Workshop do Núcleo de Apoio à Pesquisa em Software Livre
São Carlos, 16 a 17 de Outubro de 2014.

Segurança da Informação baseada em OpenFlow e Computação Autonômica

Luiz Arthur F. Santos, Rodrigo Campiolo,
Prof. Dr Daniel Macêdo Batista

Departamento de Ciência da Computação – IME/USP
Email: {luizsan,campiolo,batista}@ime.usp.br

Introdução

- **Problemas de pesquisa**:
  - Crescimento do número de ataques contra redes locais;
  - Surgimento de novos desafios, tal como, BYOD;
  - Aumento na complexidade dos ataques à segurança (ex. BlackHole);
  - Ineficácia das ferramentas/administradores em deter ataques.

- **Possíveis soluções**:
  - Combinar ferramentas/métodos;
  - Computação Autonômica – CA;
  - Redes Definidas por Software (SDN);
  - Uso de fontes de informações distribuídas e heterogêneas.

Objetivo

Unir métodos de CA com os conceitos de SDN para desenvolver uma arquitetura de rede local capaz de detectar e reagir dinamicamente a problemas de segurança que afetem redes locais, isso com o mínimo de intervenção humana.

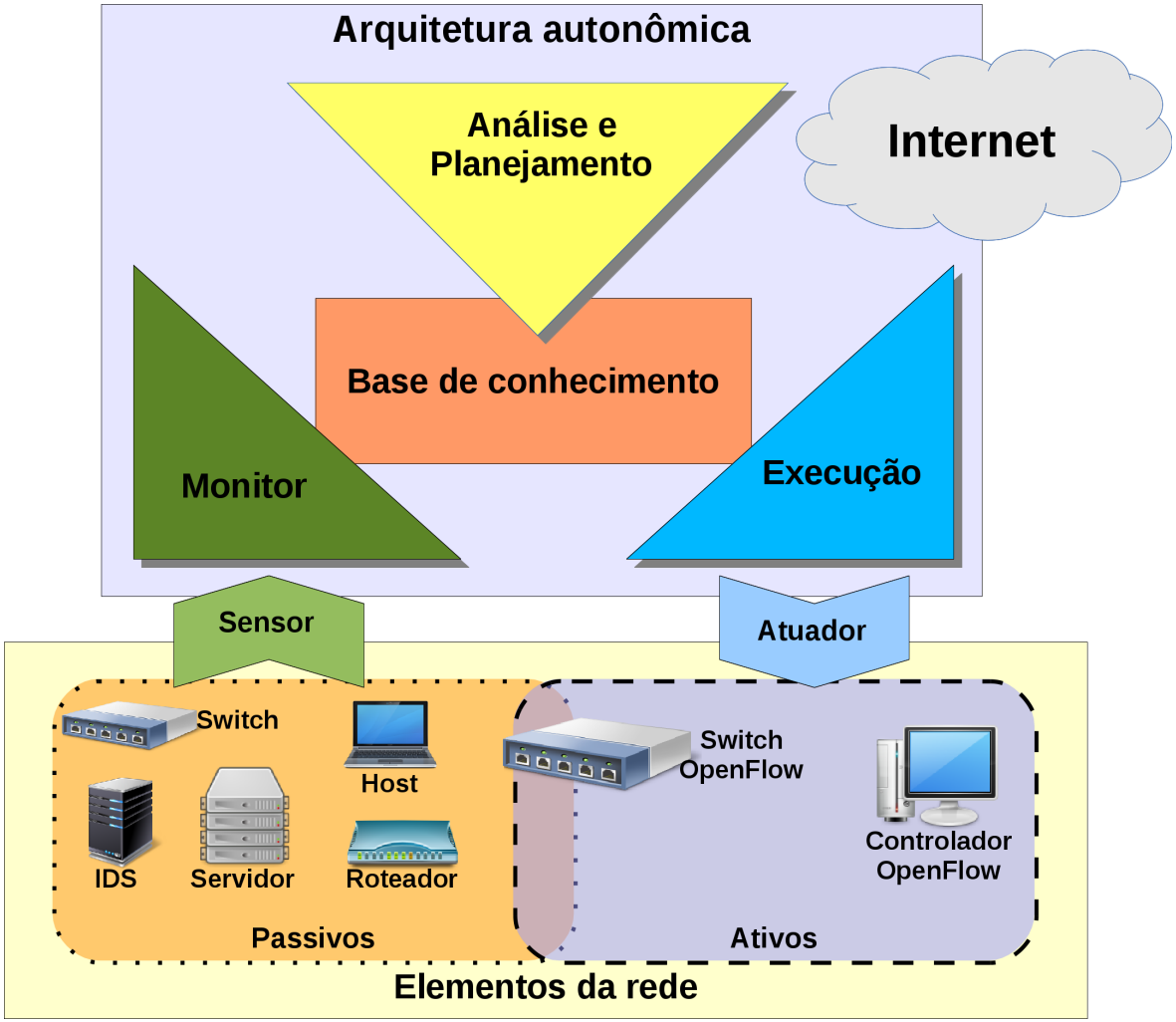
Objetivos específicos:

- Uso de técnicas que permitam extrair informações:
  - Locais (Sistemas de Detecção de Intrusão – IDS e OpenFlow);
  - Externas (Mensagens postadas na Internet).
- Criar regras de segurança que permitam mitigar problemas de forma proporcional a cada tipo de ataque.
- Desenvolver e disponibilizar ferramentas que implementem as técnicas propostas sob licença livre.

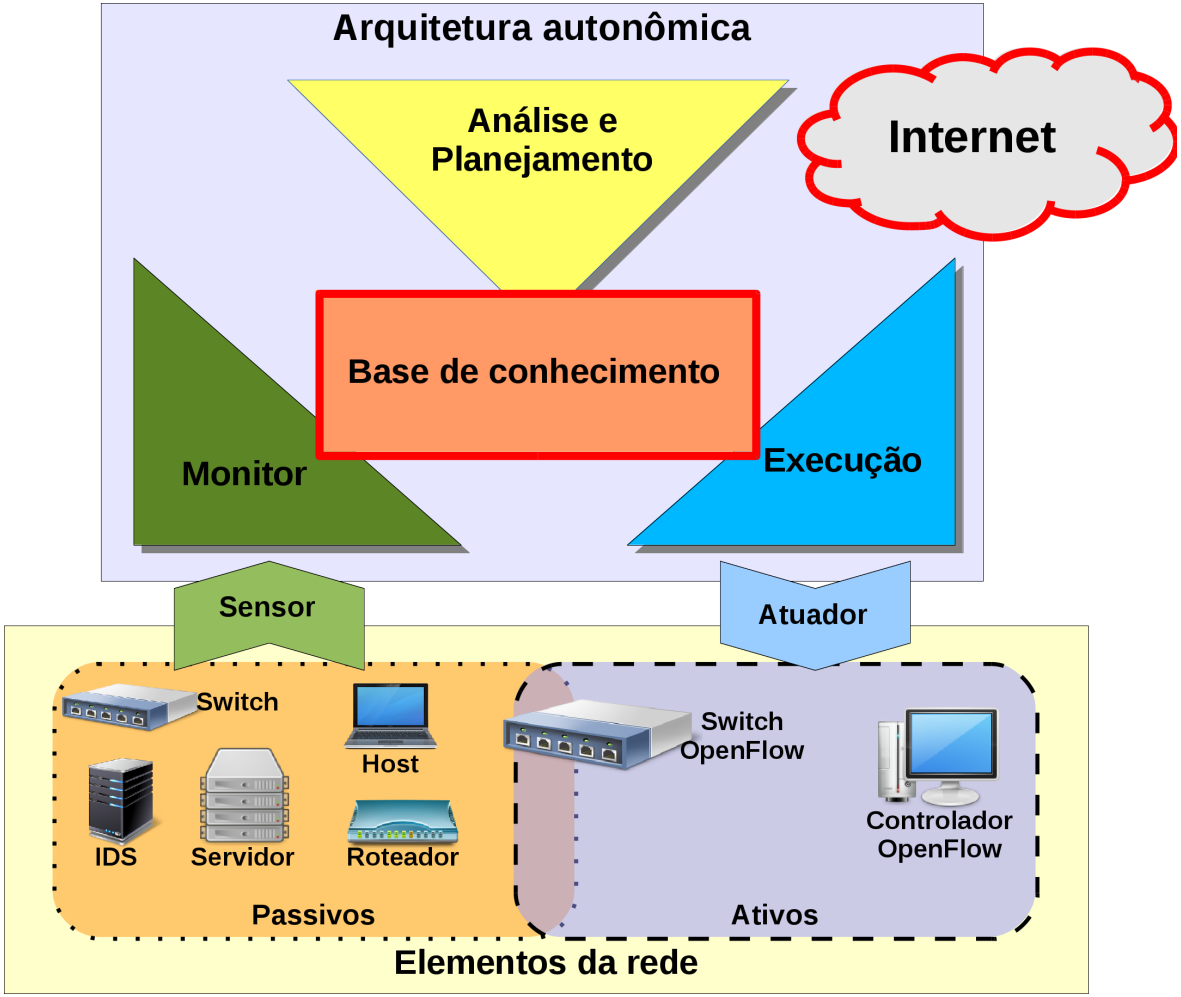
Contribuições

- Desenvolvimento de arquitetura e métodos que permitam integrar CA e SDN, para mitigar problemas de segurança em redes de computadores locais;
- Combinação de informações de fontes heterogêneas internas e externas ao ambiente de rede local, para a geração e reação autonômica a incidentes de segurança;
- Desenvolvimento de métodos que permitam reagir dinamicamente e proporcionalmente aos diferentes tipos de problemas de segurança;
- Protótipo de aplicação de segurança em software Livre;
- Investigação da efetividade do uso de SDN em aplicações de segurança.

Arquitetura Proposta



Resultados – Parte 1

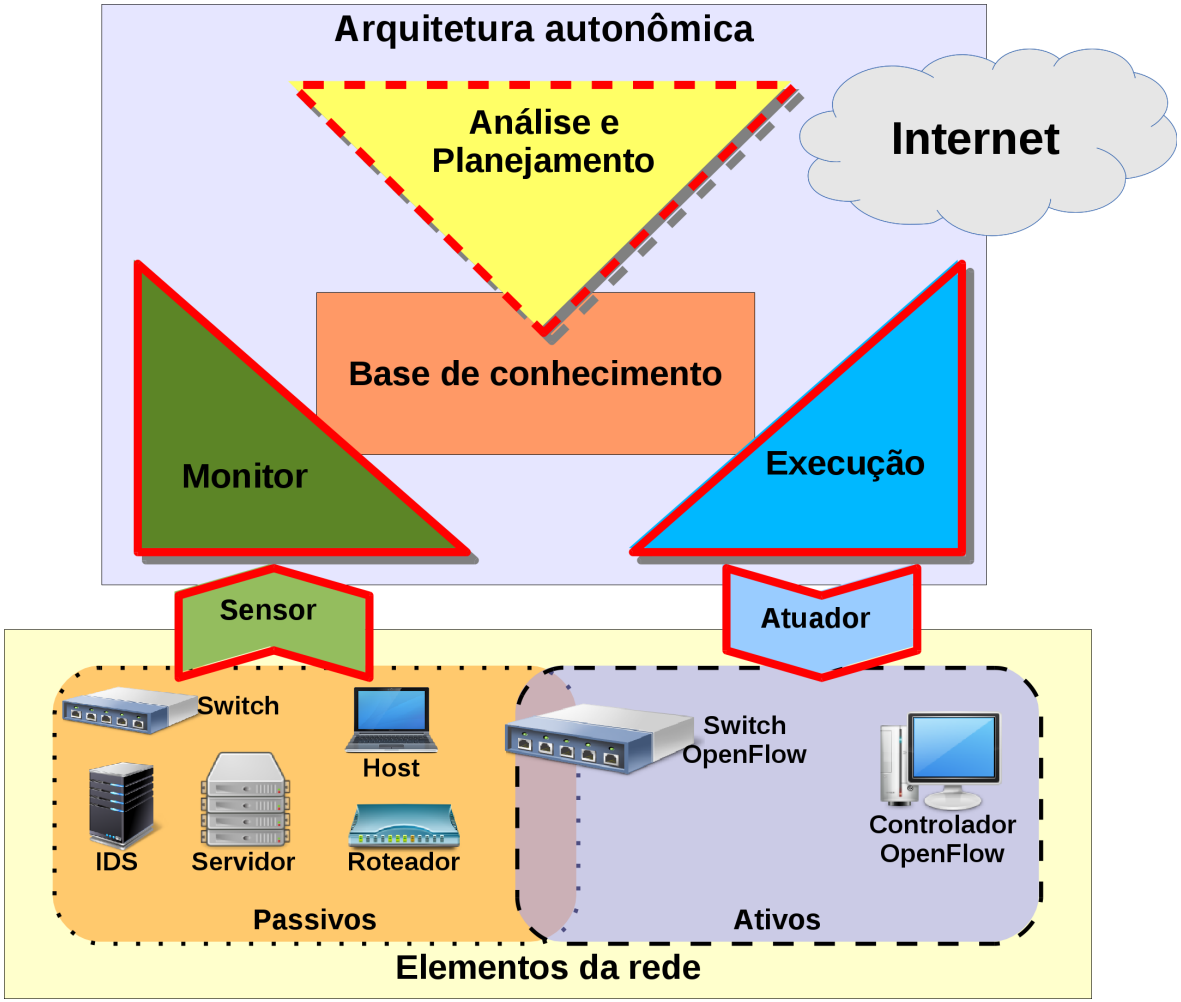


Resultados – Parte 1

- Analisar um conjunto de mensagens do Twitter para verificar se as mensagens ajudam na identificação e alerta antecipado de possíveis problemas de segurança.

- Elaboração de um mecanismo para extrair notificações de segurança de computadores em mensagens postadas no *microblog* Twitter.

Resultados – Parte 2



Resultados – Parte 2

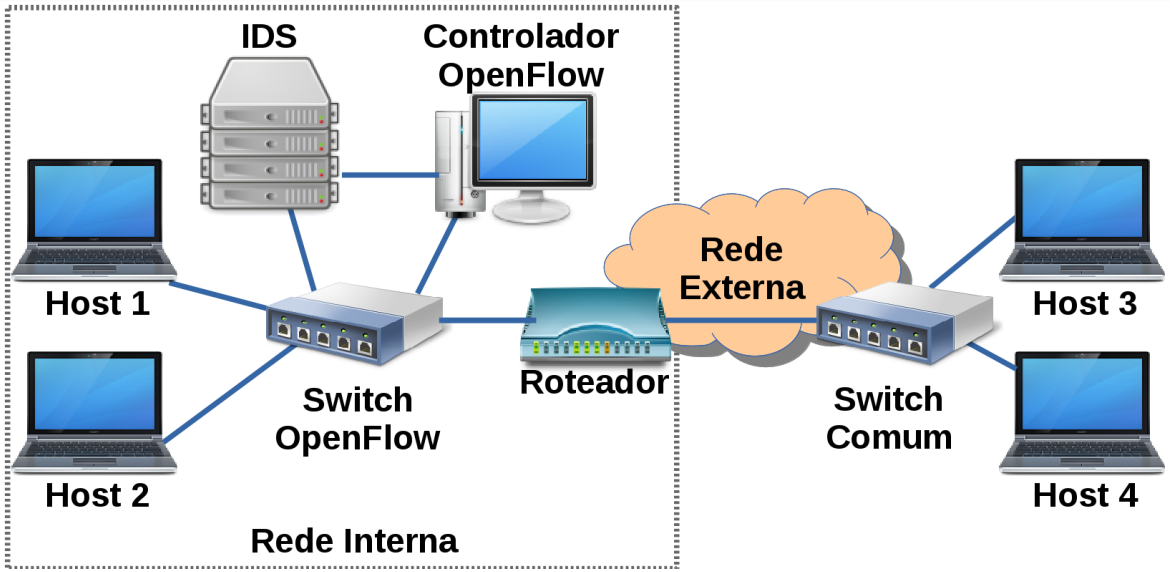
- Desenvolver arquitetura autonômica que une IDS e SDN, na figura do OpenFlow, para mitigar ações maliciosas em redes de computadores locais.

- Implementação de um protótipo da arquitetura proposta e disponibilização do código fonte :

  https://github.com/luizsantos/Of-IDPS.

WoSiDA

Resultados – Parte 2

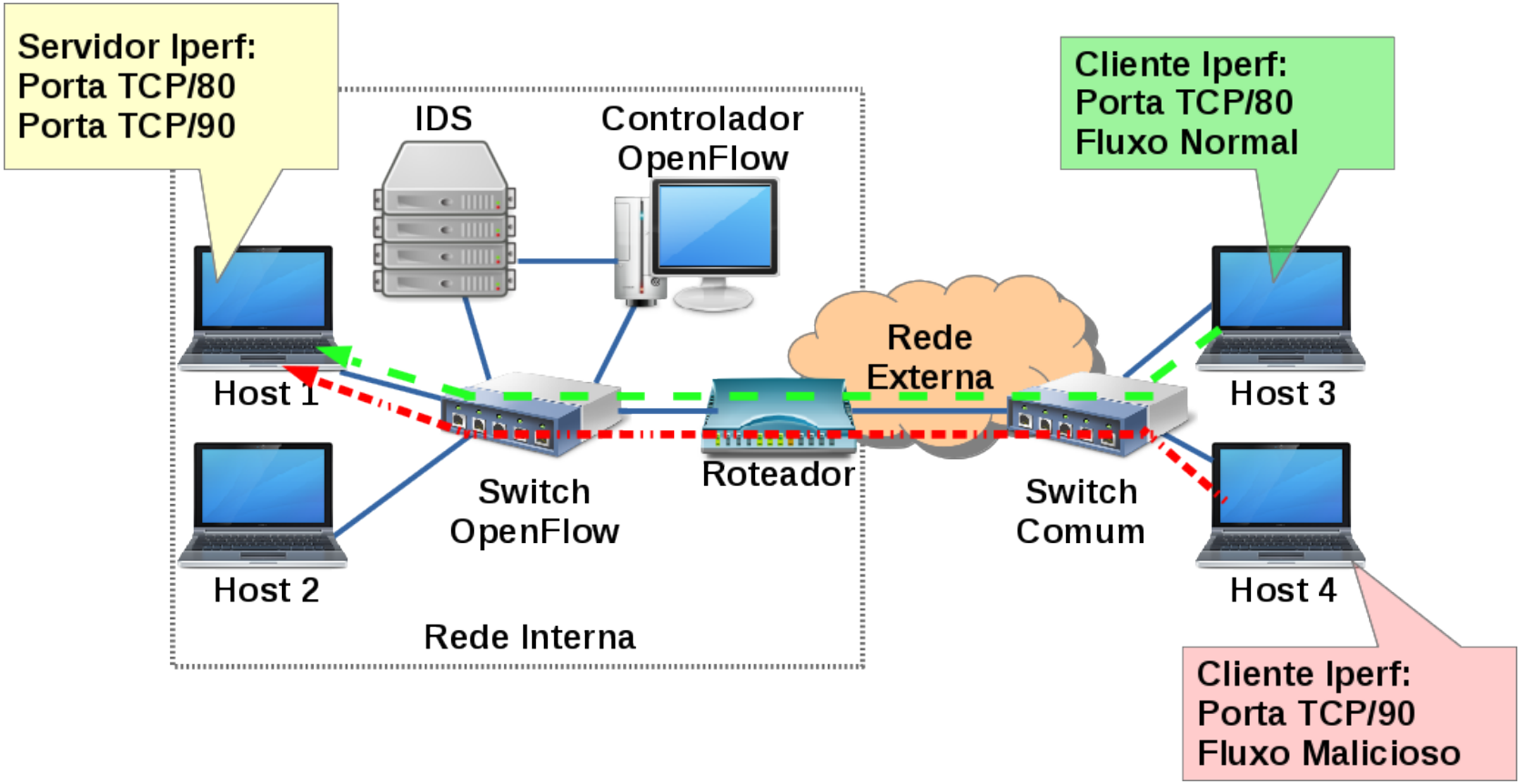


- **Controlador OpenFlow:**
  - Of-IDPS – OpenFlow Intrusion Detection and Prevention System (Nossa Proposta);
  - OpenFlow Beacon 1.0.4.

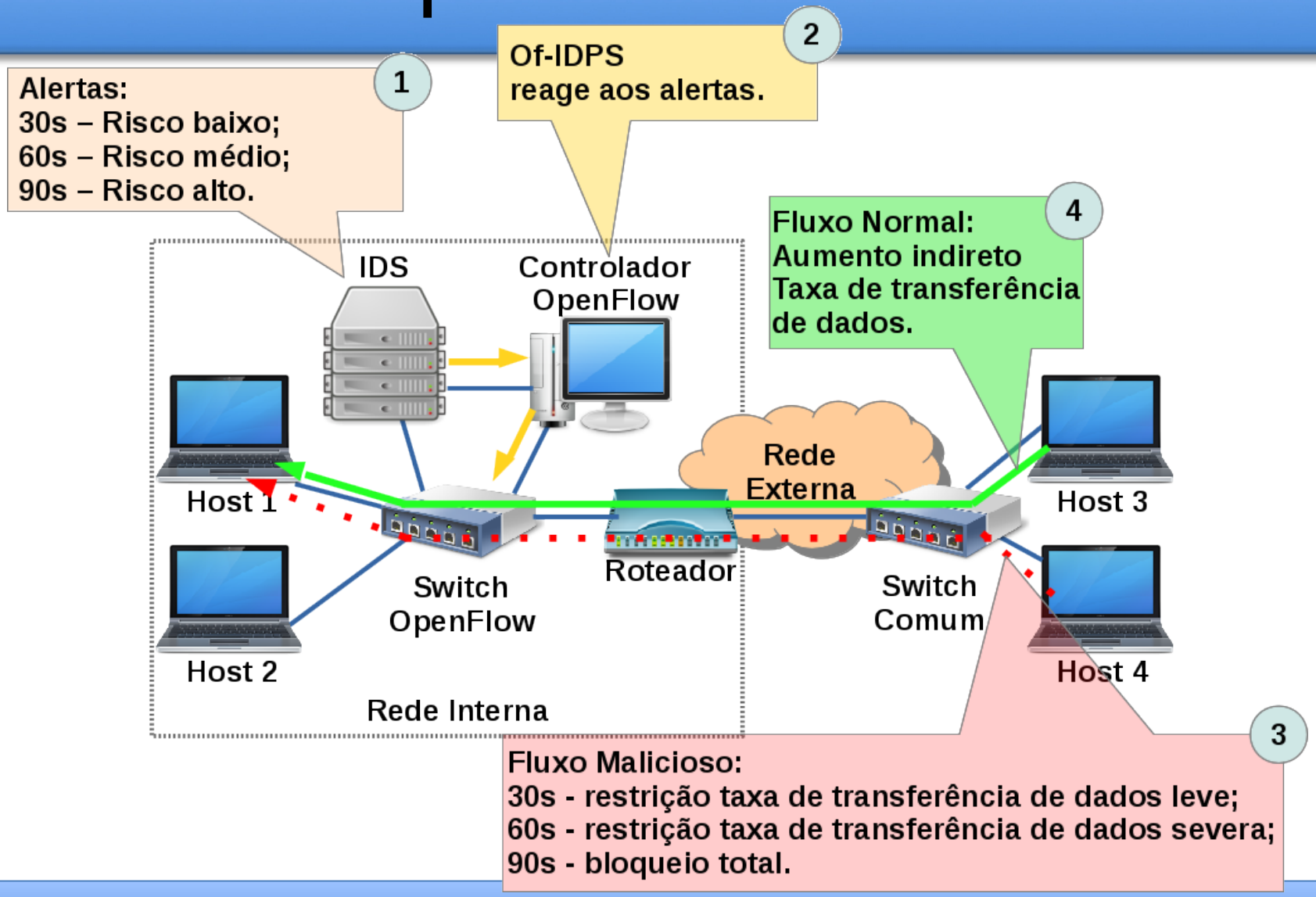
- **Outros elementos da rede (simulados):**
  - Mininet 2.1.0;
  - Open vSwitch 1.9.0

Experimento 1

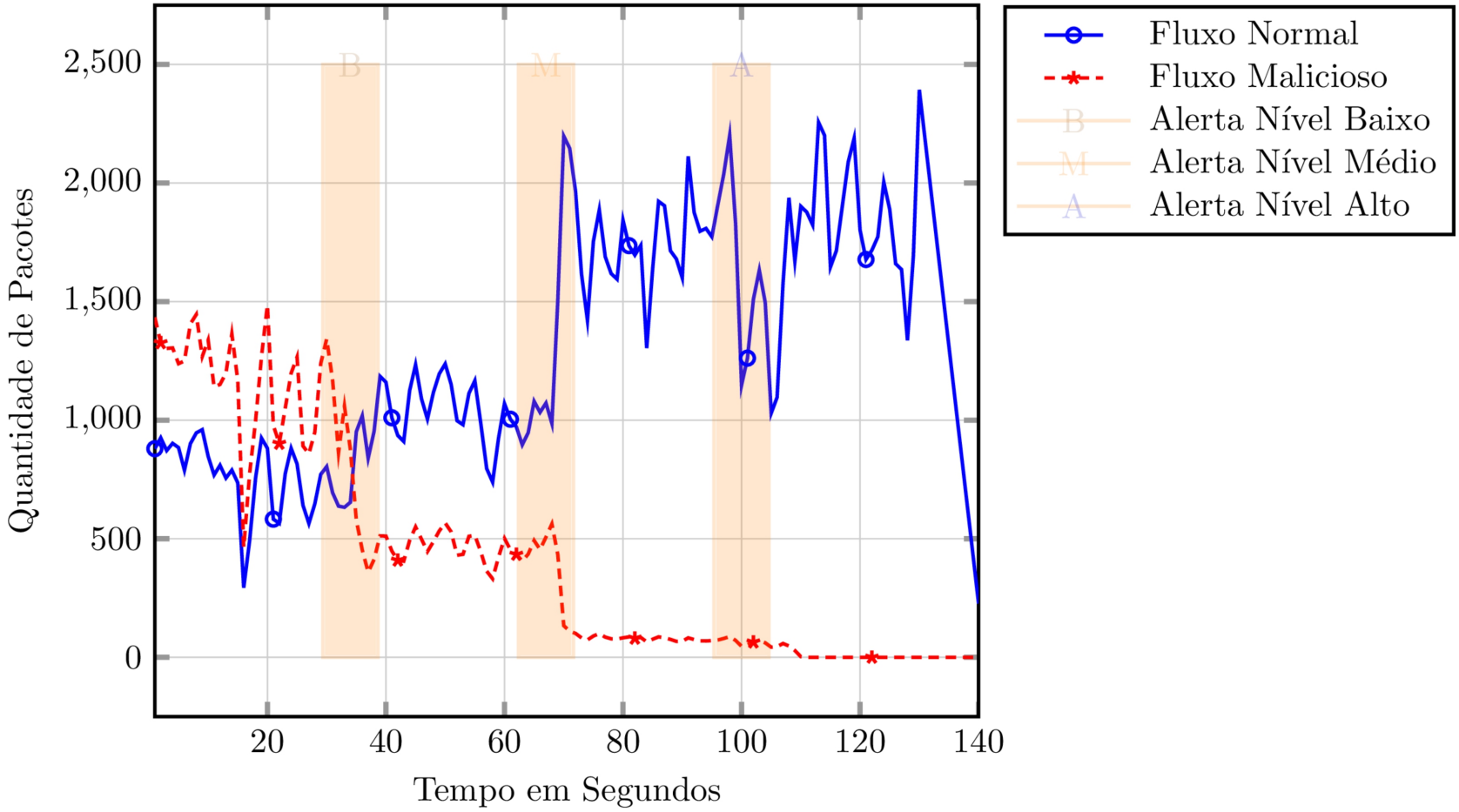
- Execução e resposta do Of-IDPS a alertas do IDS:



Experimento 1

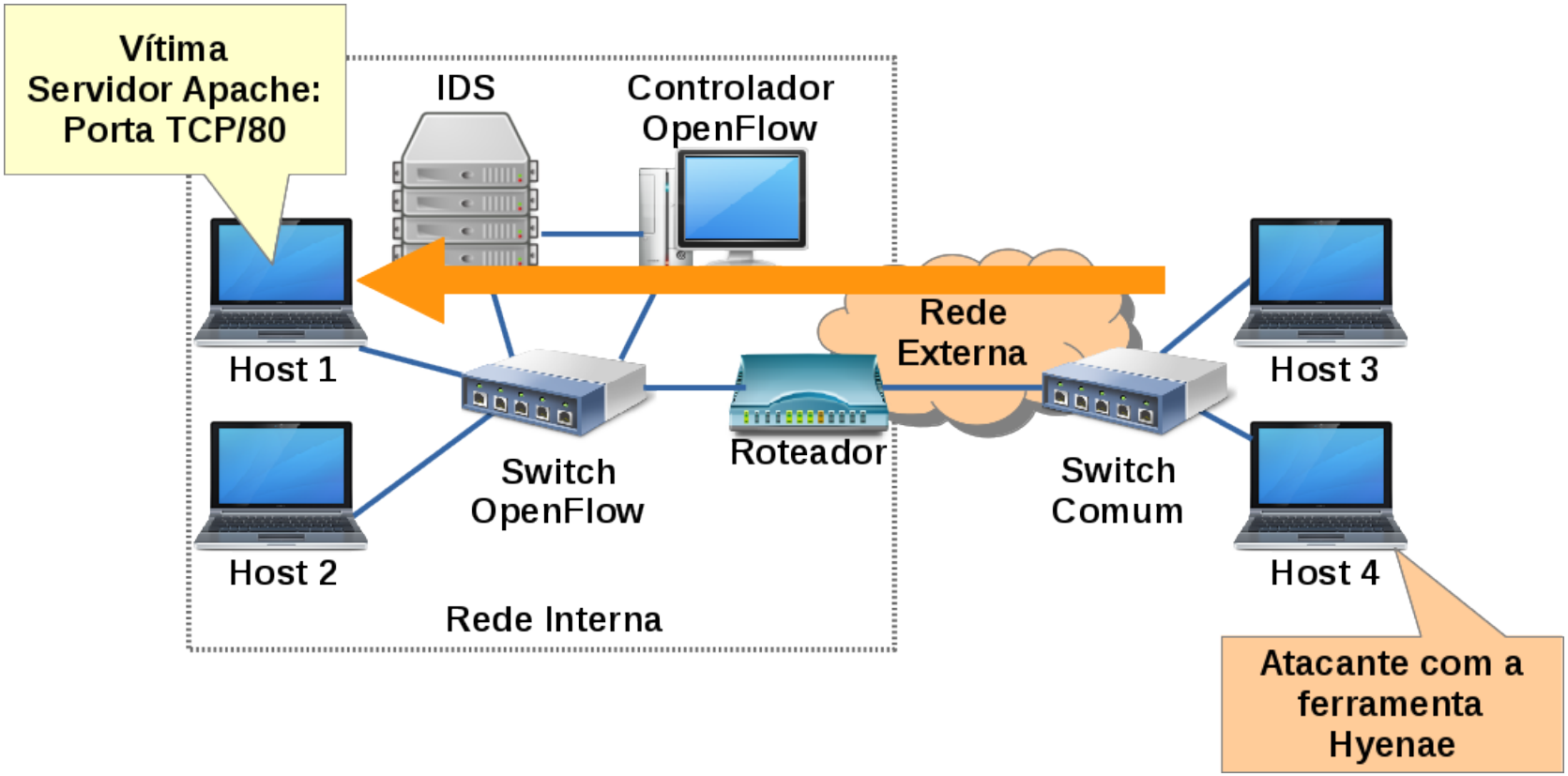


Resultados – Exp. 1

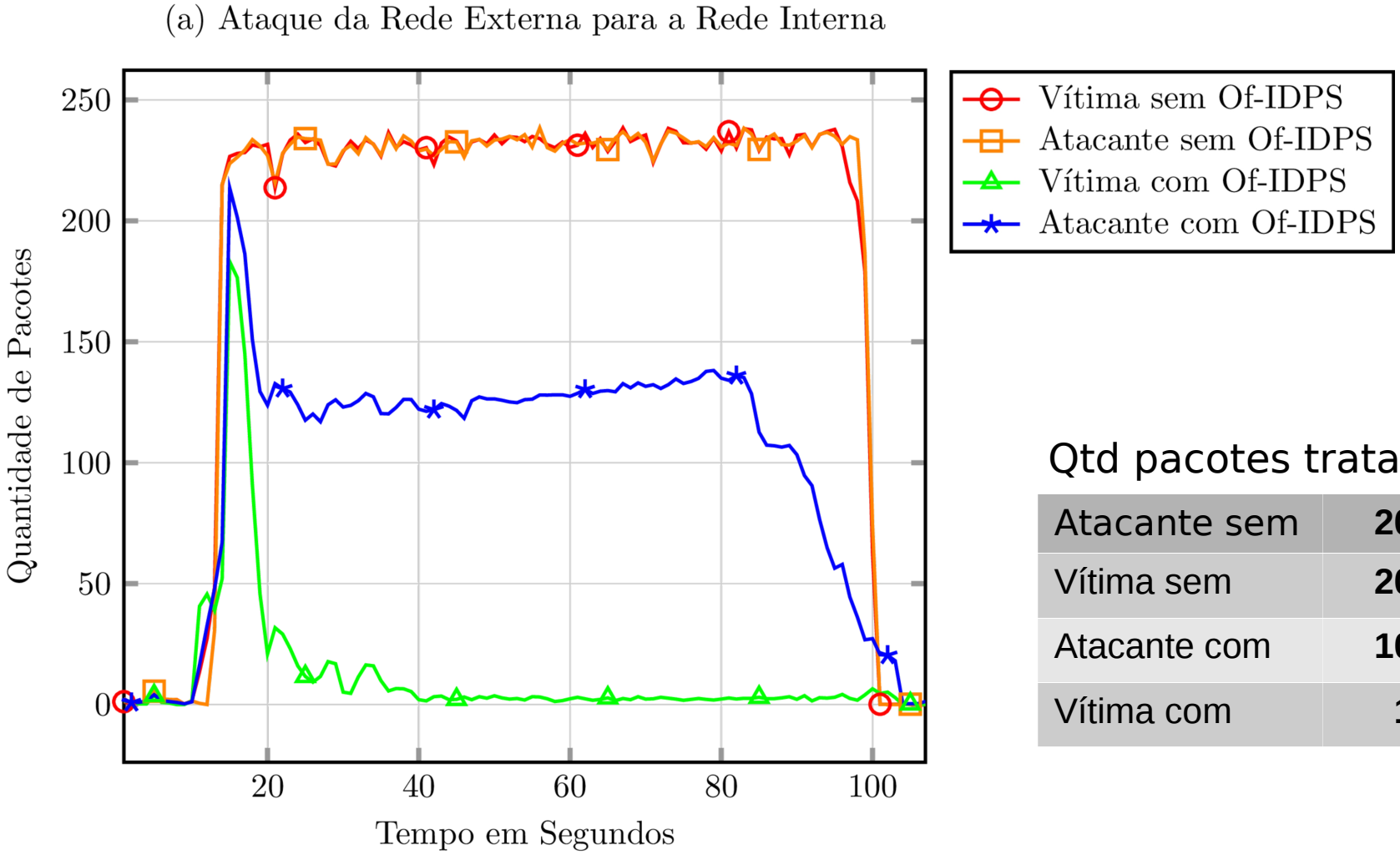


Experimento 2

- Reação a ataques de negação de serviço TCP/SYN:



Resultados – Exp. 2



Qtd pacotes tratados:

Atacante sem	**20.014**
Vítima sem	**20.014**
Atacante com	**10.646**
Vítima com	**1.279**

Considerações Parciais

- A arquitetura proposta consegue identificar desequilíbrios causados por problemas de segurança e reagir evitando a degradação massiva nos recursos da rede.

- A criação de um sistema de segurança autonômico que integra IDS e OpenFlow mostra-se uma solução efetiva e prática para detectar ameaças de segurança em redes locais.

- Há alertas de segurança postados em redes sociais e tais mensagens podem ser exploradas para auxiliar na identificação de problemas de segurança em redes.

Próximos Passos:

- Explorar mais a integração das estatísticas de redes obtidas com o OpenFlow.
- Correlacionar informações obtidas a partir de outras fontes localizadas em segmentos comuns e distintos da rede.
- Utilizar métodos de aprendizado de máquina para a geração de políticas de segurança baseadas nos ataques anteriores.

Perguntas ?

Luiz Arthur F. Santos
luizsan@ime.usp.br

Rodrigo Campiolo
campiolo@ime.usp.br

Daniel Macêdo Batista
batista@ime.usp.br

Obrigado!