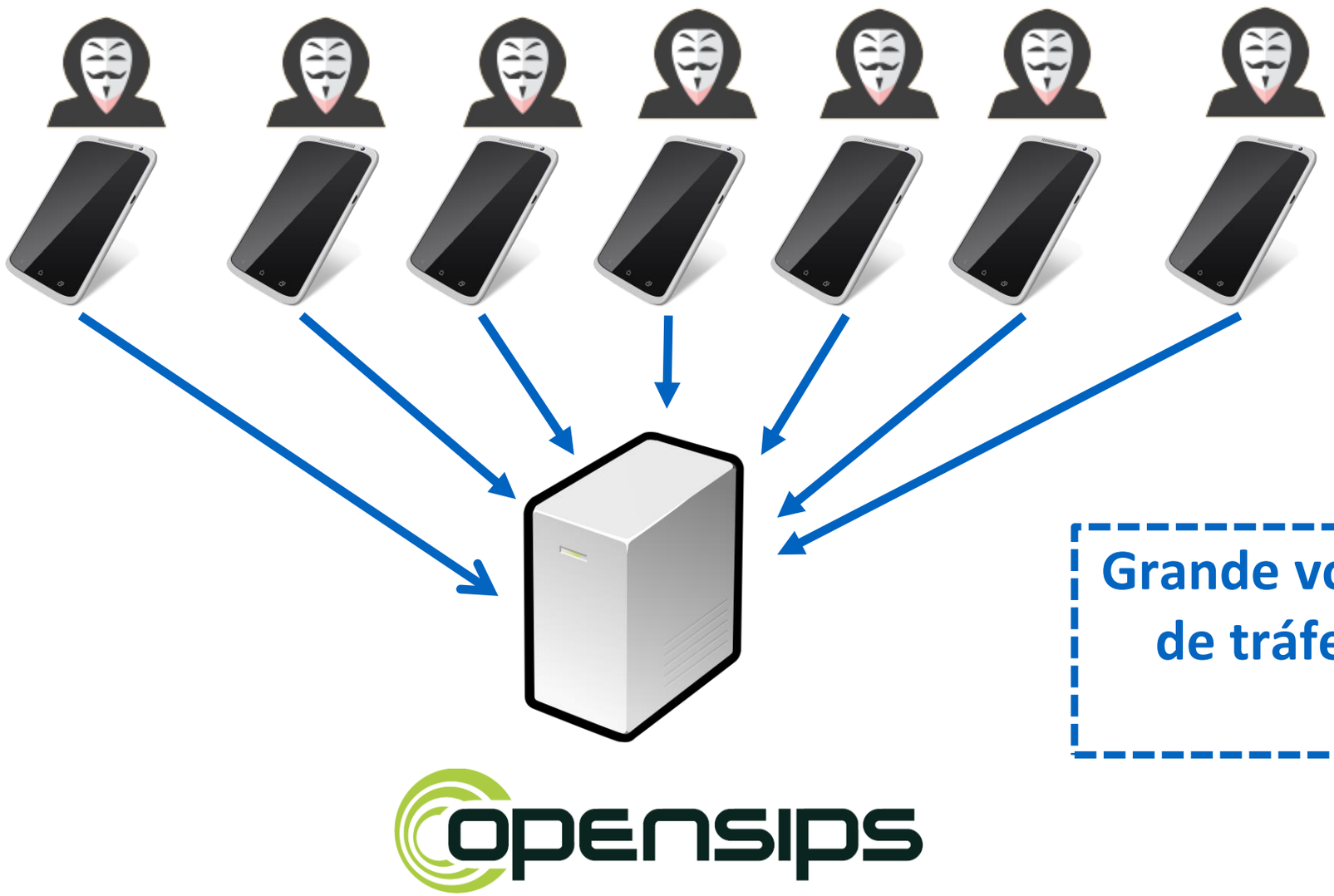
- SBC (OpenSIPS);
- SRC (OpenSIPS);
- SRL (OpenSIPS);
- GWT (Asterisk);
- PBX IP (OpenSIPS e Asterisk).



Vulnerabilidades do OpenSIPS

- Flexibilidade de roteamento e integração;
- Alto desempenho em processar chamadas (milhares por segundo);
- Diversos módulos que estendem suas funcionalidades.
- **Vulnerável a ataques de negação de serviço**.

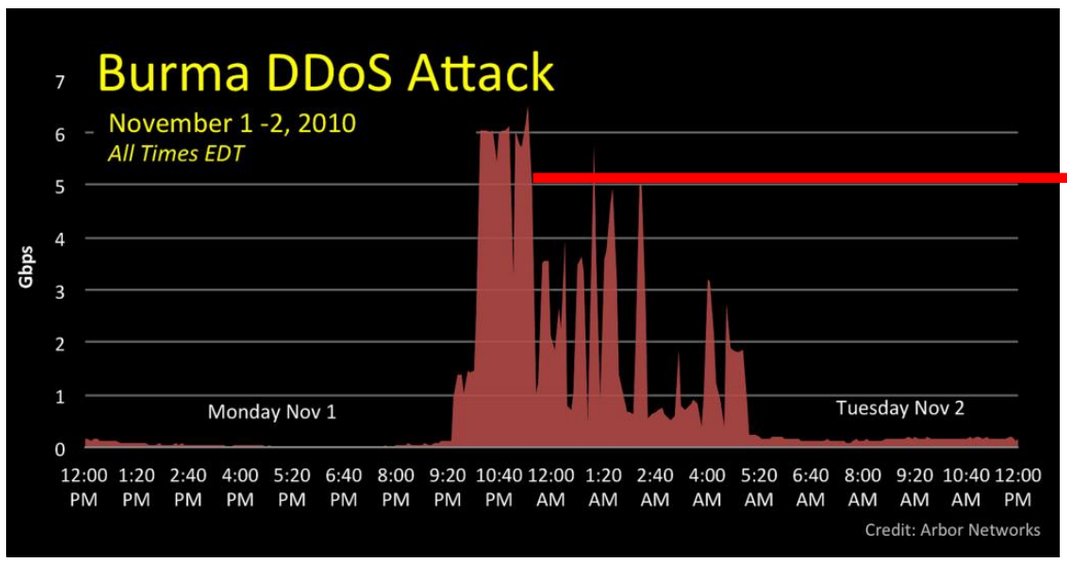
SIP *Flooding*



Grande volume de tráfego.

Módulo PIKE

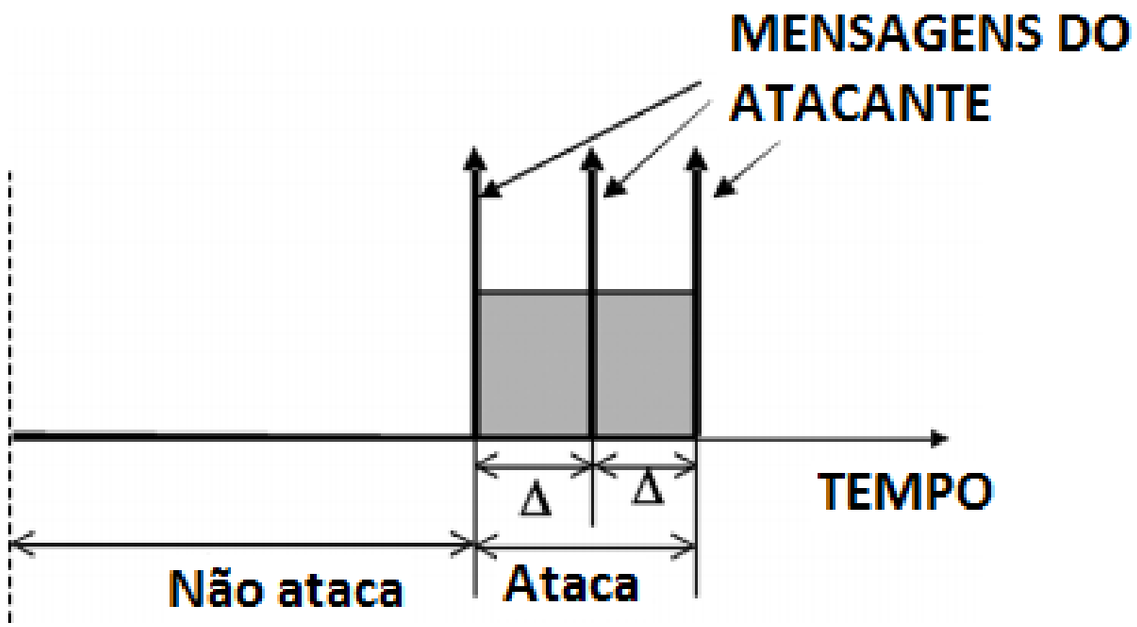
- Análise do fluxo de tráfego da rede;
- Mecanismo de bloqueio por IP;
- Parâmetros: **Sampling_time_unit** e **reqs_density_per_unit**.



Variação abrupta no tráfego!

Módulo PIKE

- Limitações:
  - Ineficaz contra atacantes que fazem uso de IP *spoofing*;
  - Atacante pode estimar os valores dos parâmetros **Sampling_time_unit** e **reqs_density_per_unit**;

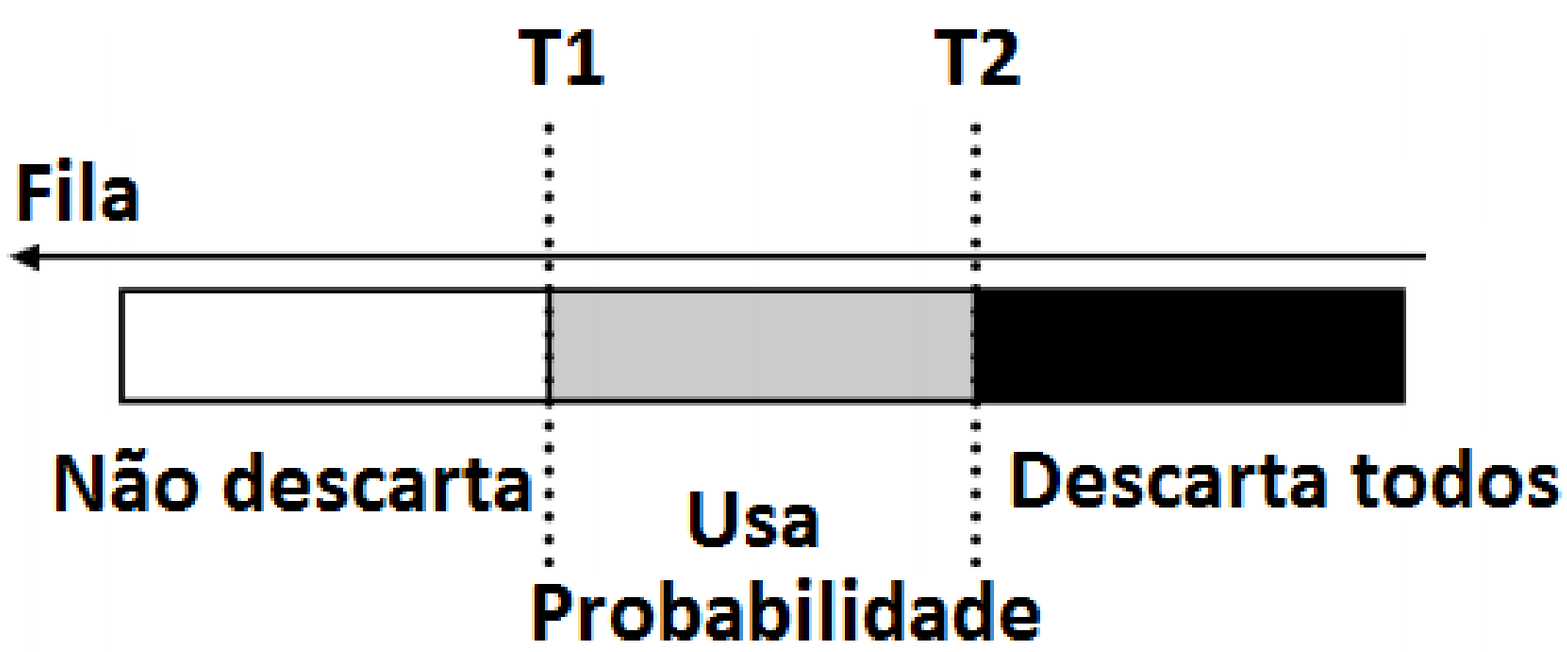


Módulo PIKE

- Limitações:
  - Pode resultar no bloqueio do serviço para todas as requisições por trás do endereço IP de um roteador NAT ou *proxy* SIP.

Módulo RATELIMIT

- Limita o fluxo de tráfego com base no tipo de requisição SIP;
- Random Early Detection (RET).
.



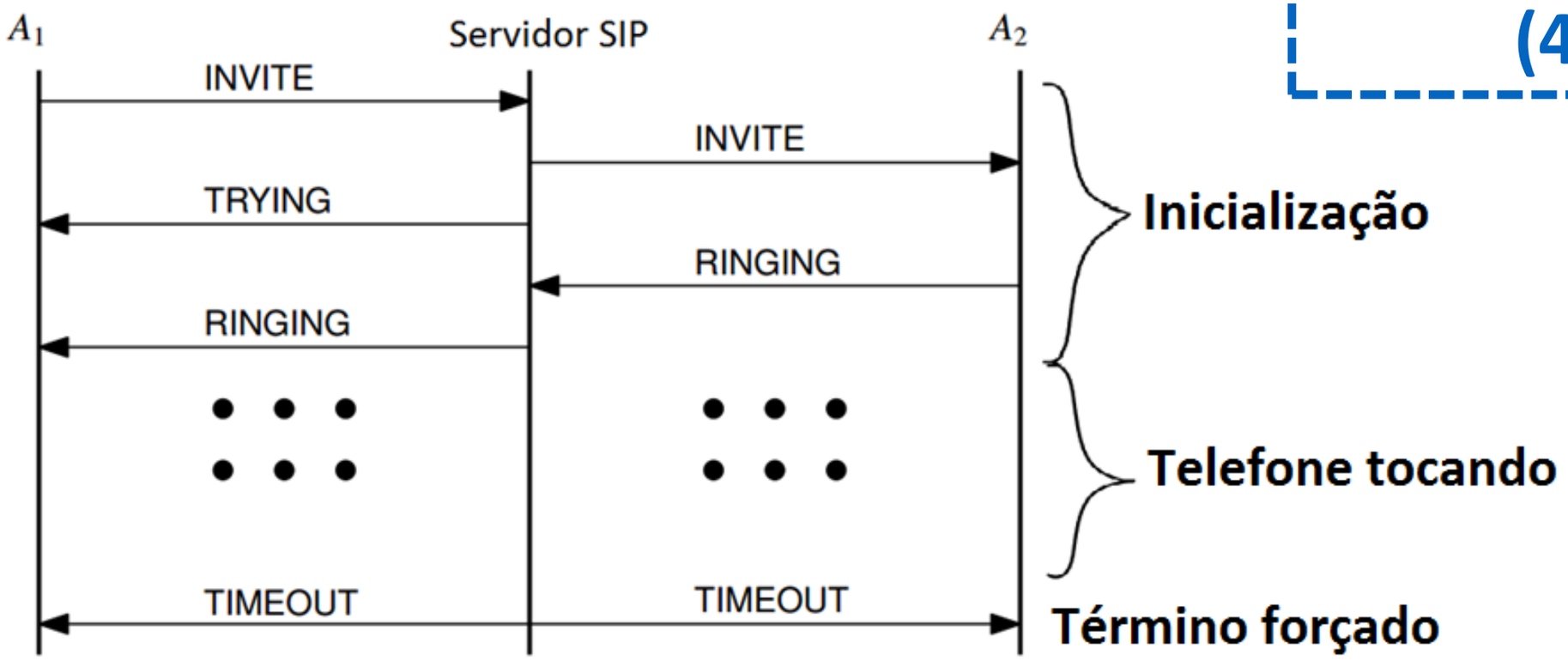
Módulo RATELIMIT

- Limitações:
  - O atacante pode manter o *buffer* do RATELIMIT completamente cheio com os seus pedidos;
  - Qualquer nova mensagem de um cliente legítimo é descartada.

Ringing-based Attack

- Ocupar de forma continua e por longos períodos de tempo a memória do servidor:

Módulo TM: fr_inv_timer (40s)

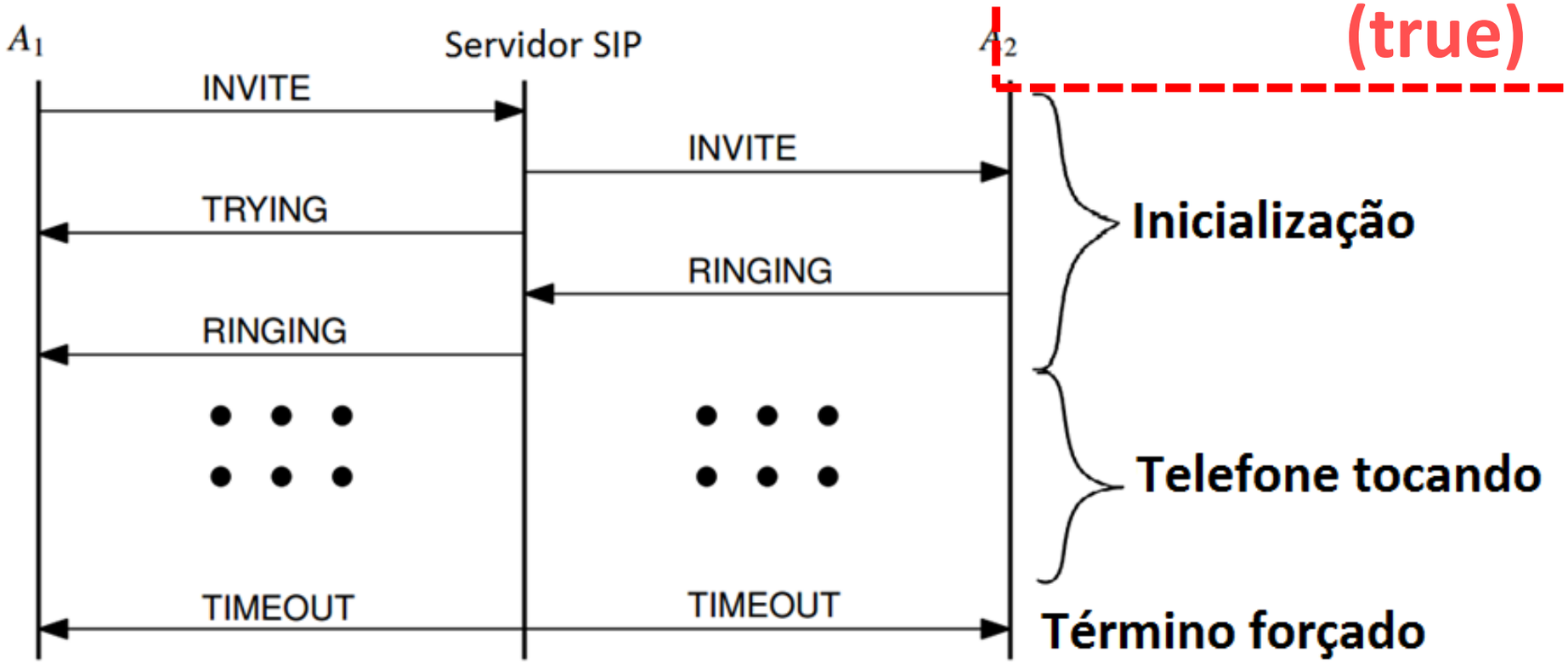


Ringing-based Attack

- Ocupar de forma continua e por longos períodos de tempo a memória do servidor:

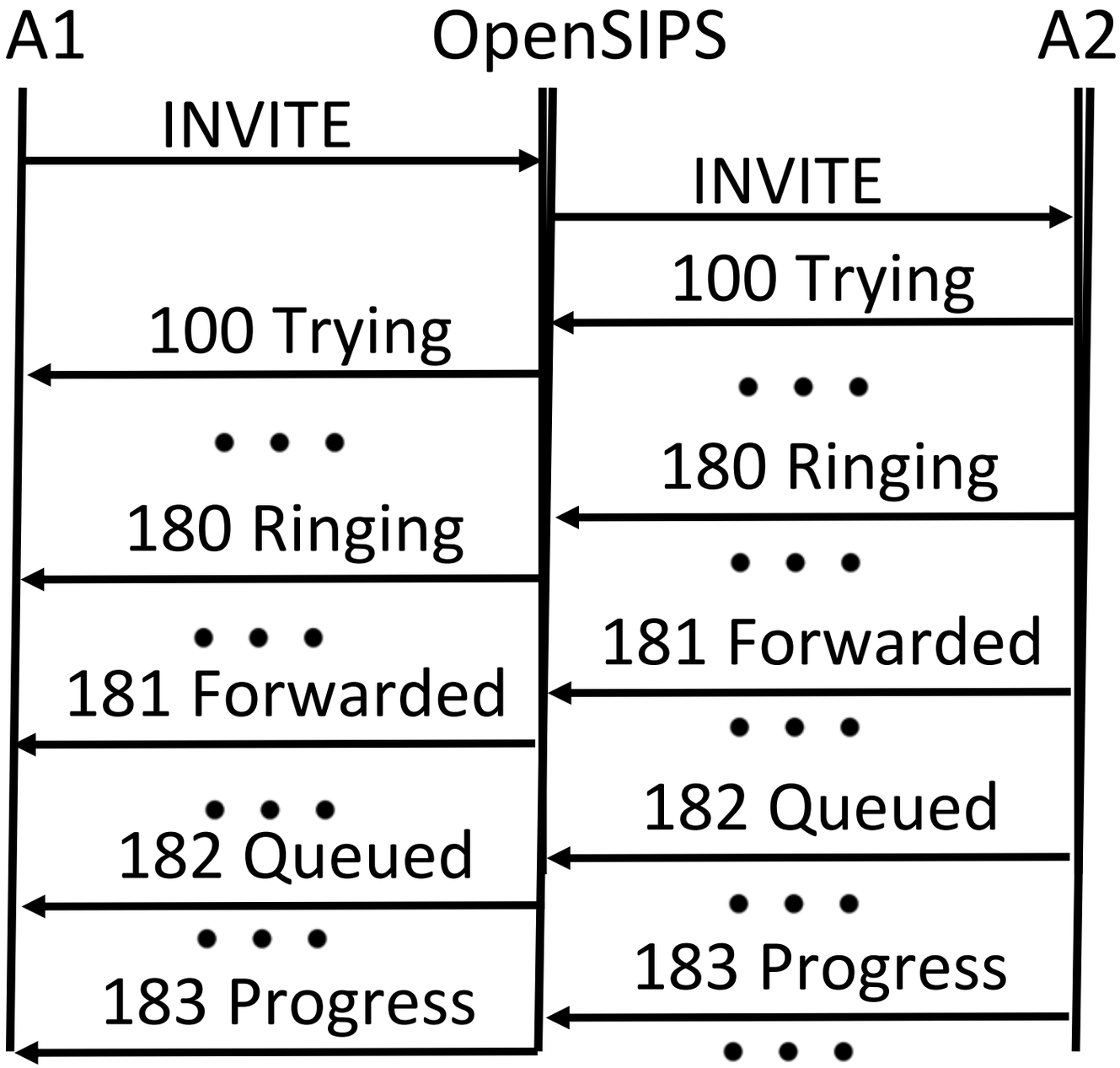
PERIGOSO!!!!!

Módulo TM: restart_fr_on_each_reply (true)



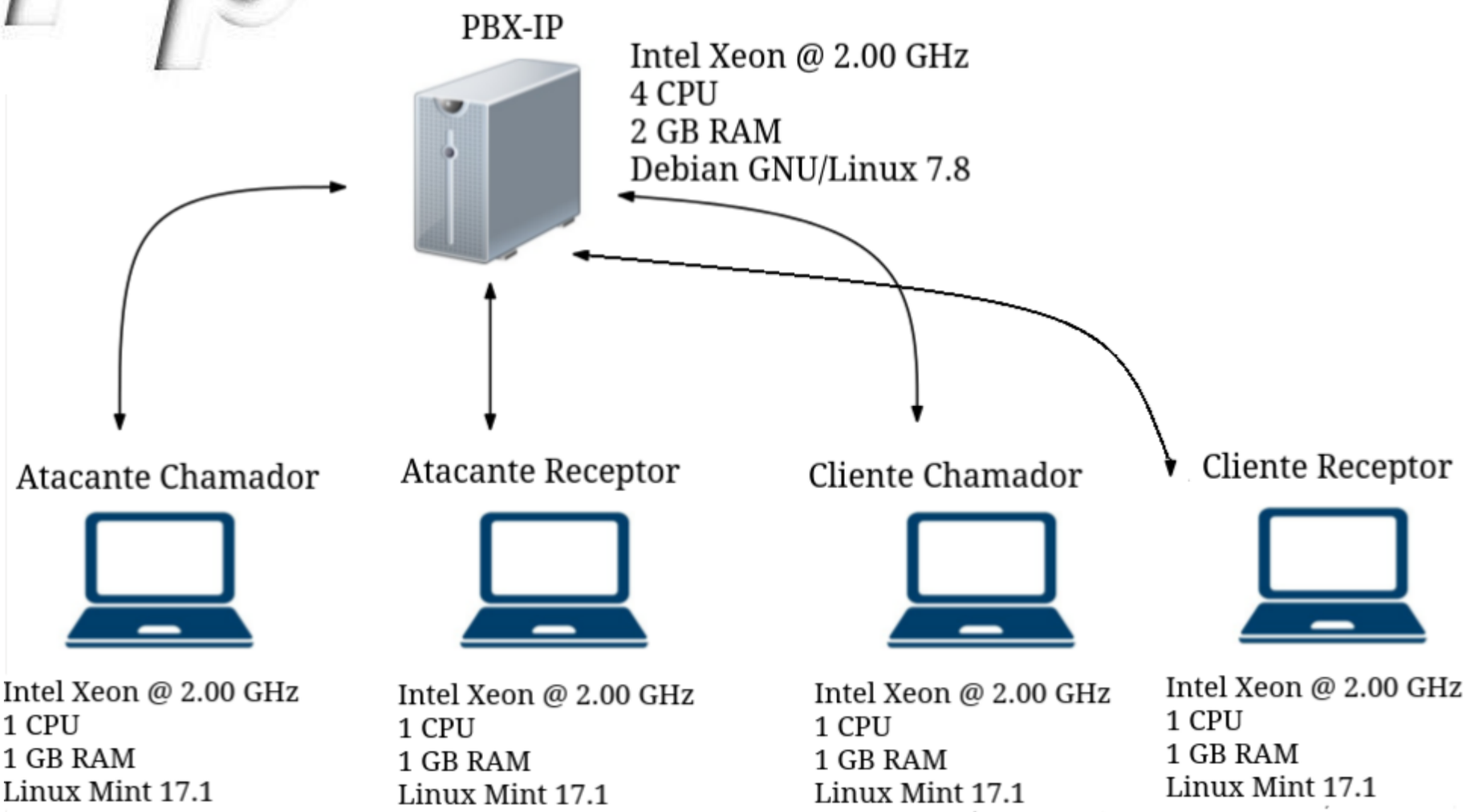
Provisional Ringing-based Attack

- Engana **fr_inv_timer** por 5 rodadas (mais de 3 minutos).



Experimento

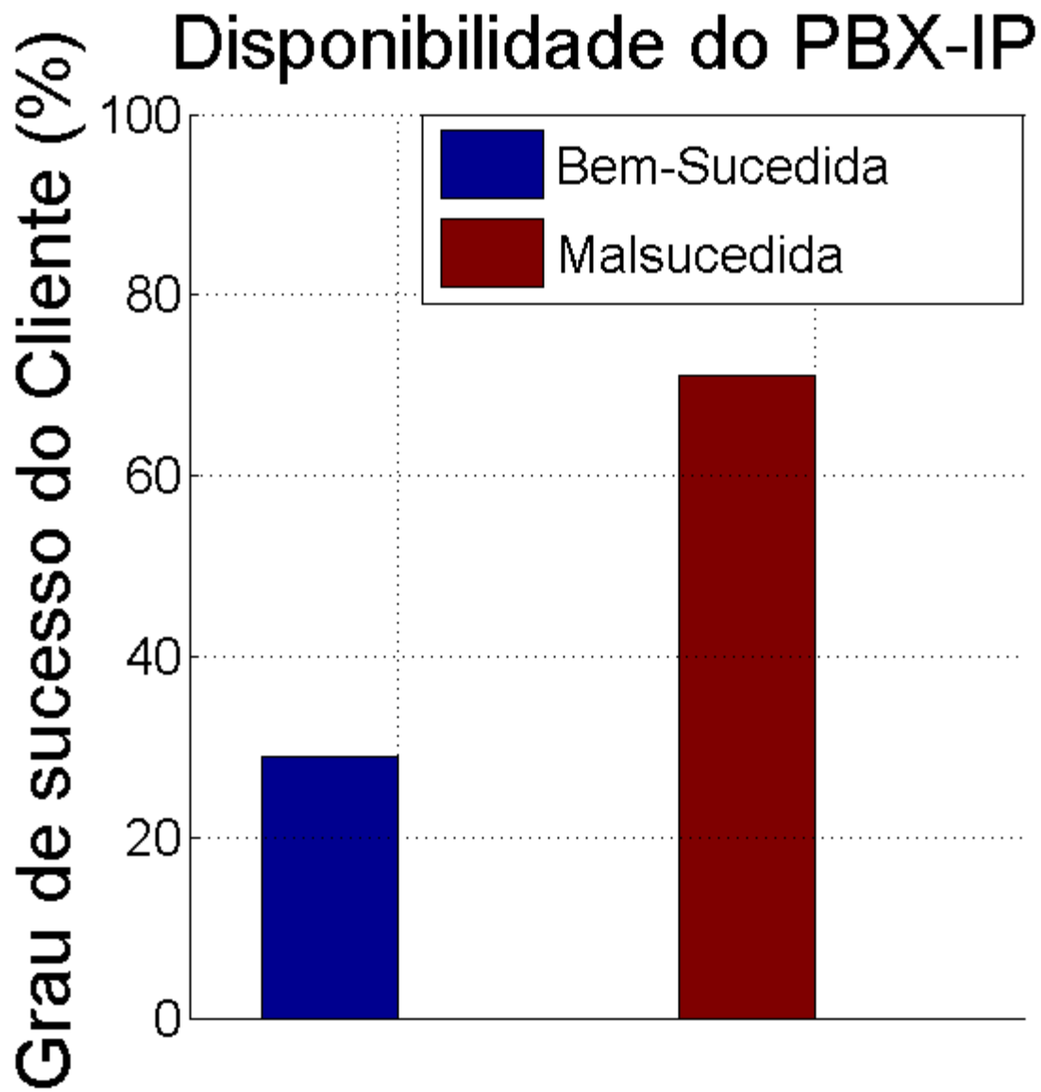
SIPp



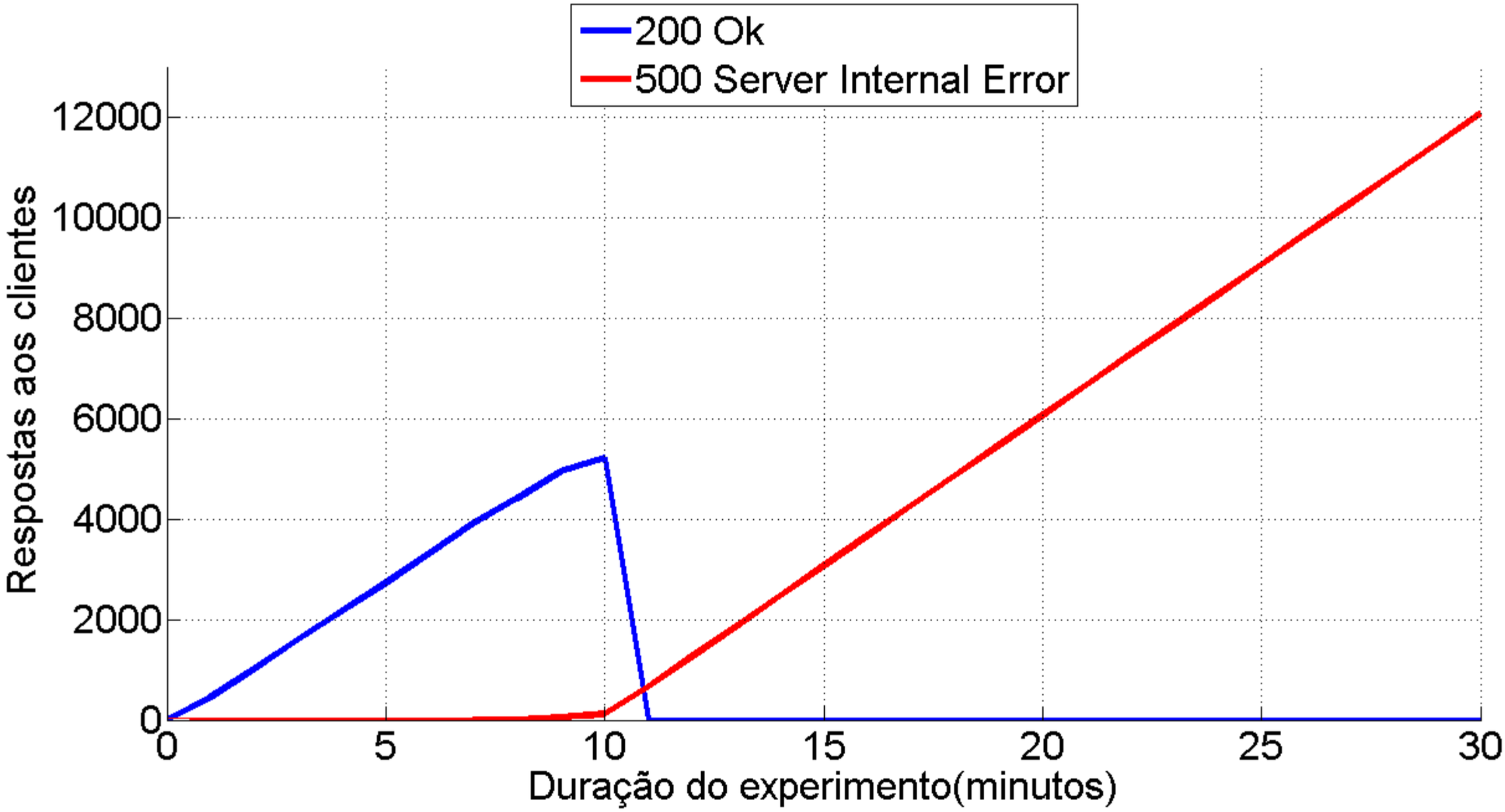
Experimento

- Parâmetros do experimento:
  - **Duração do toque das chamadas de clientes honestos**: distribuição gama com média de 20 segundos;
  - **Duração do toque das chamadas de atacantes:** 195 segundos (5*fr_inv_timer);
  - **Taxa de tráfego dos clientes honestos:** 10 chamadas por segundo;
  - **Taxa de tráfego dos atacantes:** 40 chamadas por segundo;
  - **Tempo total do experimento:** 30 minutos.

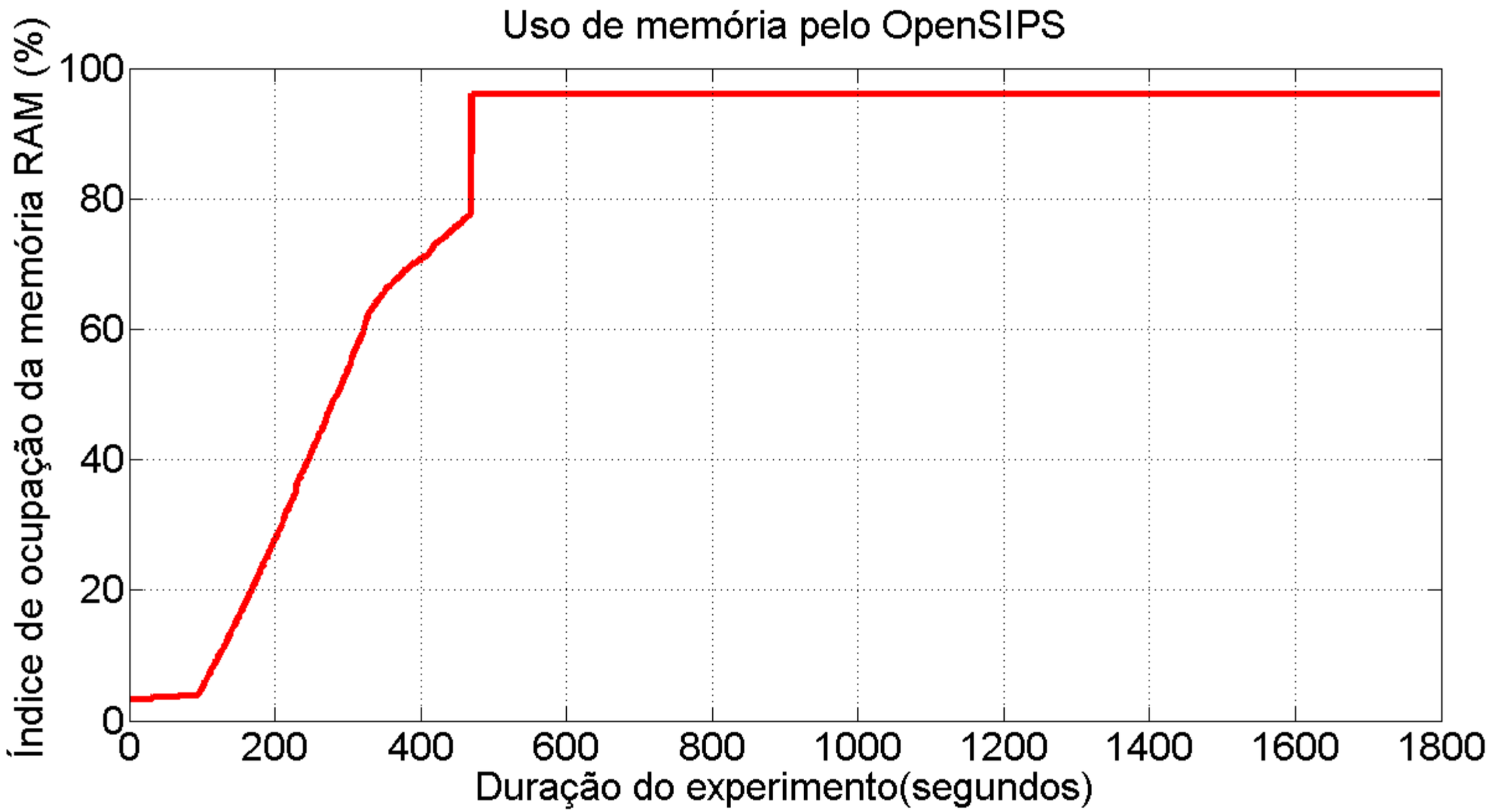
Resultados do Experimento



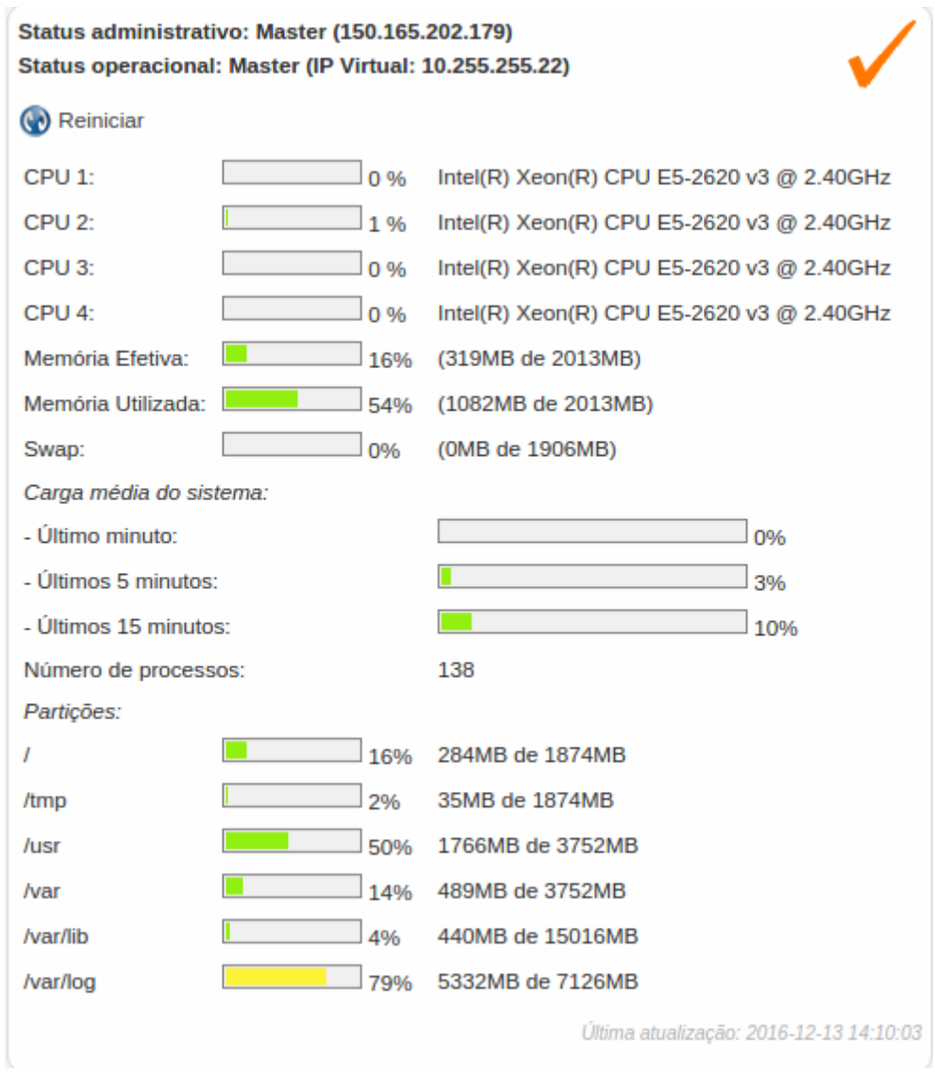
Resultados do Experimento



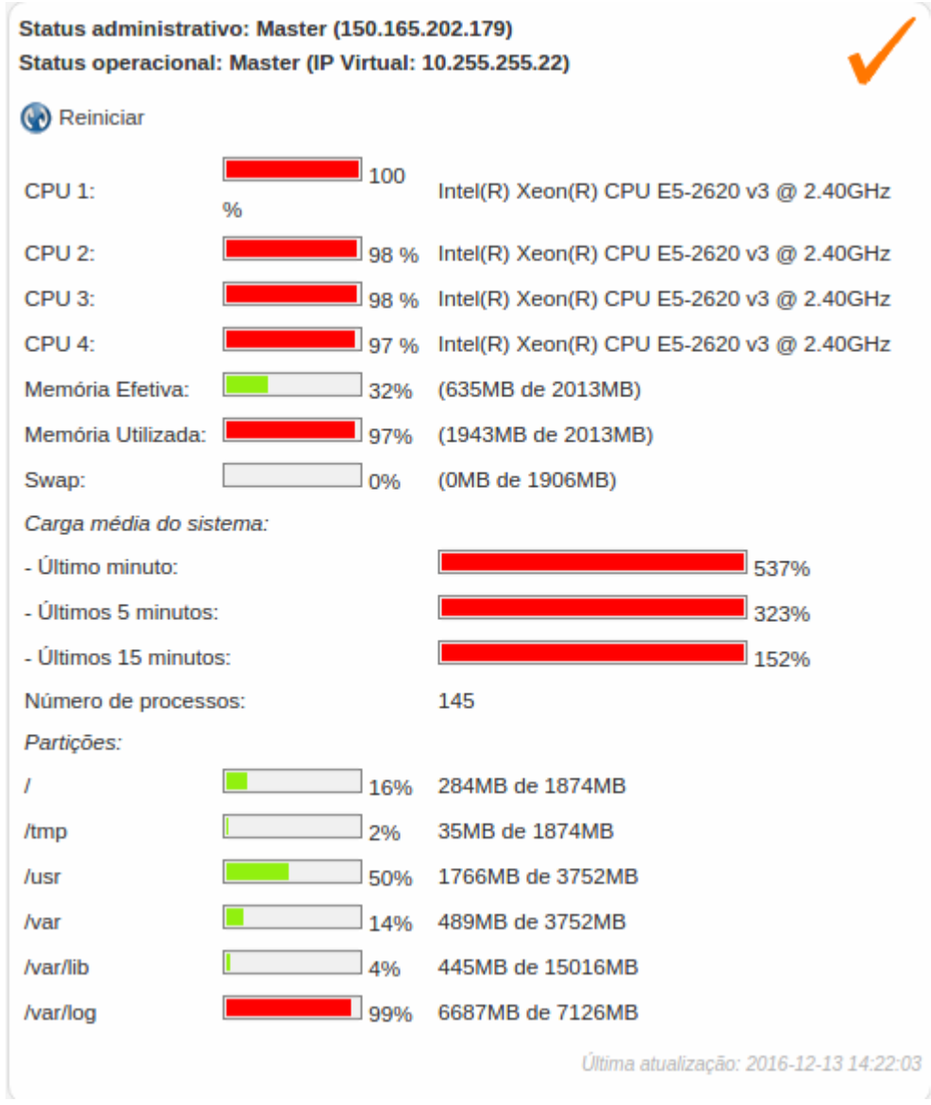
Resultados do Experimento



Resultados do Experimento



Antes do Ataque

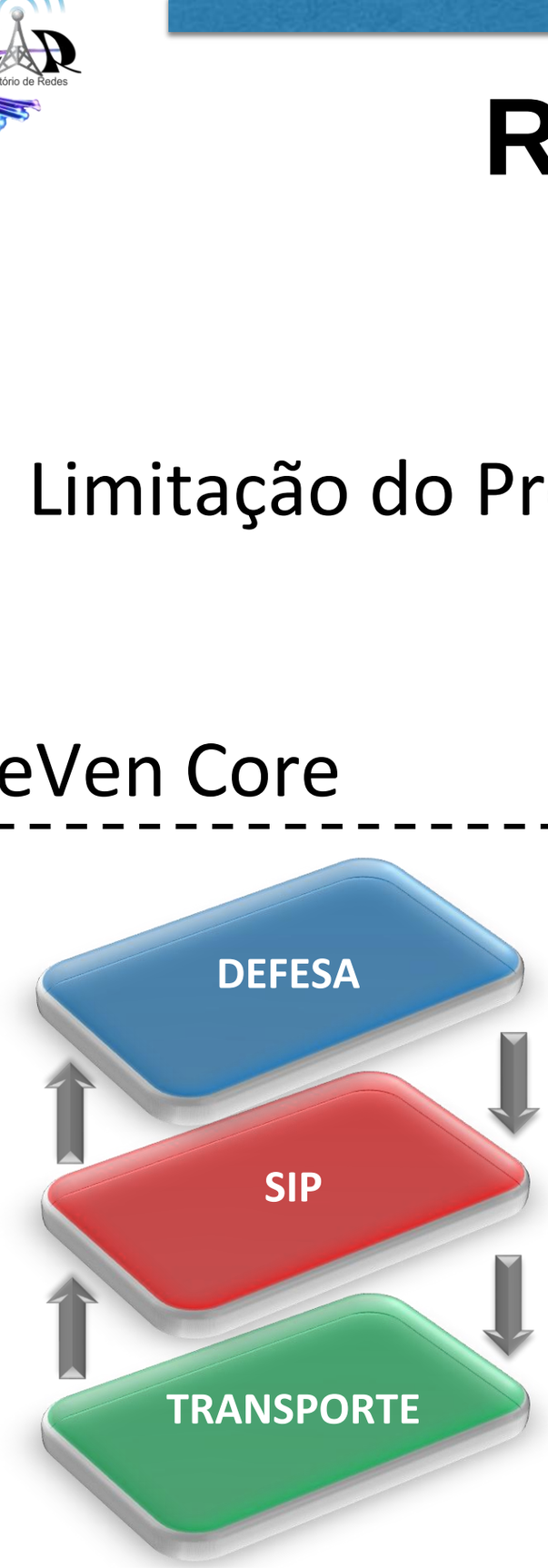


Depois do Ataque

Resultados com o SeVen

Limitação do Protótipo.

SeVen Core



Consulta o estado do servidor protegido e aplica a defesa

Processa as mensagens SIP de acordo com RFC3261

Envia/Recebe pacotes (UDP)

SeVen Shared Libraries

OpenSIPS MI JSON

OpenSIPS.so

Asterisk.so

Asterisk AMI HTTP

Resultados com o SeVen

Limitação do Protótipo.

Down!

OpenSIPS MI JSON

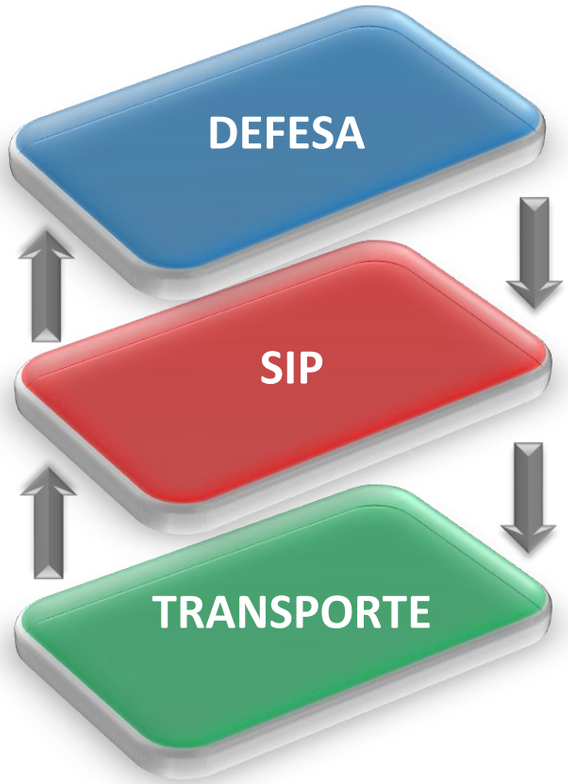
SeVen Shared Libraries

OpenSIPS.so

Asterisk.so

Asterisk AMI HTTP

SeVen Core



Consulta o estado do servidor protegido e aplica a defesa

Processa as mensagens SIP de acordo com RFC3261

Envia/Recebe pacotes (UDP)

Resultados com o SeVen

- Solução:
  - Desenvolver o piloto SeVen-VoIP como dois módulos:
    - SeVen OpenSIPS;
    - SeVen Asterisk;

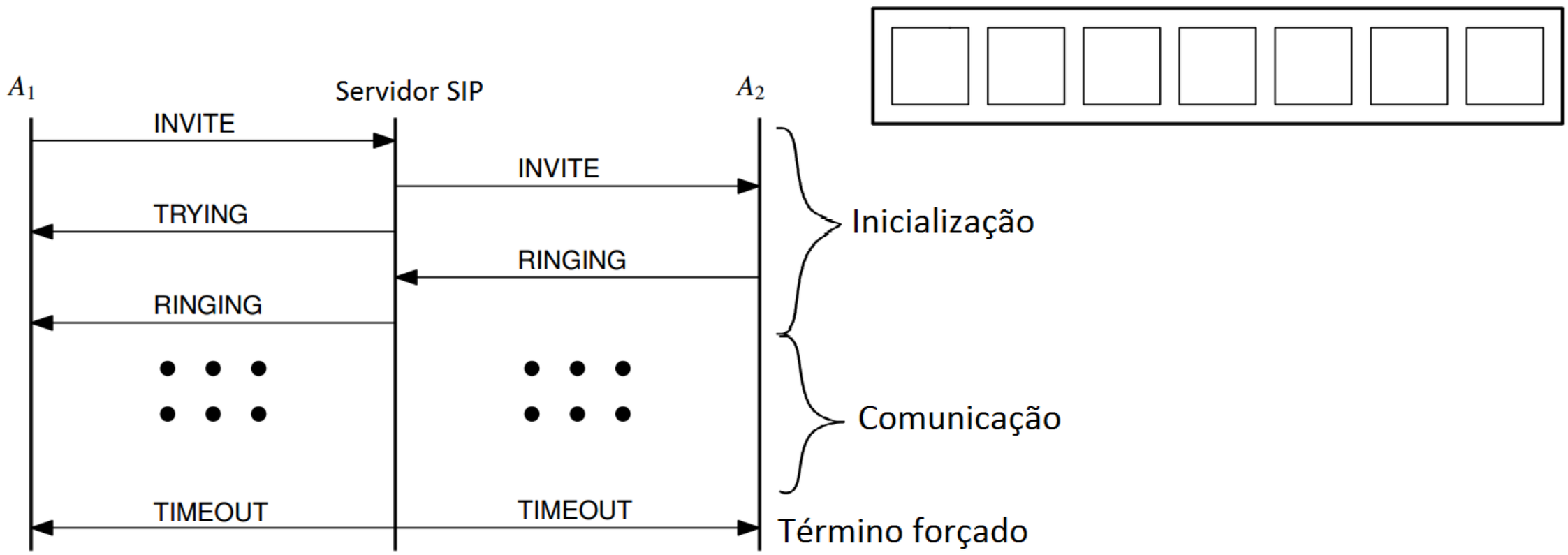
Vulnerabilidades do Asterisk

- Servidor de telecomunicações;
- IP PBX, Gateway VoIP, etc.

- **Vulnerável a ataques** *Telephony Denial of Service.*

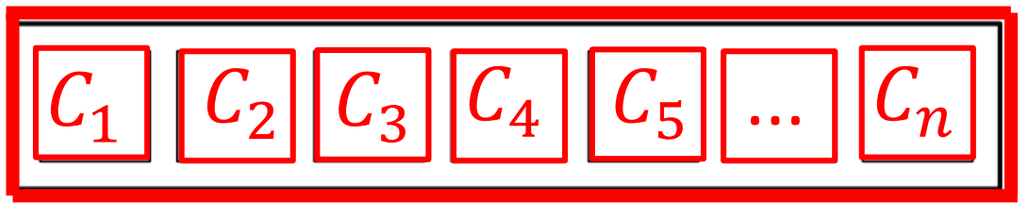
Telephony Denial of Service

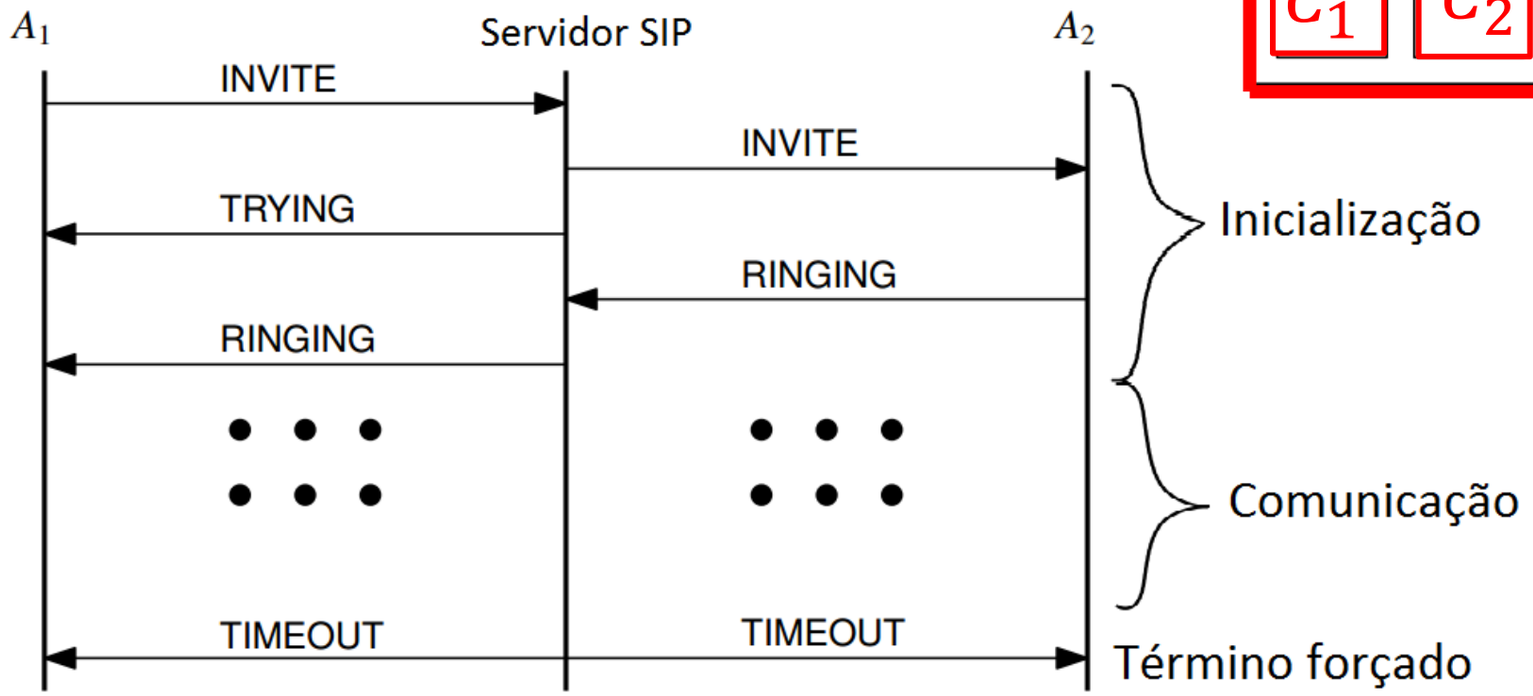
- Ocupar lentamente e continuamente todos os recursos alocados pelo Asterisk para manter uma chamada.



Telephony Denial of Service

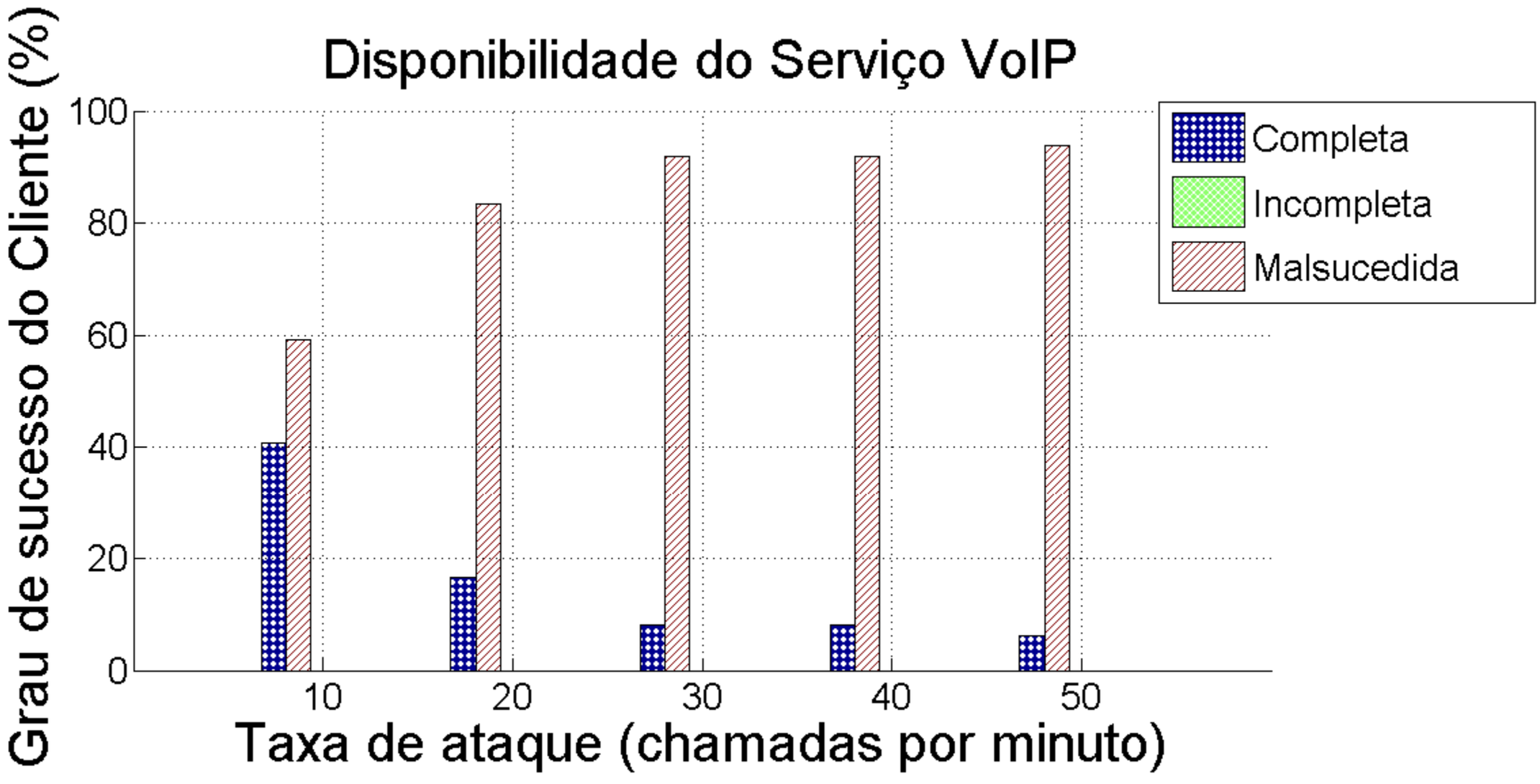
- Ocupar lentamente e continuamente todos os recursos alocados pelo Asterisk para manter uma chamada.





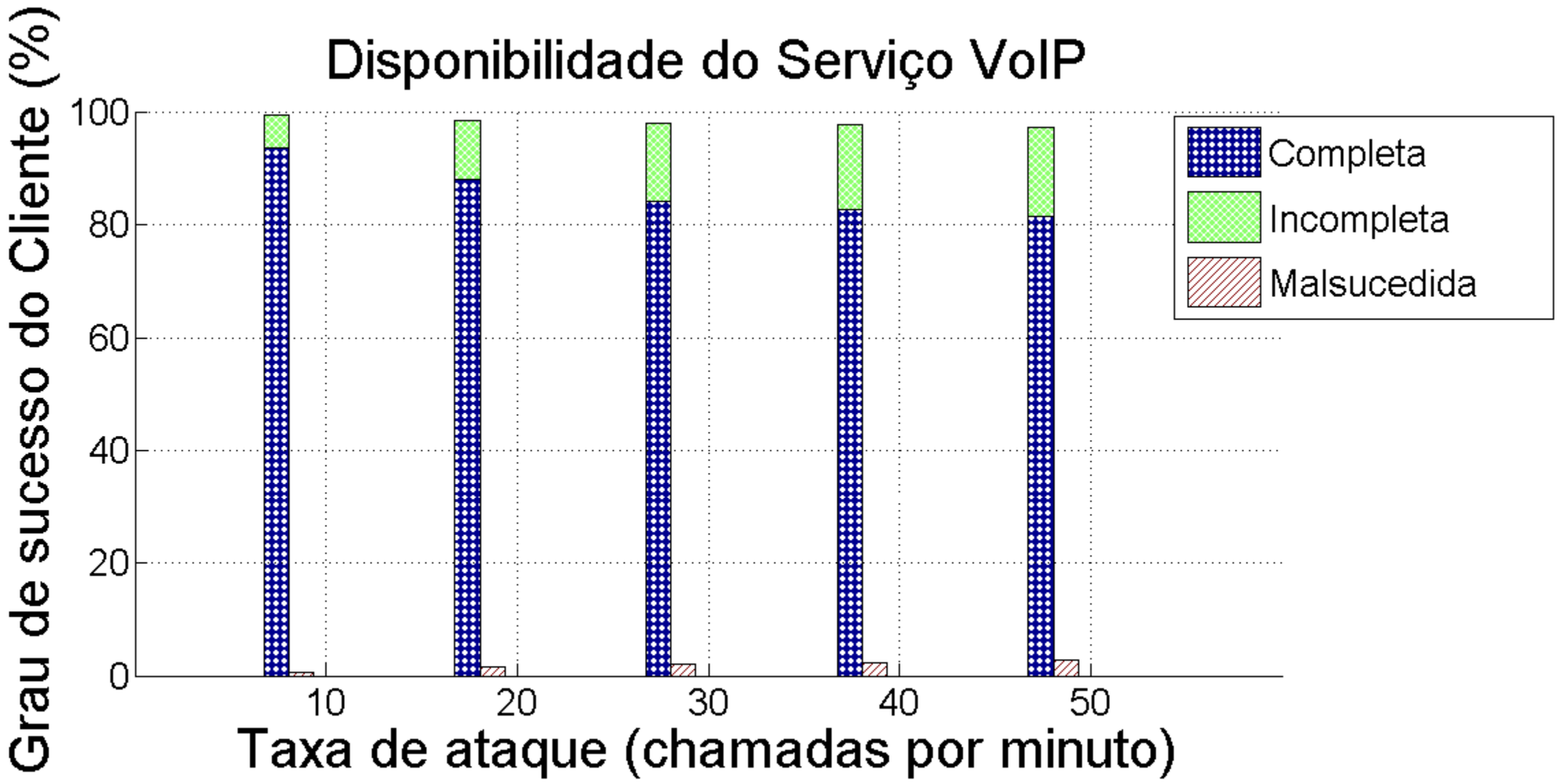
Experimentos na Rede do Lar

- Resultados sem SeVen:



Experimentos na Rede do Lar

- Resultados com SeVen:



Experimentos com o fone@RNP

- PBX-IP: Inutilizar o correio de Voz;
- Gateway Transparente.

Perguntas/comentários ?!