



SBRC
2016



A Selective Defense for Mitigating Coordinated Call Attacks

**Marcilio O. O. Lemos¹, Yuri Gil Dantas², Iguatemi E. Fonseca¹,
Vivek Nigam¹ and Gustavo Sampaio¹**

¹Federal University of Paraíba (UFPB) – Brazil

²Technische Universität Darmstadt - Germany

DDoS e VoIP

Massive DDoS attacks a growing threat to VoIP services

TelePacific Communications tells of VoIP floods



By [Ellen Messmer](#) | [Follow](#)

Network World | Oct 4, 2011 11:33 AM PT

 TECH & GADGETS

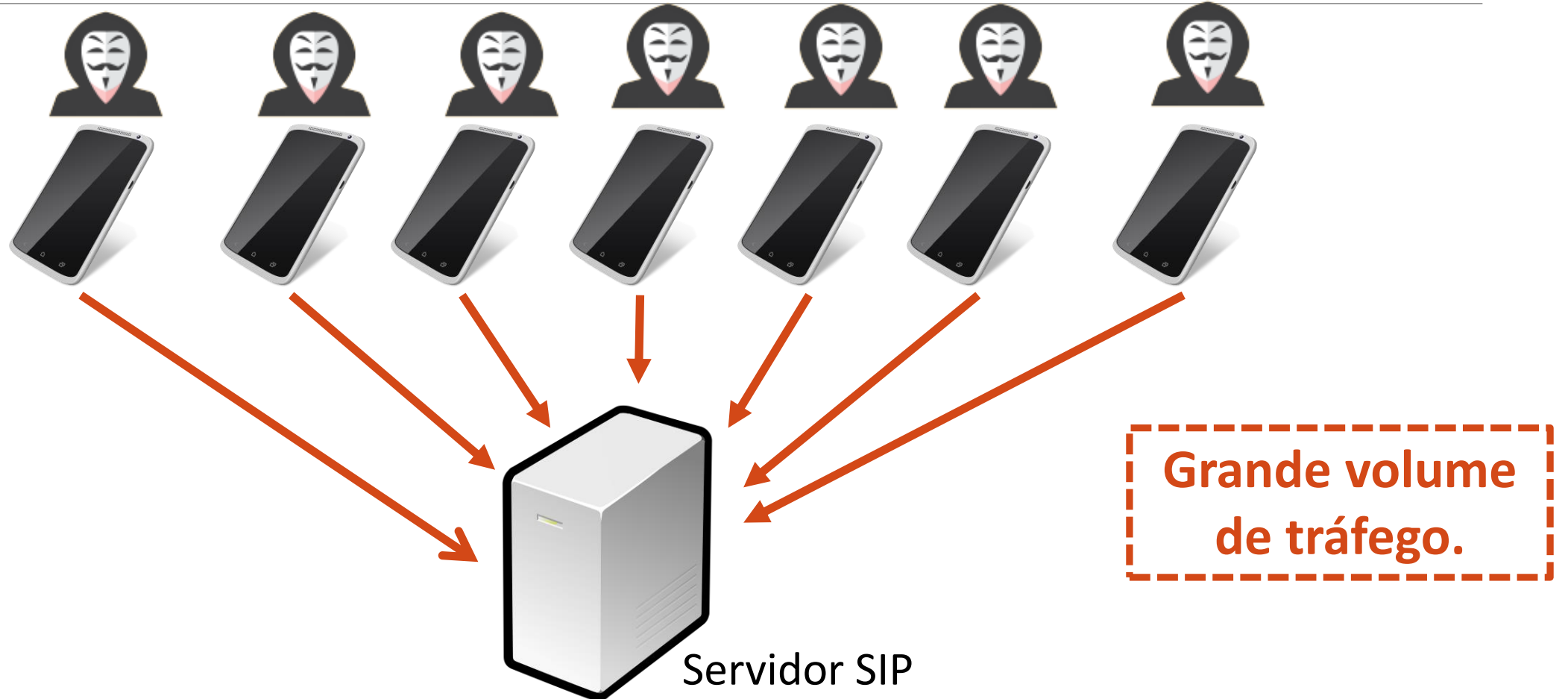


DDoS Hacker Attacks Draw Attention To VoIP (In)Security

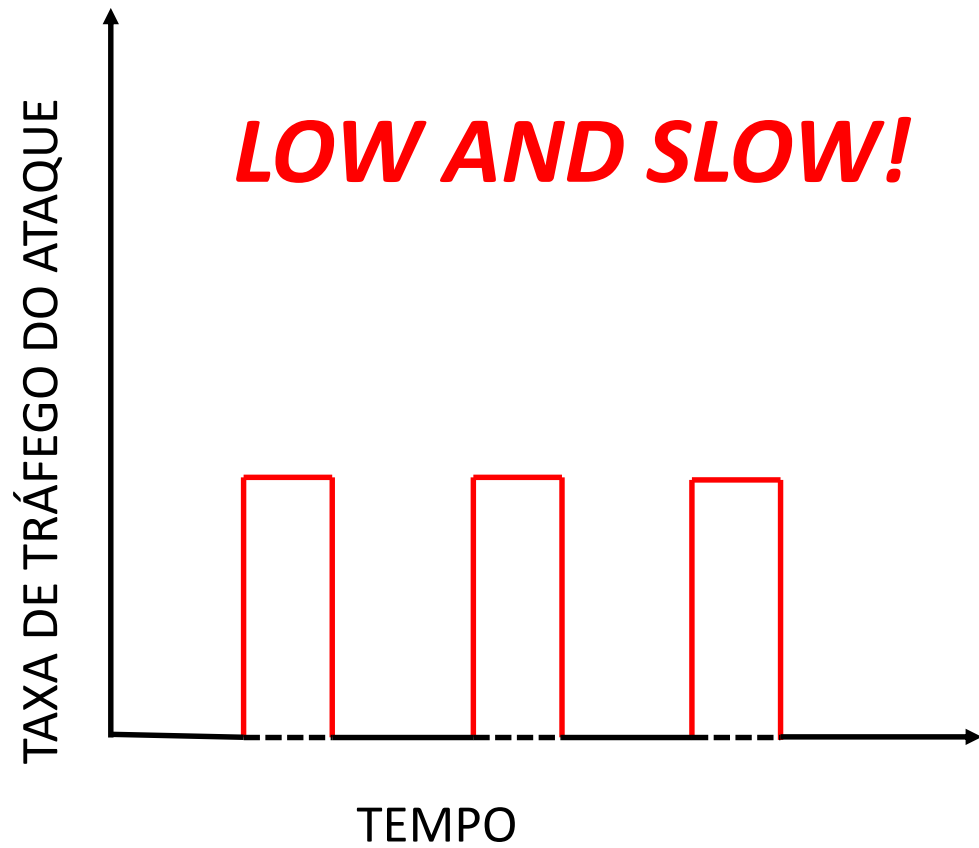
by [Iain Pemberton](#) July 30, 2013

[Follow @Avaya](#)

DDoS no VoIP



Low-rate DDoS



Low-rate DDoS



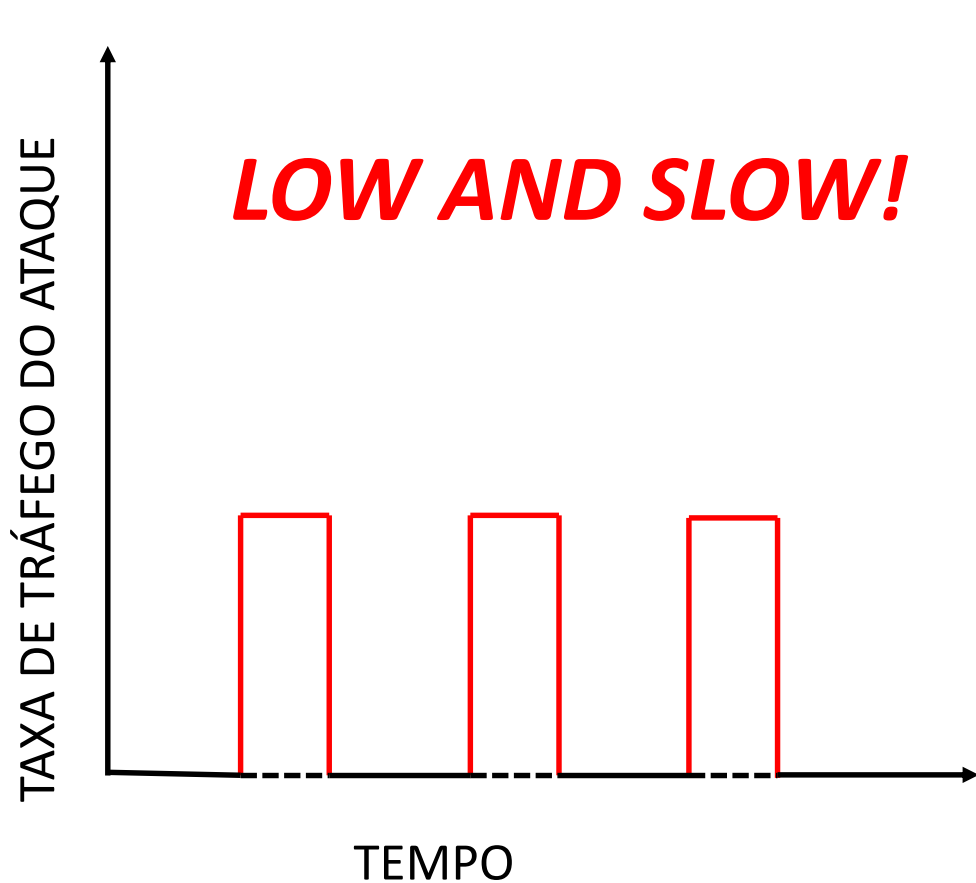
HTTP

Slow Read

Rudy

Slowloris

Low-rate DDoS



HTTP

Slow Read

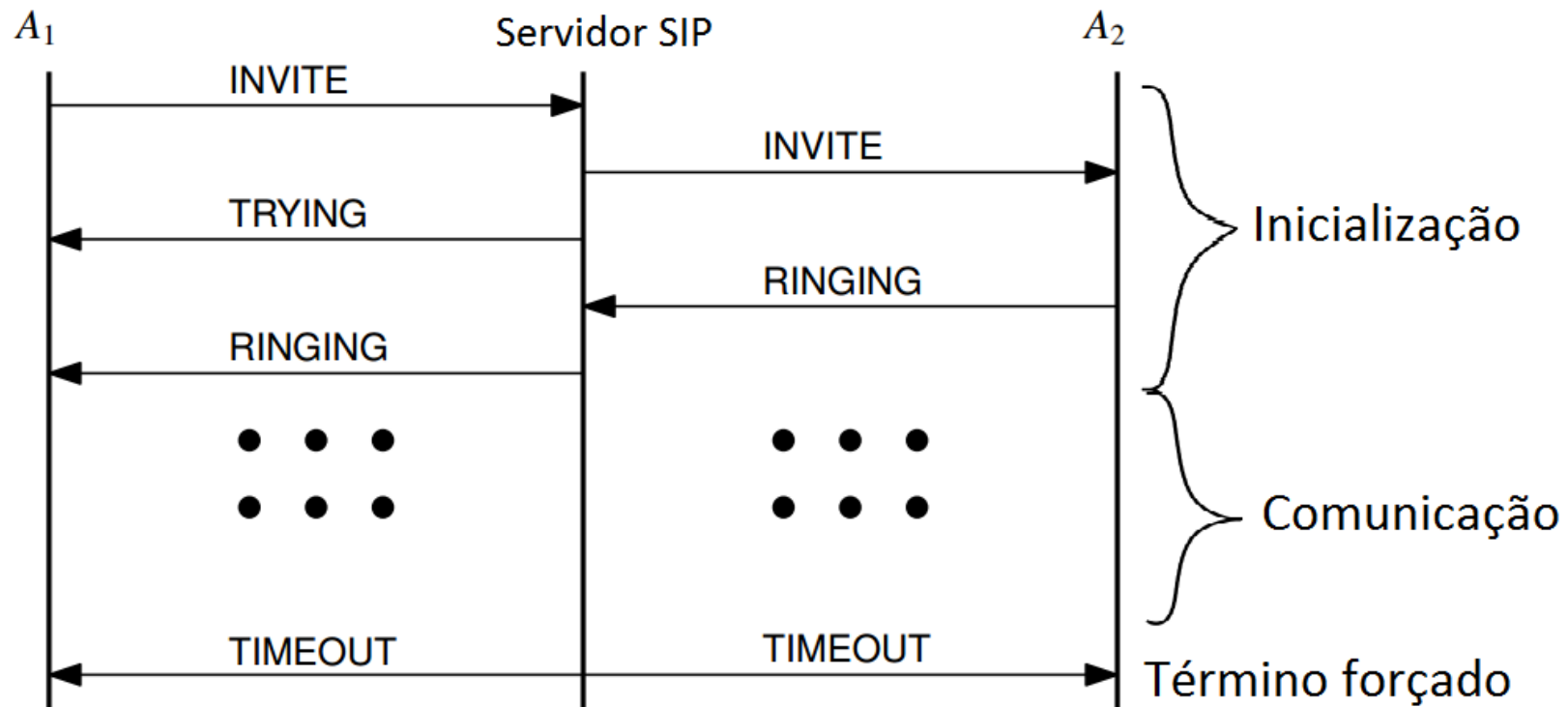
Rudy

Slowloris

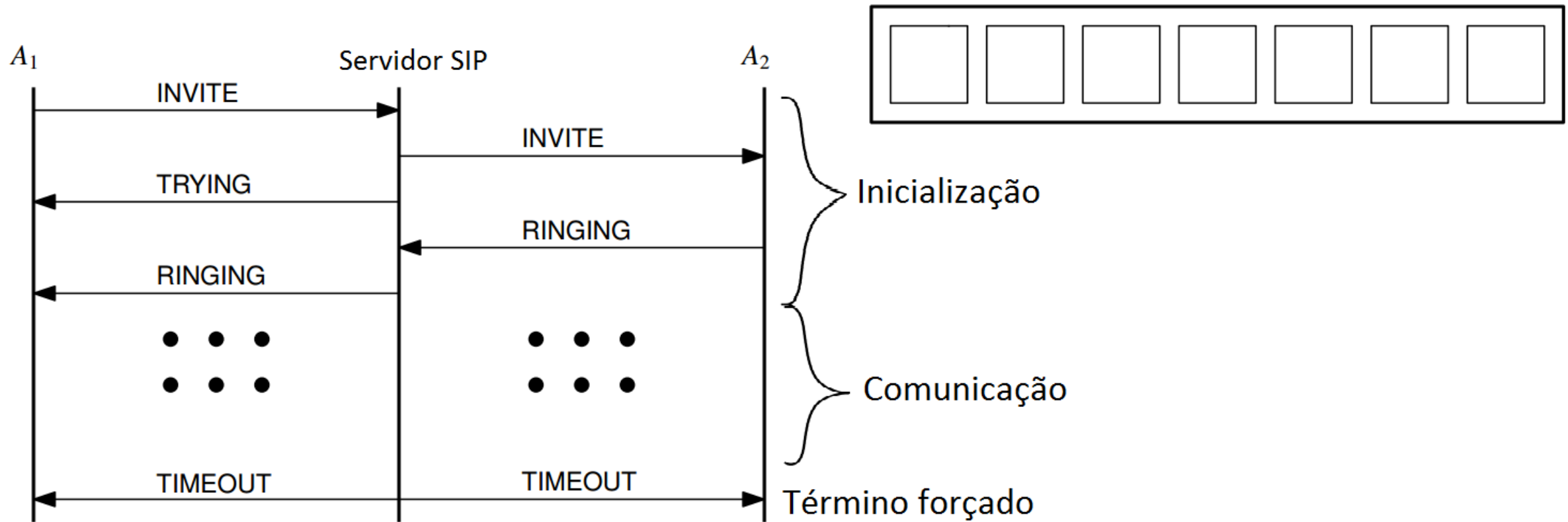
VoIP

Coordinated Call Attack

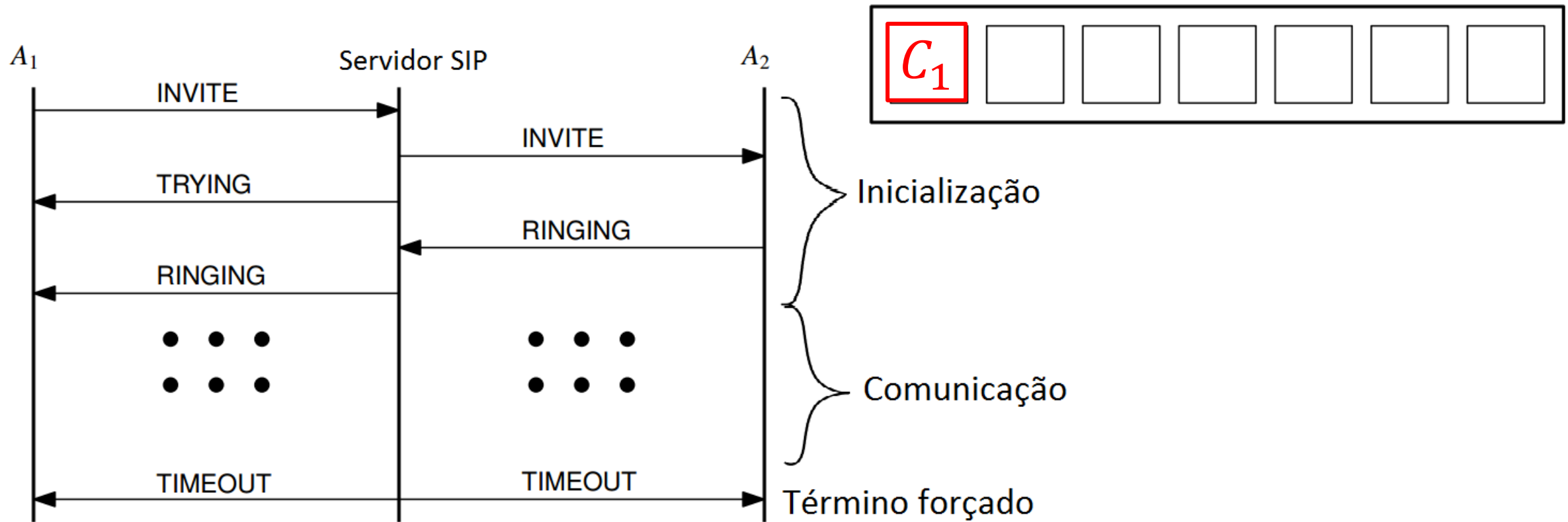
Coordinated Call Attack



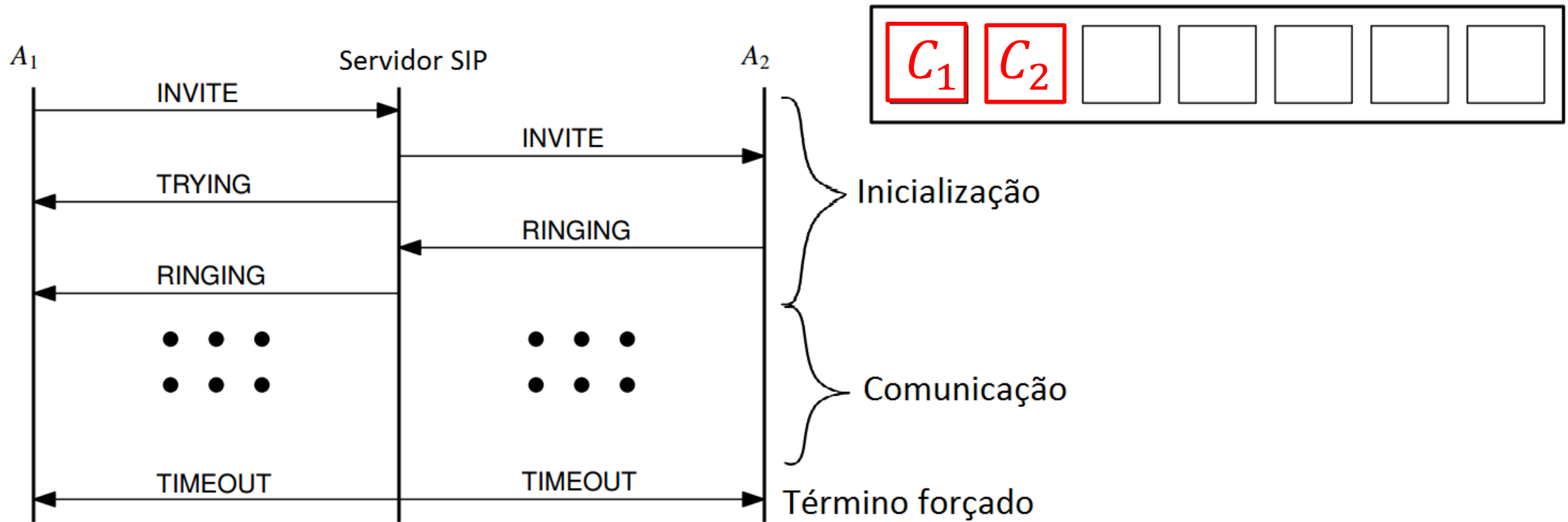
Coordinated Call Attack



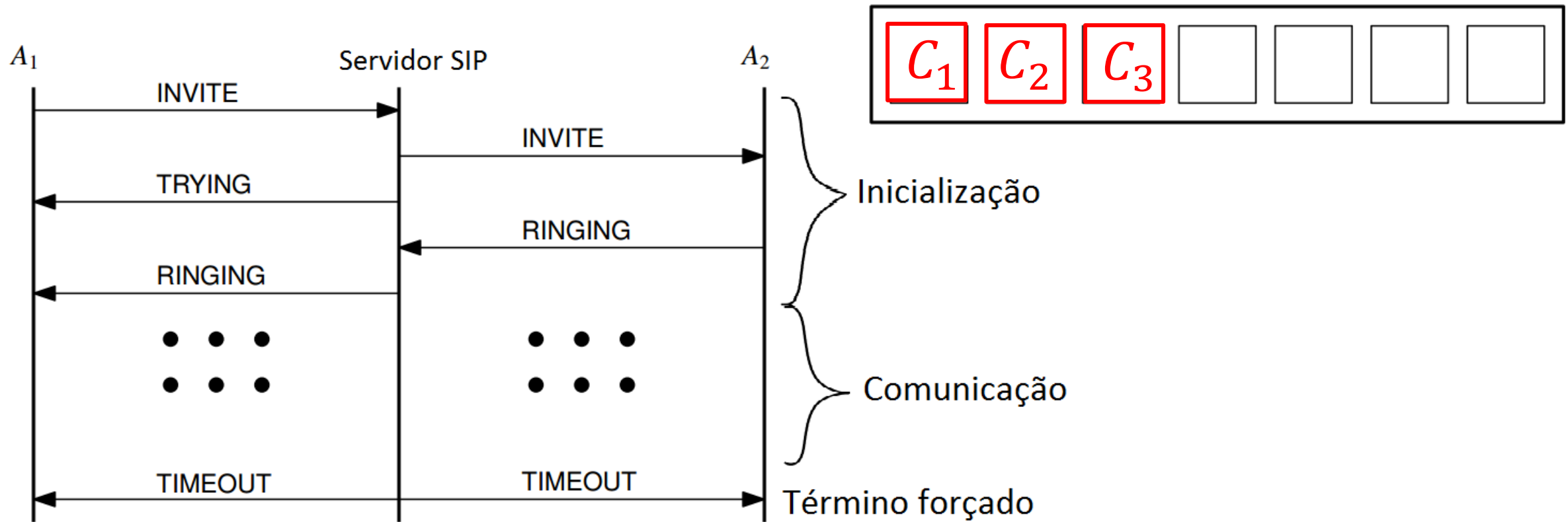
Coordinated Call Attack



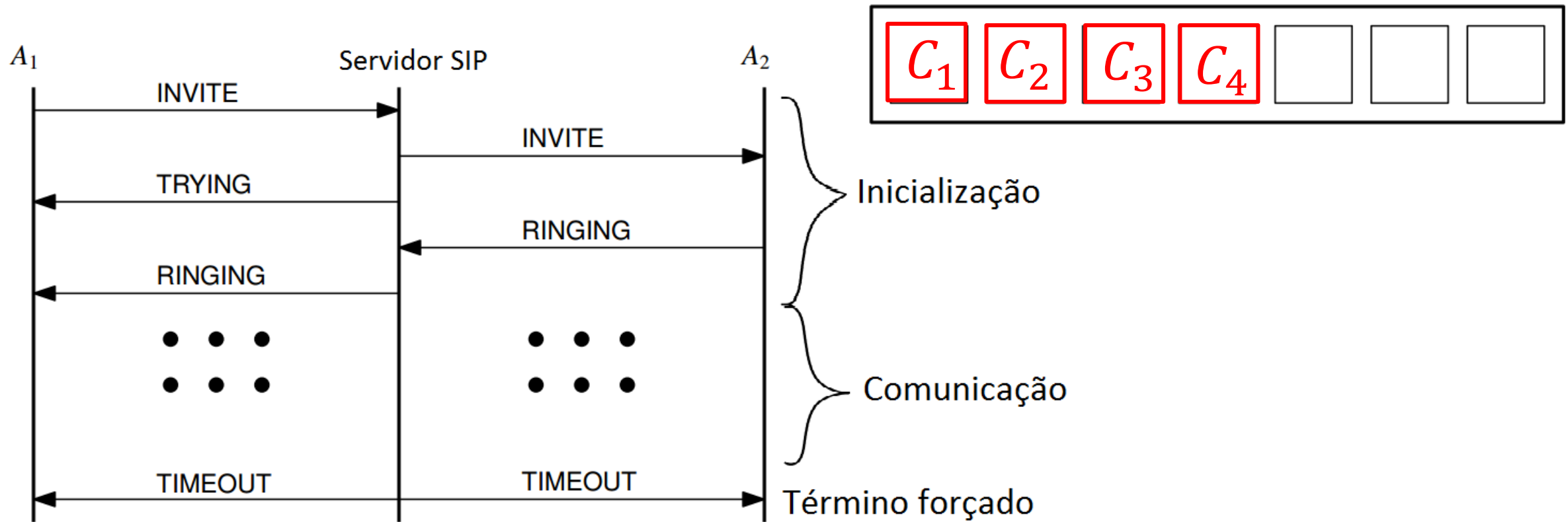
Coordinated Call Attack



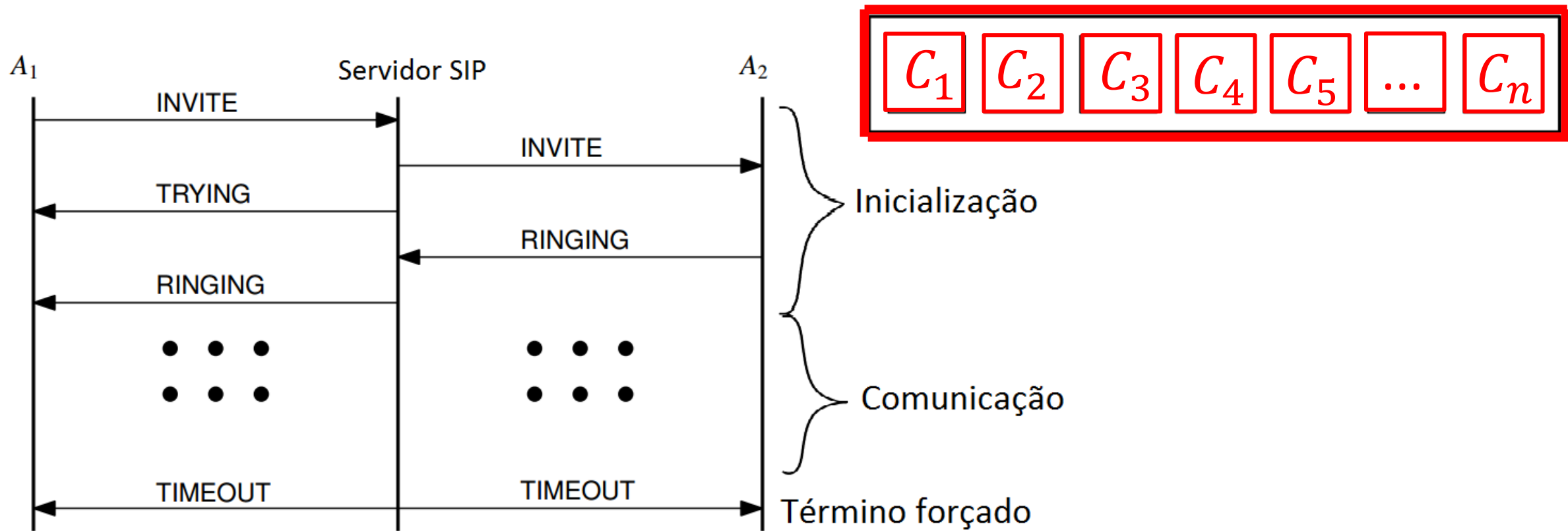
Coordinated Call Attack



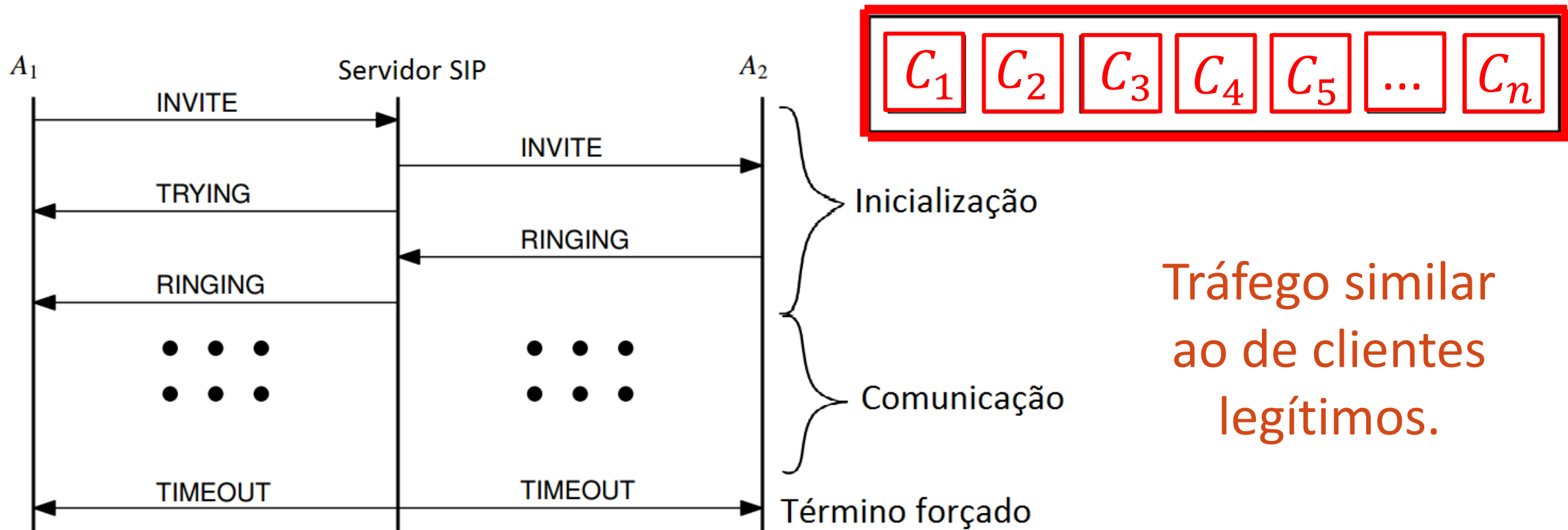
Coordinated Call Attack



Coordinated Call Attack



Coordinated Call Attack



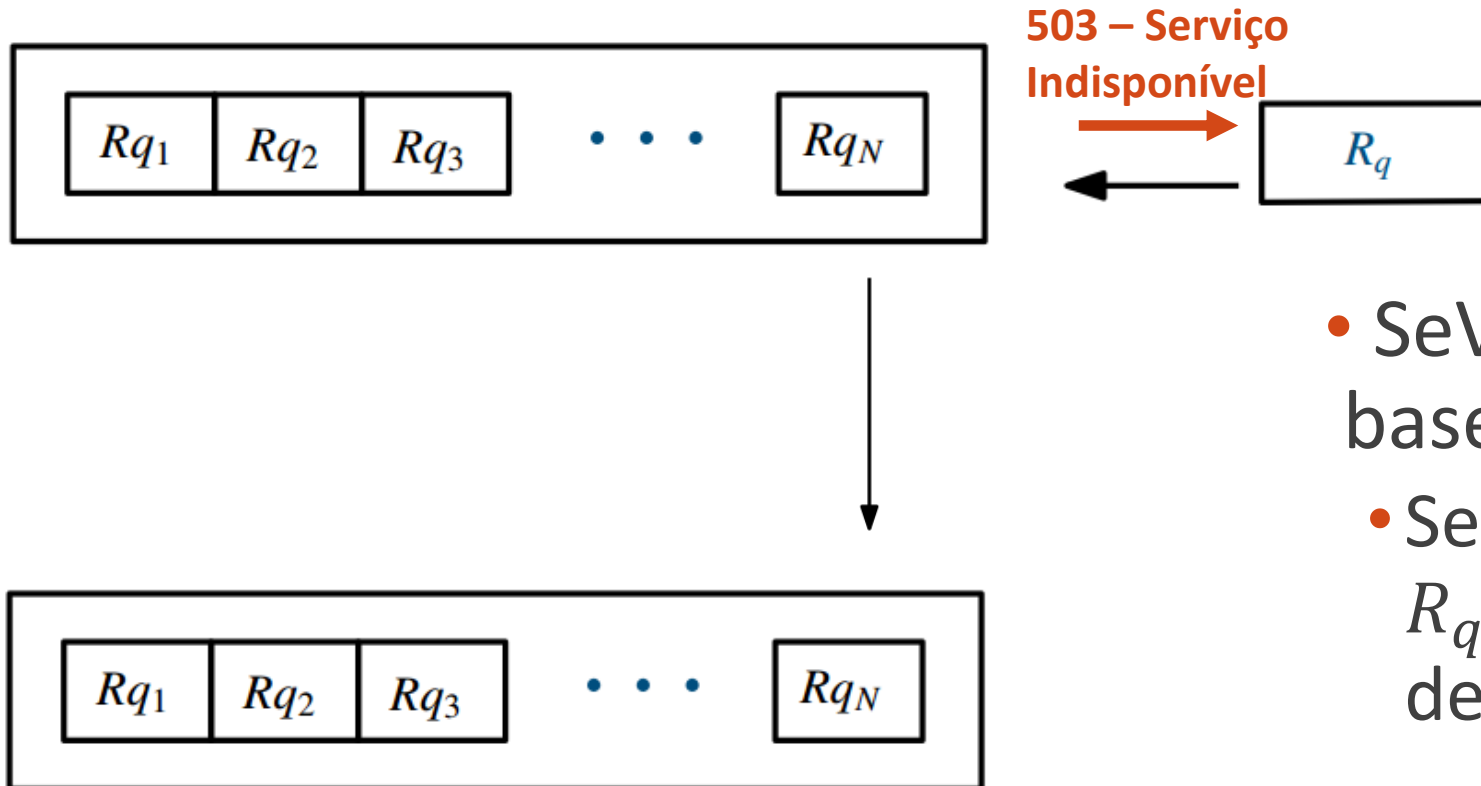
Tráfego similar
ao de clientes
legítimos.

SeVen

- Ferramenta de Defesa que faz uso de estratégias seletivas para mitigar DDoS Low-rate (HTTP);
- **Objetivo: Propor uma estratégia seletiva apropriada para o VoIP (SIP).**

Algoritmo

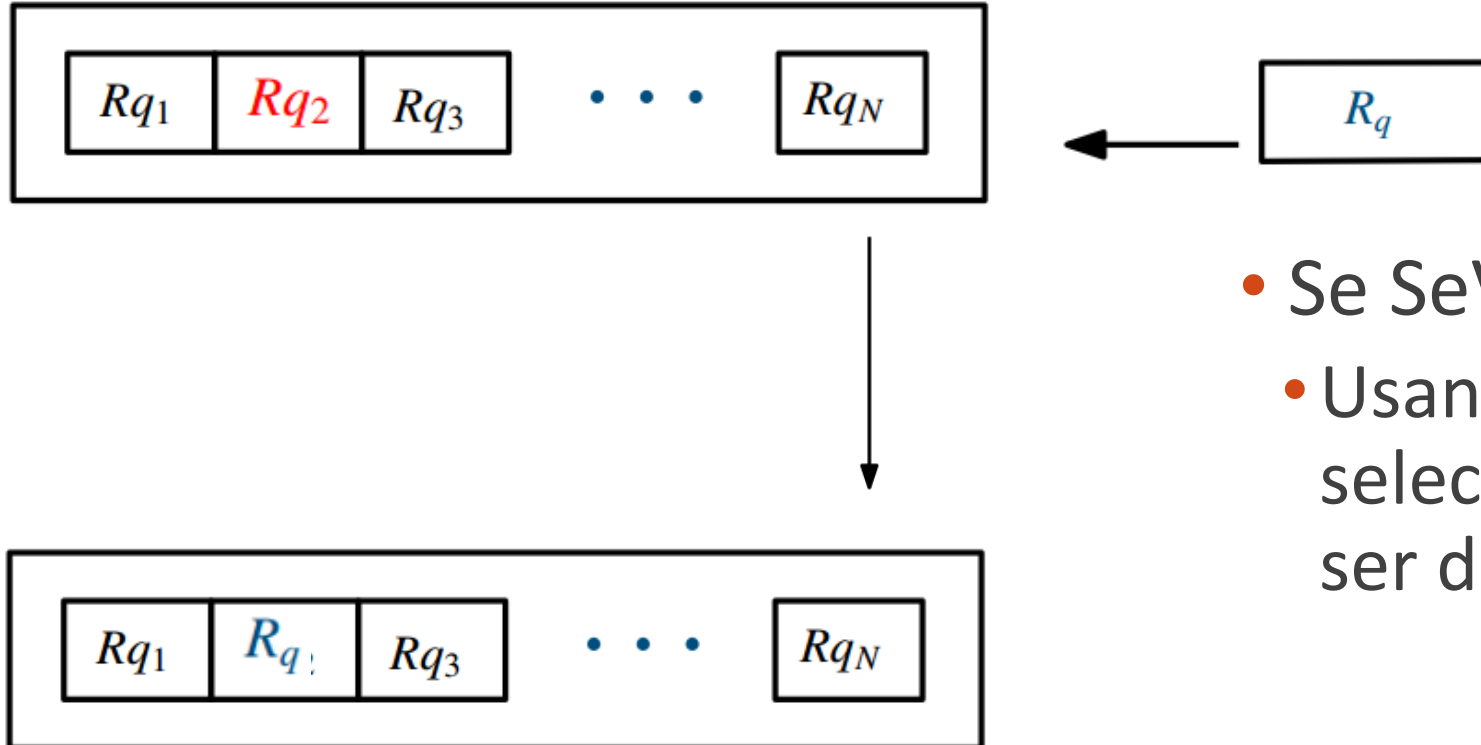
- Servidor sobrecarregada e nova requisição R_q :



- SeVen toma uma decisão com base na probabilidade P_1 :
- Se SeVen decidir não processar R_q ela simplesmente é descartada.

Algoritmo

- Servidor sobrecarregada e nova requisição R_q :

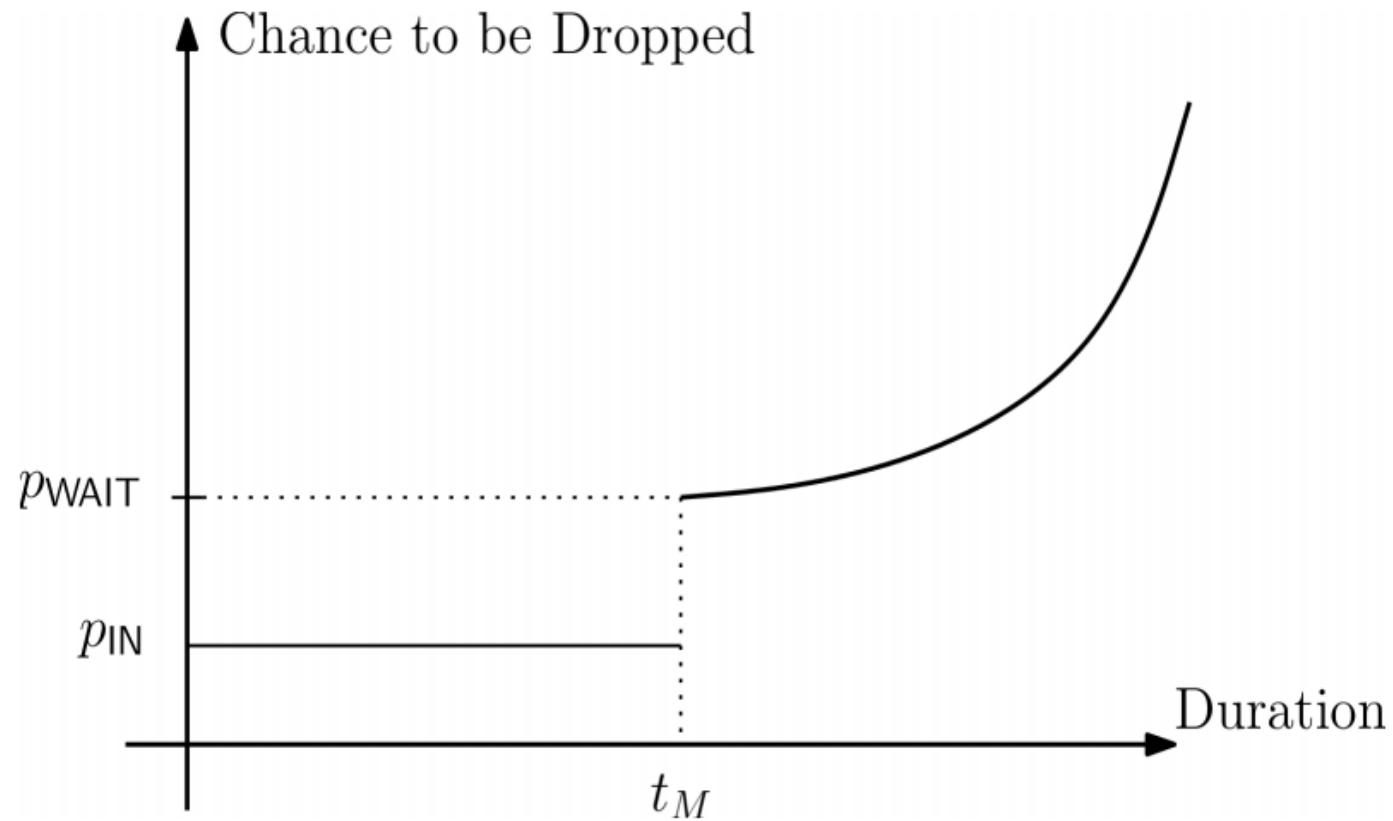


- Se SeVen decide processar R_q :
- Usando a probabilidade P_2 , ele seleciona uma requisição para ser descartada

SeVen – Cenário VoIP

- Assumindo que a duração média t_M das chamadas é conhecida:
 - Consideramos três casos:
 - Chamadas WAITING;
 - Chamadas INCALL com $t < t_M$;
 - Chamadas INCALL com $t \geq t_M$;

Comportamento do SeVen



Exemplo de Execução

$\mathcal{P}_0 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle]$

$Max = 3$

$t_M = 5$

Exemplo de Execução

$\mathcal{P}_0 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle]$

$m_1 = \langle id_3, INVITE \rangle$

$Max = 3$

$t_M = 5$

Exemplo de Execução

$$\mathcal{P}_0 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle]$$

$$m_1 = \langle id_3, INVITE \rangle$$

$$\mathcal{P}_1 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle, \langle id_3, WAITING, 0 \rangle]$$

$$Max = 3$$

$$t_M = 5$$

Exemplo de Execução

$$\mathcal{P}_0 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle]$$

$$m_1 = \langle id_3, INVITE \rangle$$

$$\mathcal{P}_1 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle, \langle id_3, WAITING, 0 \rangle]$$

$$m_2 = \langle id_2, ACK \rangle$$

$$Max = 3$$

$$t_M = 5$$

Exemplo de Execução

$$\mathcal{P}_0 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle]$$

$$m_1 = \langle id_3, INVITE \rangle$$

$$\mathcal{P}_1 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle, \langle id_3, WAITING, 0 \rangle]$$

$$m_2 = \langle id_2, ACK \rangle$$

$$\mathcal{P}_2 = [\langle id_1, INCALL, 9 \rangle, \langle id_2, INCALL, 1 \rangle, \langle id_3, WAITING, 0 \rangle]$$

$$Max = 3$$

$$t_M = 5$$

Exemplo de Execução

$$\mathcal{P}_0 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle]$$

$$m_1 = \langle id_3, INVITE \rangle$$

$$\mathcal{P}_1 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle, \langle id_3, WAITING, 0 \rangle]$$

$$m_2 = \langle id_2, ACK \rangle$$

$$\mathcal{P}_2 = [\langle id_1, INCALL, 9 \rangle, \langle id_2, INCALL, 1 \rangle, \langle id_3, WAITING, 0 \rangle]$$

$$m_3 = \langle id_4, INVITE \rangle$$

$$Max = 3$$

$$t_M = 5$$

Exemplo de Execução

$$\mathcal{P}_0 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle]$$

$$m_1 = \langle id_3, INVITE \rangle$$

$$\mathcal{P}_1 = [\langle id_1, INCALL, 8 \rangle, \langle id_2, WAITING, 0 \rangle, \langle id_3, WAITING, 0 \rangle]$$

$$m_2 = \langle id_2, ACK \rangle$$

$$\mathcal{P}_2 = [\langle id_1, INCALL, 9 \rangle, \langle id_2, INCALL, 1 \rangle, \langle id_3, WAITING, 0 \rangle]$$

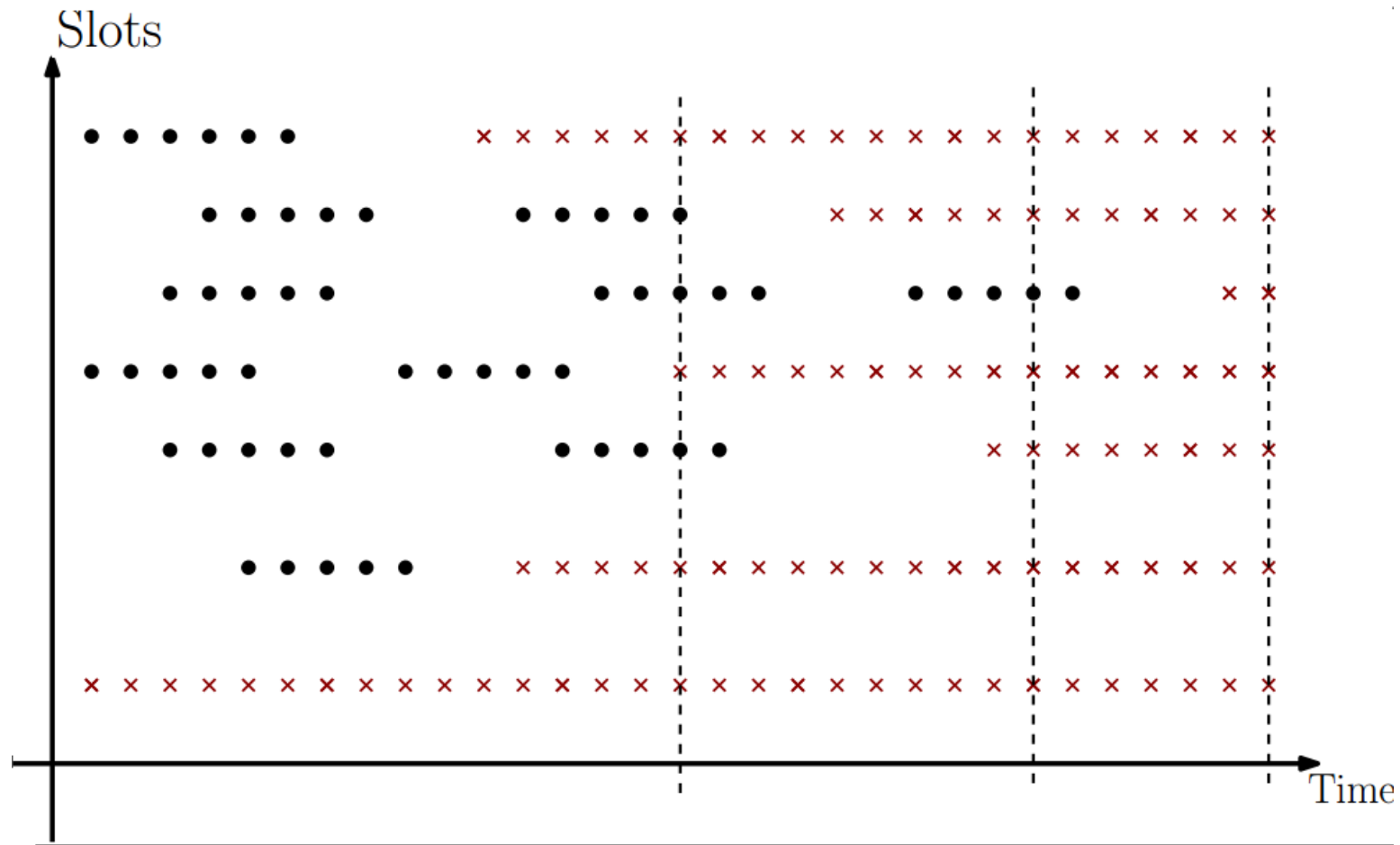
$$m_3 = \langle id_4, INVITE \rangle$$

$$\mathcal{P}_3 = [\langle id_2, INCALL, 1 \rangle, \langle id_3, WAITING, 0 \rangle, \langle id_4, WAITING, 0 \rangle]$$

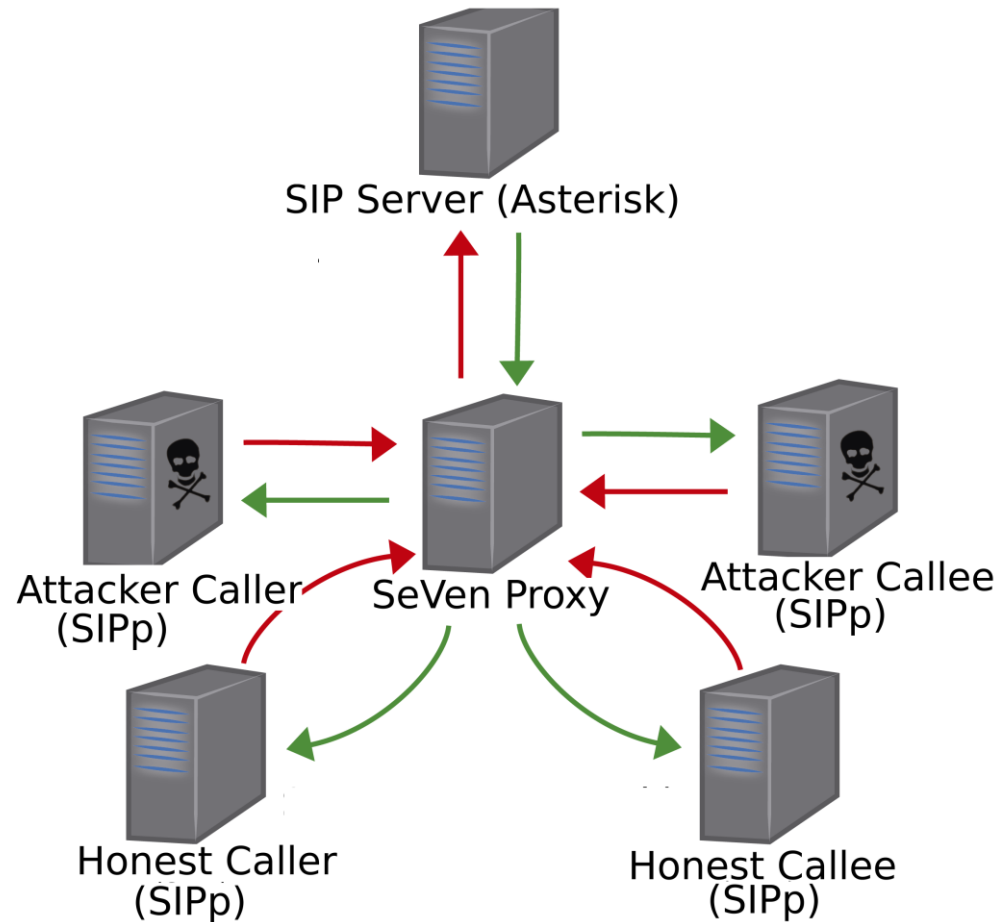
$$Max = 3$$

$$t_M = 5$$

Intuição



Topologia dos Experimentos



Parâmetros dos Experimentos

- $t_M = 5$ minutos;
- Capacidade do servidor: 50 chamadas simultâneas;
- Duração das chamadas dos clientes: uniforme $(0, 2 \times t_M]$;
- Duração das chamadas dos atacantes: indefinido;
- Tempo total de cada experimento: 60 minutos;
- Taxa de Tráfego: 9,9 chamadas por minuto.

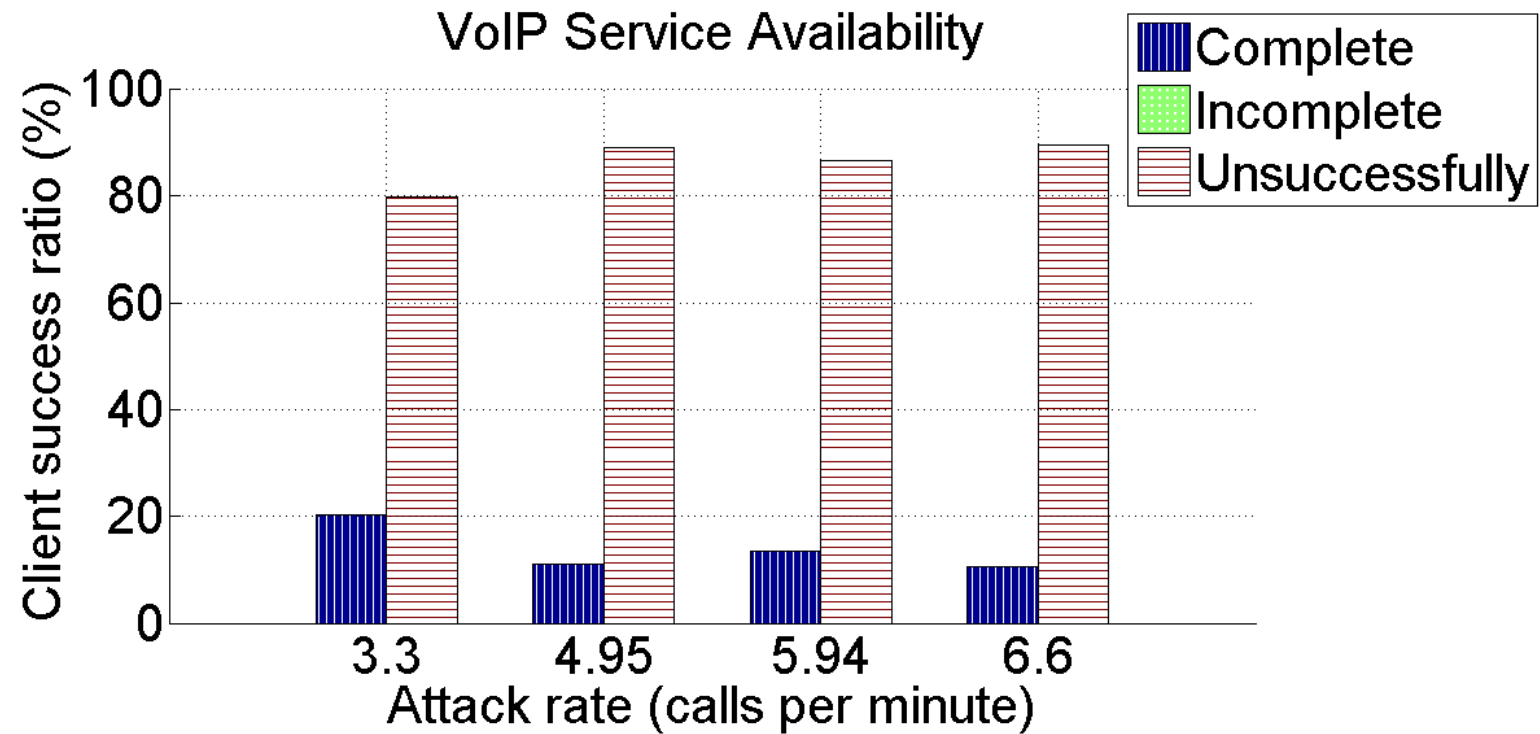
Métricas de Qualidade

- Chamadas Completadas;
- Chamadas Incompletas;
- Chamadas Malsucedidas.

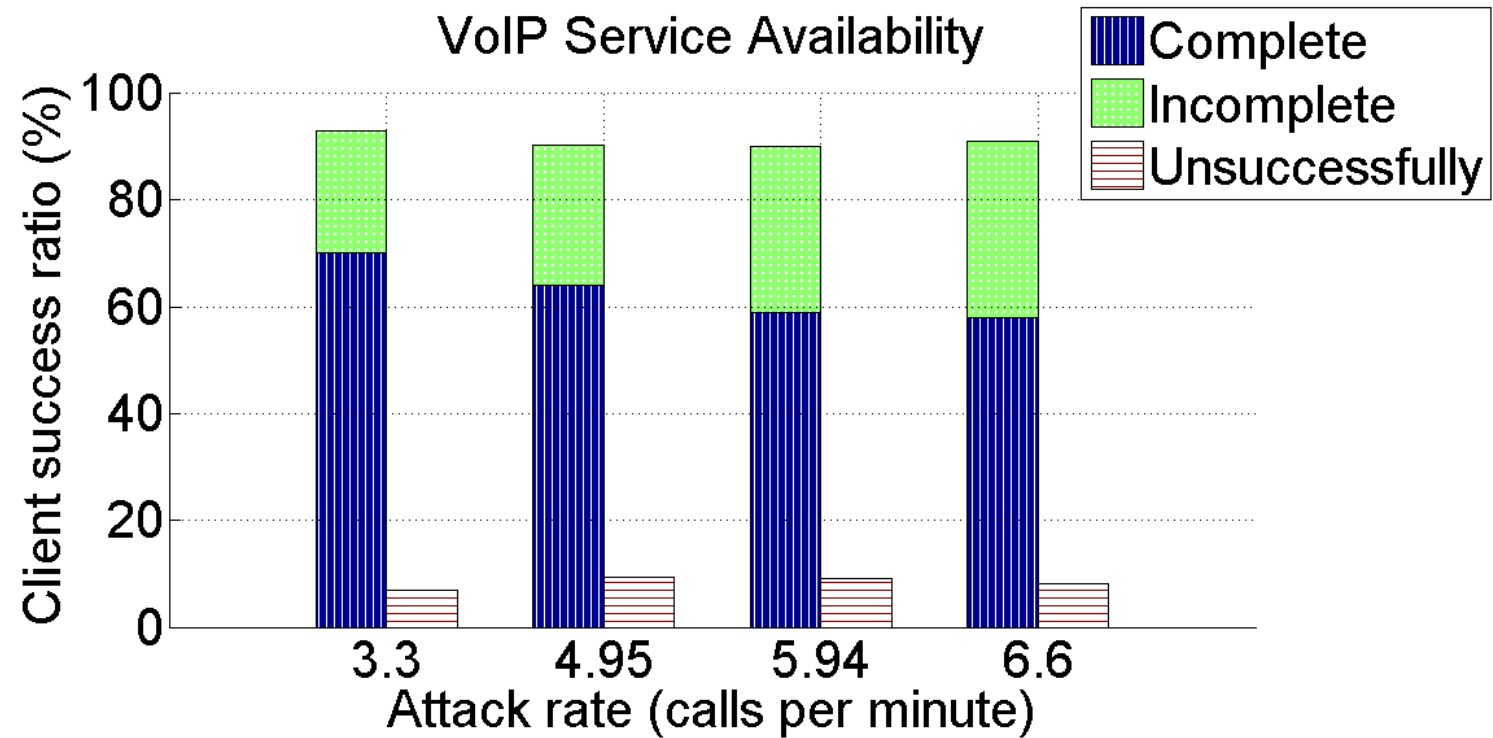
Cenários de Teste

- Com ataque e sem SeVen;
- Com ataque e com SeVen;
- Sem ataque e sem SeVen.

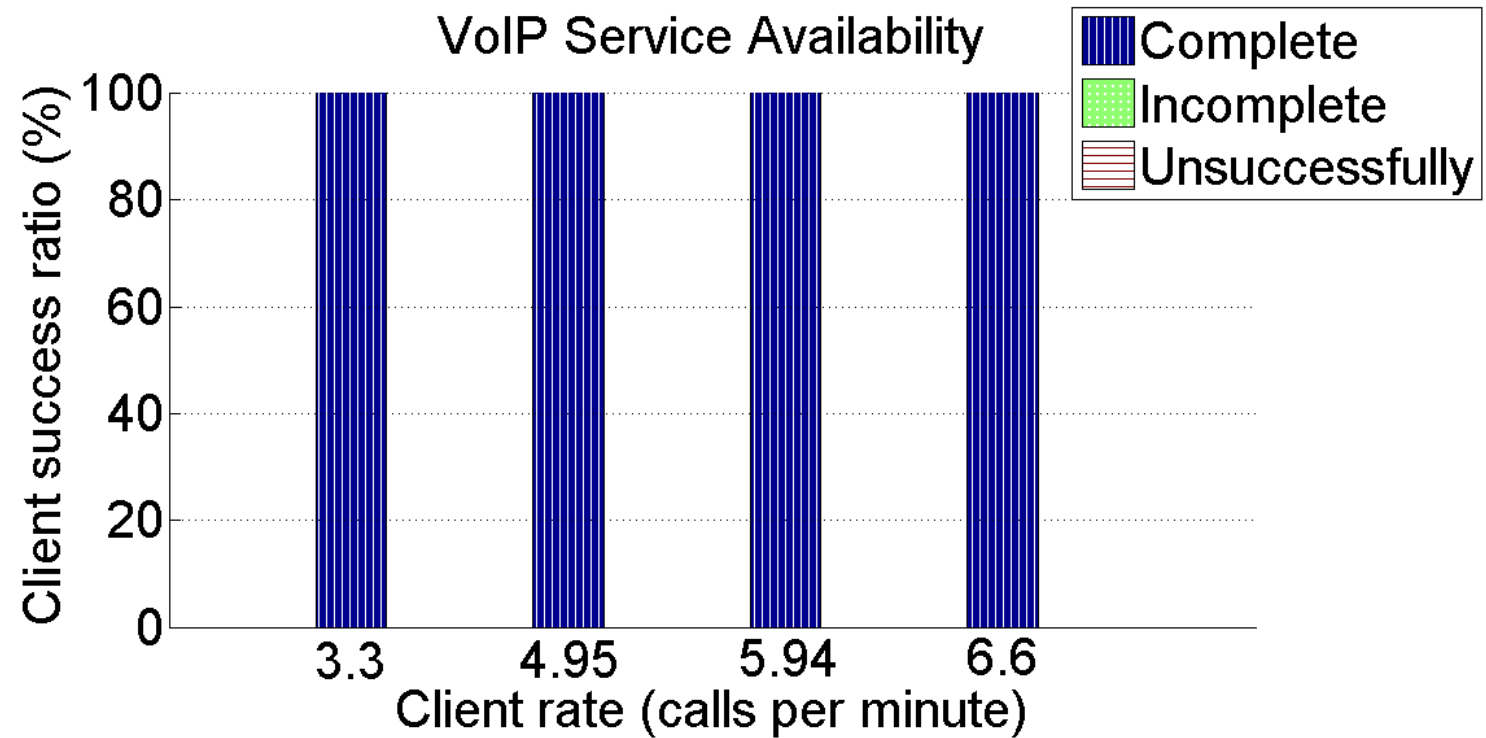
Resultados sem o SeVen



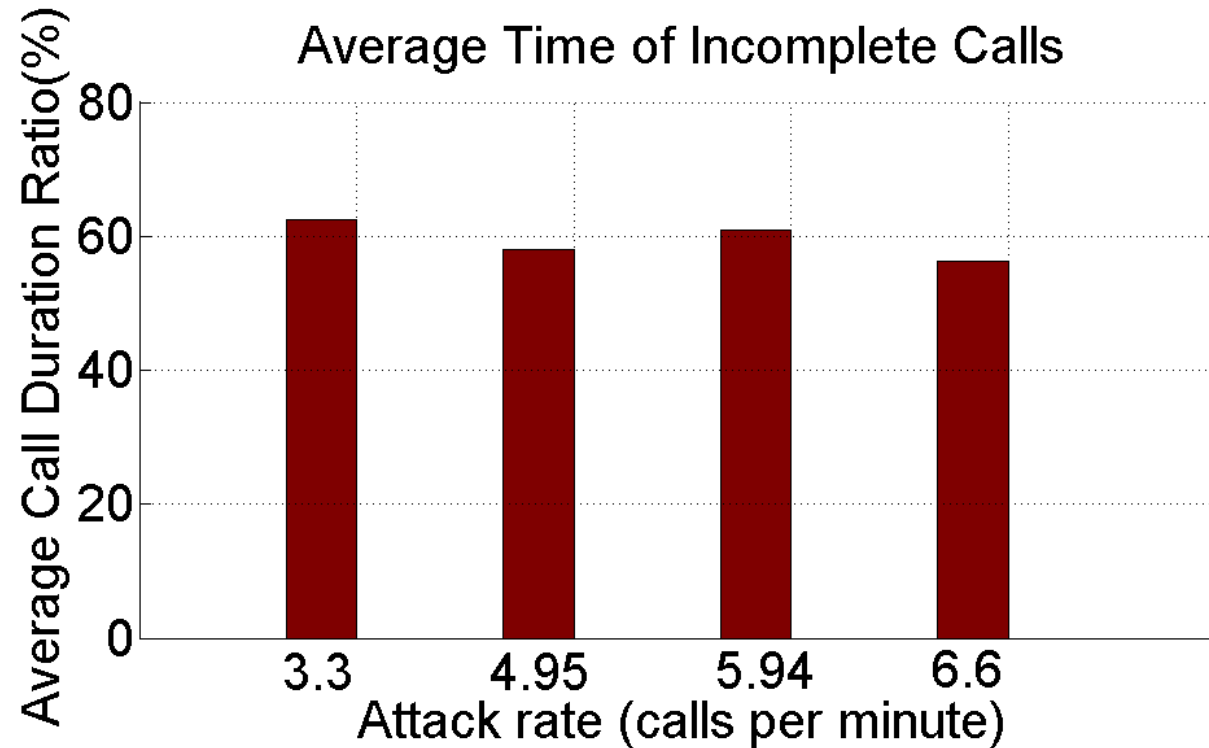
Resultados com o SeVen



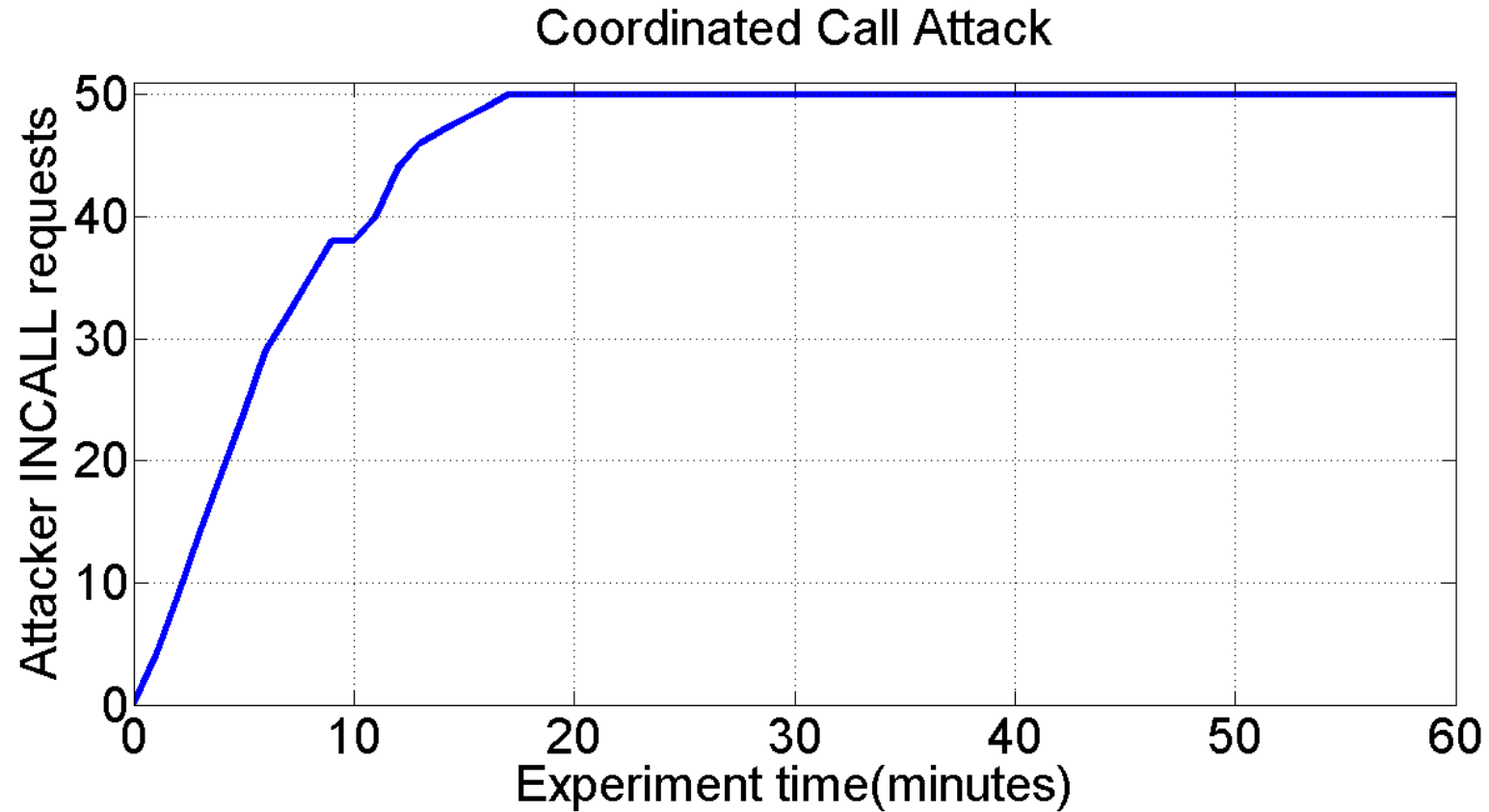
Resultados com SeVen e Sem Ataque



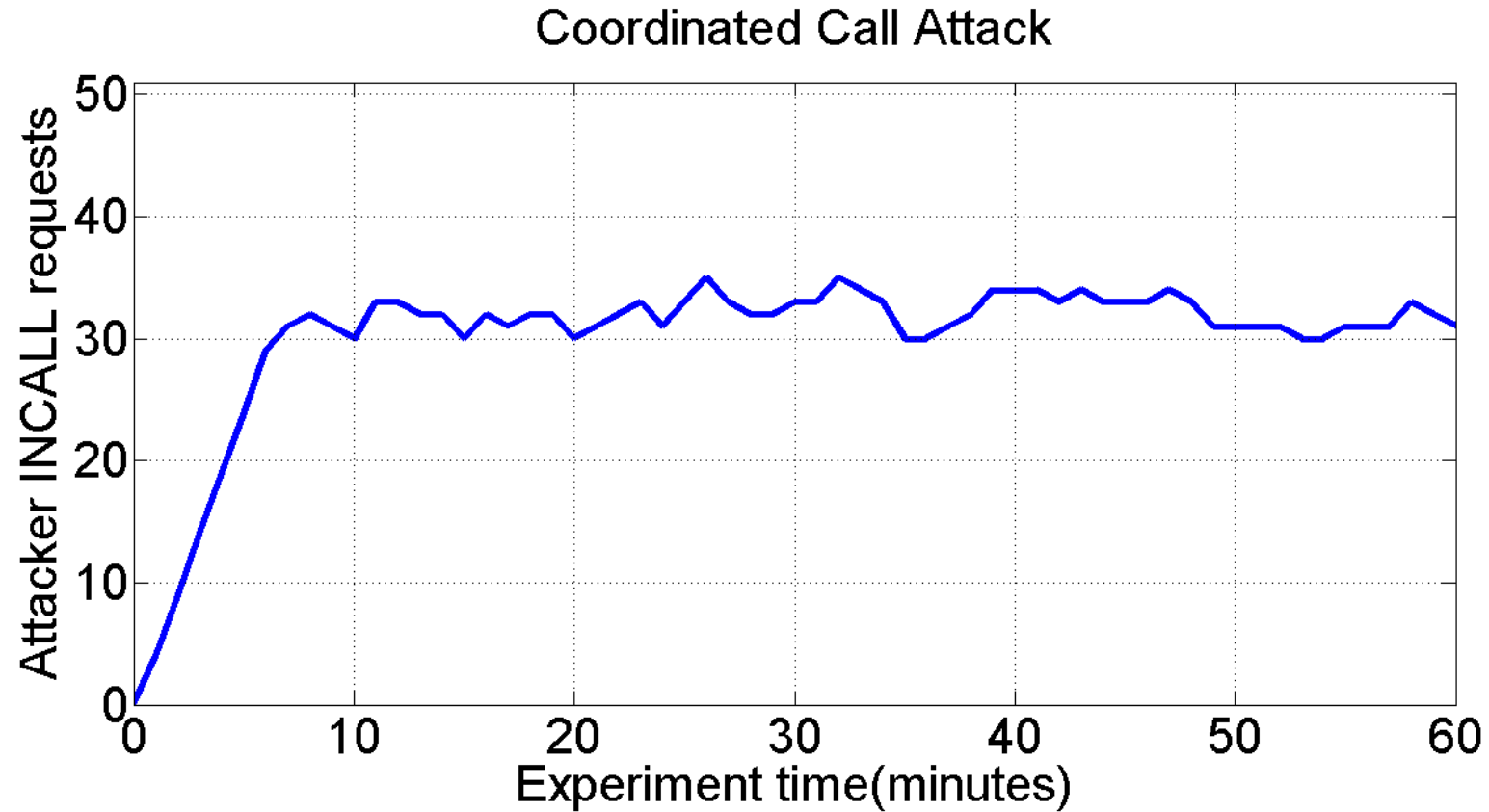
Tempo de duração média das chamadas Incompletas



Ocupação dos Atacantes sem o SeVen



Ocupação dos Atacantes com o SeVen



Conclusão e Trabalhos Futuros

- Estratégia seletiva adequada para mitigar o *Coordinated Call Attack*:
 - Sem SeVen: disponibilidade entre 10 e 20%;
 - Com SeVen: 90% dos clientes conseguiram se comunicar, sendo que 60%~80% deles completaram a chamada.

- Trabalhos futuros:
 - Investigar outros ataques ao VoIP (eg. *Dial Attack*) ;

Referências

- Massive DDoS attacks a growing threat to VoIP services.
<http://www.networkworld.com/article/2181743/voip/massive-ddosattacks-a-growing-threat-to-voip-services.html>
- DDoS Hacker Attacks Draw Attention To VoIP (In)Security
<http://www.business2community.com/tech-gadgets/ddos-hacker-attacks-draw-attention-to-voip-insecurity>
- A Selective Defense for Application Layer DDoS Attacks, 2014. Yuri Gil Dantas, Vivek Nigam, Iguatemi E. Fonseca. JISIC 2014:75-82.

That's all Folks!

Perguntas!?

Comportamento do SeVen

- Equações:

$$r \leq \frac{N_T}{N_T + \text{Factor}}; \quad (1)$$

$$r \in [0, 1]$$

$$d(t) = \begin{cases} p_{\text{WAIT}} & \text{if } t = 0 \\ p_{\text{IN}} & \text{if } 0 \leq t \leq t_M \\ p_{\text{WAIT}} + e^{\alpha t/t_M} & \text{if } t > t_M \end{cases} \quad (2)$$

- $p_{\text{IN}} = 2$;
- $p_{\text{WAIT}} = 8$;
- $\alpha = 1.89$.