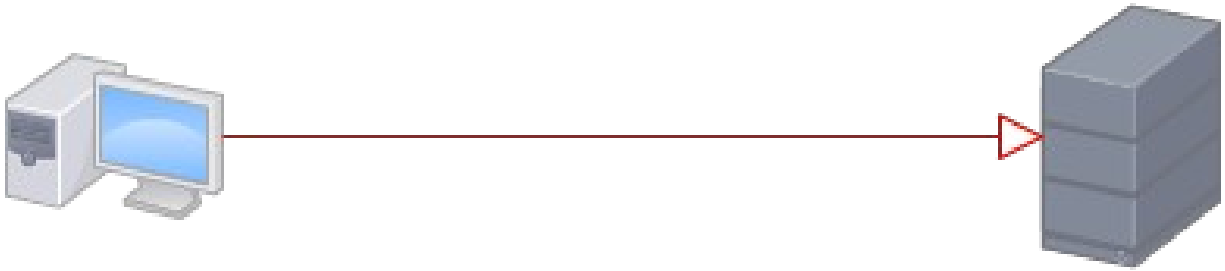
Detecção em Tempo-Real de Ataques de Negação de Serviço na Rede de Origem

Rodrigo Caetano de Oliveira Rocha
Humberto Torres Marques Neto (Orientador)

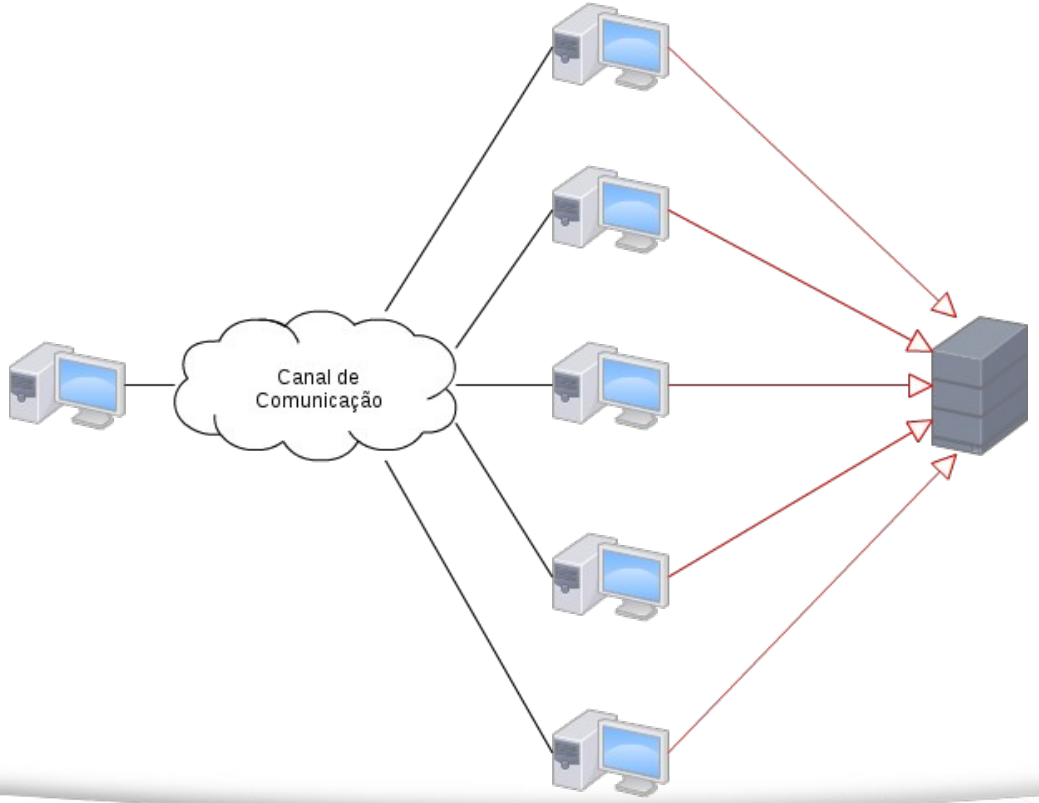
Introdução

Ataque de Negação de Serviço (DoS) é um ataque designado a tornar um recurso de rede indisponível para seus usuários legítimos.



Introdução

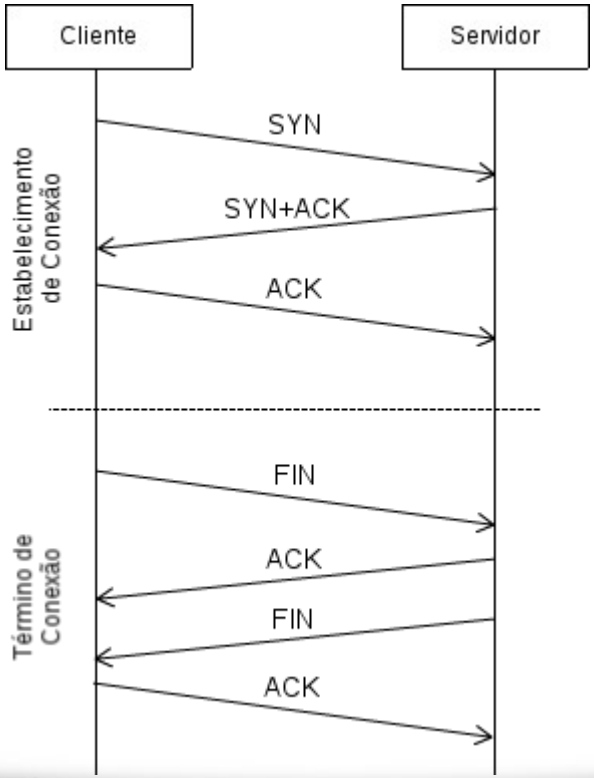
Ataque DDoS é aquele onde múltiplos sistemas comprometidos são usados para executar um ataque DoS coordenado contra um ou mais alvos.



Introdução

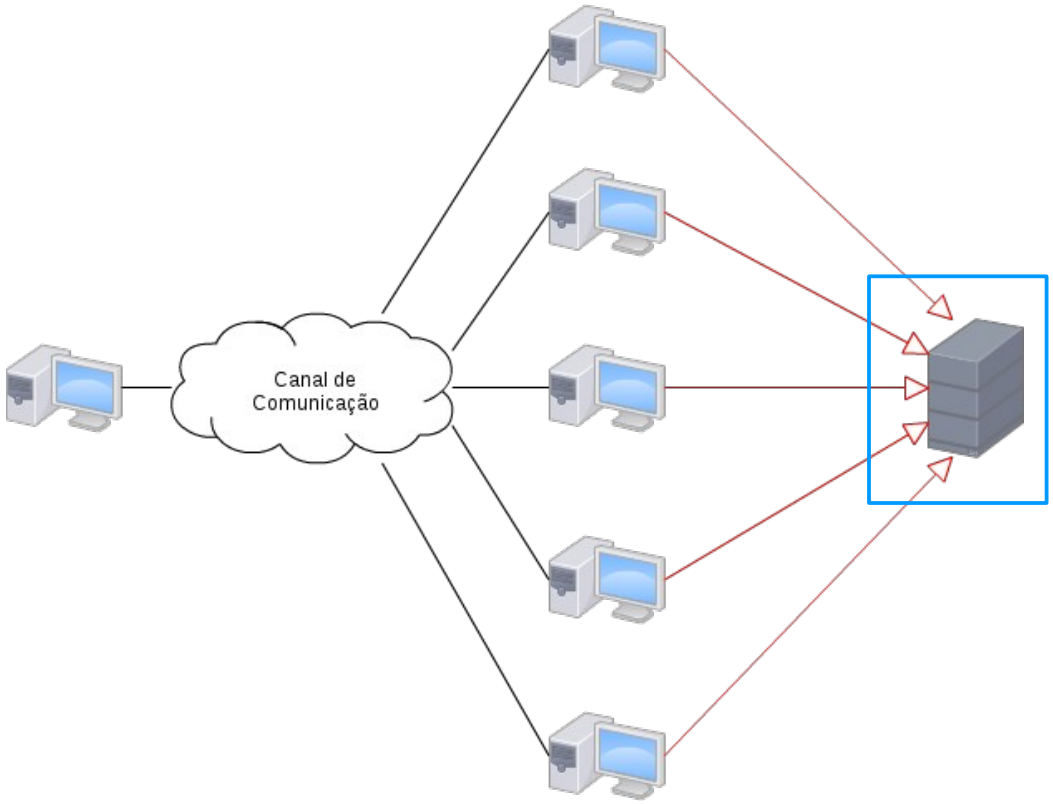
- Ataque por Inundação UDP;
- Ataque por Inundação TCP SYN.

Conexão TCP Legítima



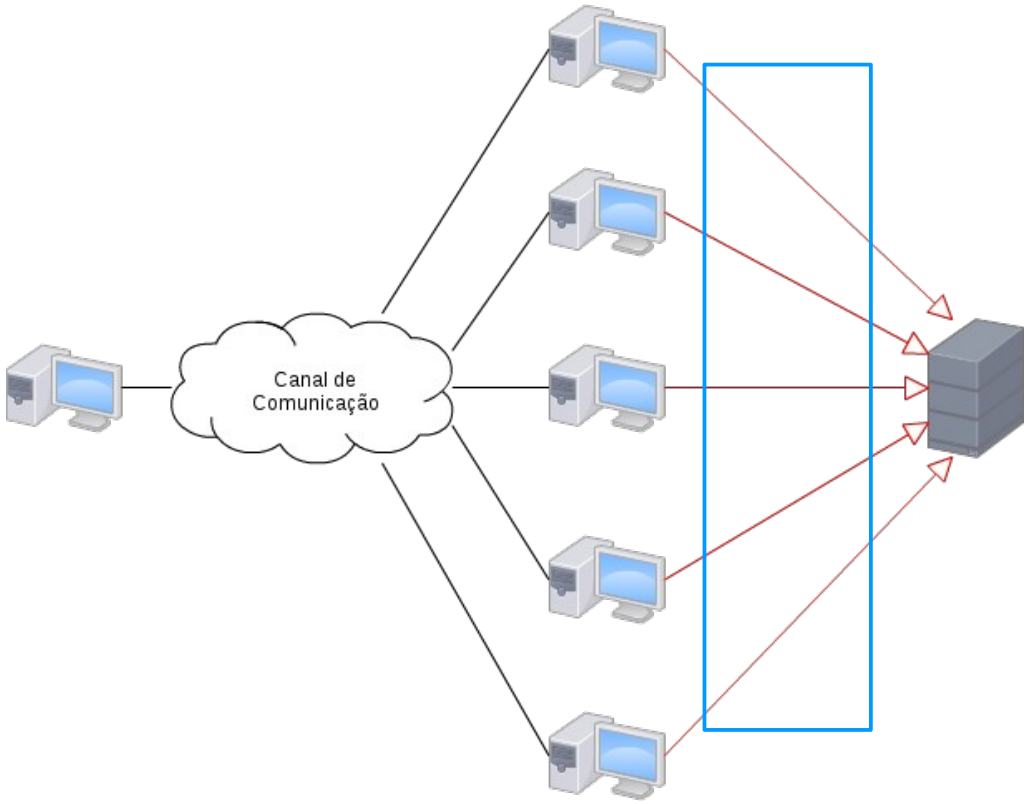
Mecanismos de Defesa

Mecanismos Implantados na Rede da Vítima



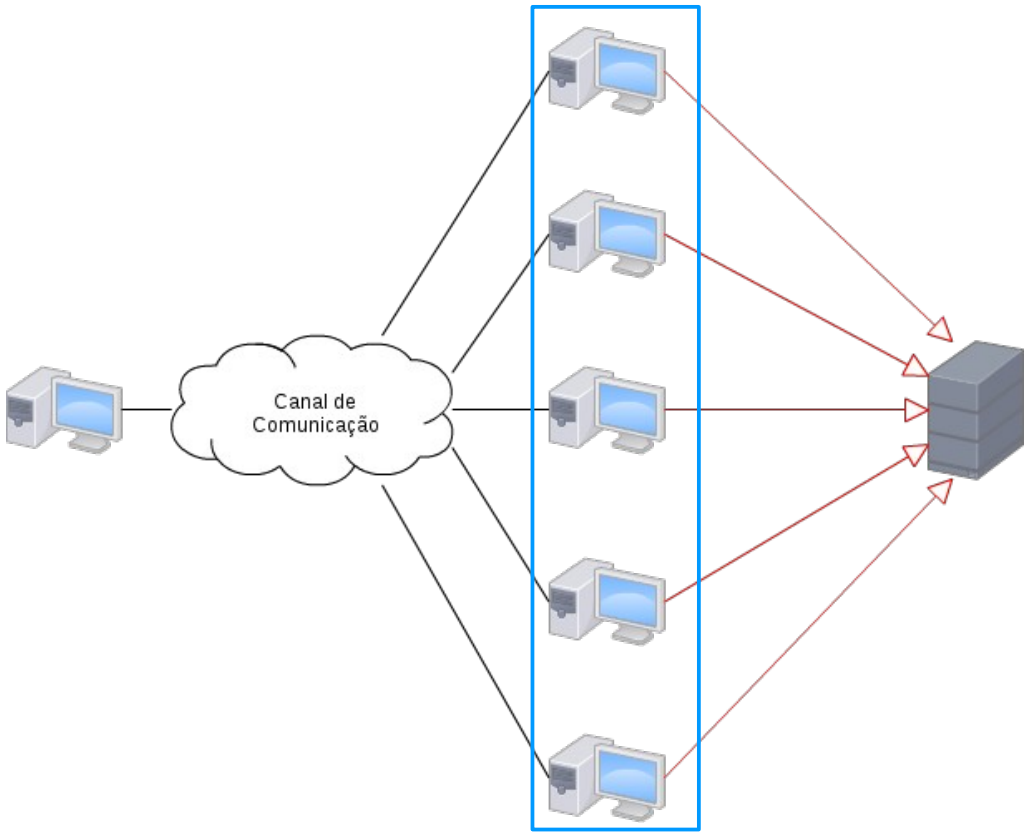
Mecanismos de Defesa

Mecanismos Implantados na Rede Intermediária



Mecanismos de Defesa

Mecanismos Implantados na Rede de Origem



Proposta

Detectar em tempo-real ataques DDoS na rede de origem

Motivação

Por que implantar um mecanismo de defesa na rede de origem do ataque?

- Usuários de sistemas agentes geralmente não sabem que seu sistema foi comprometido e que fará parte de ataques DDoS;

- Facilita rastrear os responsáveis reais pelo ataque;

Motivação

- O fluxo de ataque pode ser bloqueado antes de entrar no núcleo da Internet e ser agregado à outros fluxos;

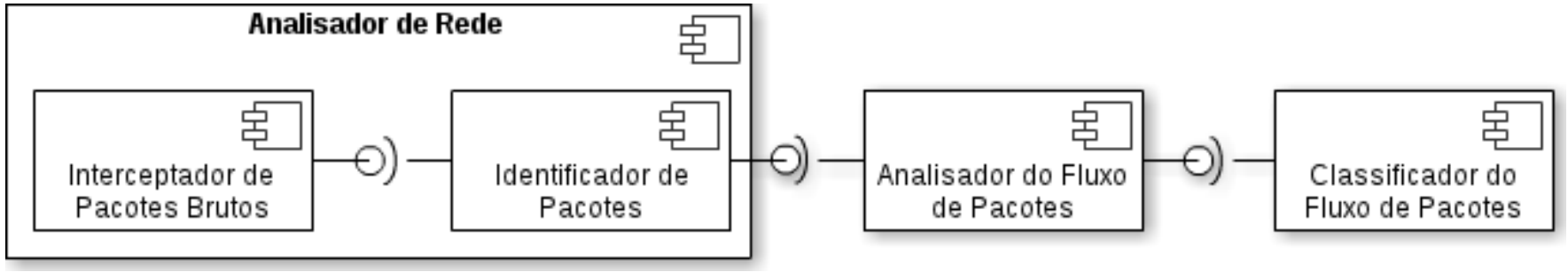
- O baixo grau de agregação de fluxos permite usar estratégias de defesa mais complexas e com maior precisão.

Classificador Bayesiano Simples

- Classificador estatístico;
- Baseado no Teorema de Bayes;
- Baseado em aprendizagem de máquina;
- Eficiente em ambas as etapas de aprendizagem e classificação.

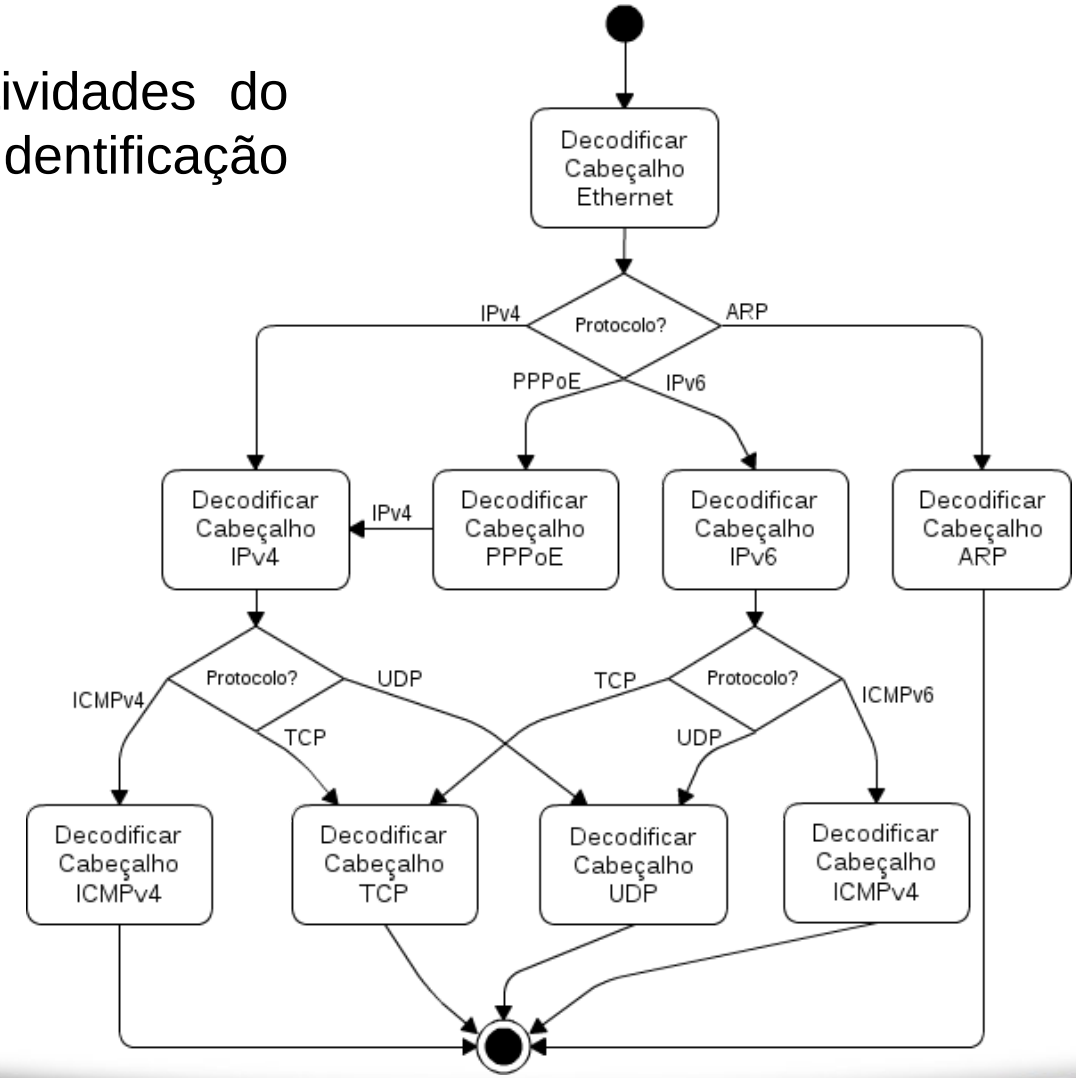
Mecanismo

Diagrama de Componentes do Mecanismo de Detecção de Ataques de Negação de Serviço



Mecanismo

Diagrama de Atividades do Componente de Identificação de Pacotes



Mecanismo

Analisador do Fluxo de Pacotes

- Janela temporal;
- Fluxos são separados por endereço IP de destino;
- Atributos de ataques por inundação TCP SYN;

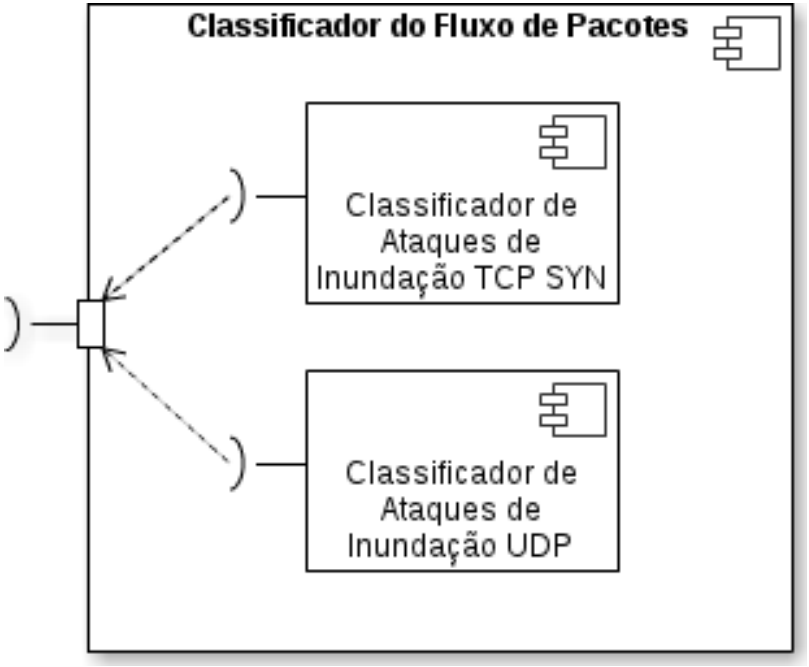
$$X = \left(P_{SYN} - \left(P_{FIN} + P_{RST} \right) \right)$$

- Atributos de ataques por inundação UDP.

$$X = \left(P_{UDP} \right)$$

Mecanismo

Classificador do Fluxo de Pacotes



Metodologia de Treinamento

Treinamento mediante simulação do comportamento de uma vítima secundária.

Tabela de Treinamento do Ataque por Inundação TCP SYN

Classe	Média (μ)	Desvio Padrão (σ)
Tráfego Normal (C_N)	1.367528	15.162268
Tráfego de Ataque (C_A)	33709.571429	22649.832694

Tabela de Treinamento do Ataque por Inundação UDP

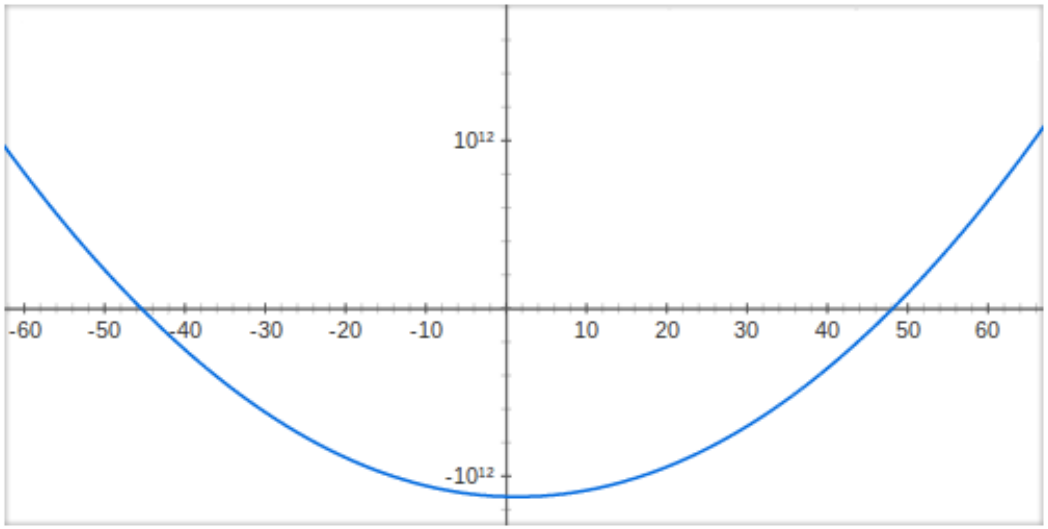
Classe	Média (μ)	Desvio Padrão (σ)
Tráfego Normal (C_N)	124.352941	344.498086
Tráfego de Ataque (C_A)	35768.285714	21922.441377

Avaliação Matemática

Classificador de ataques por inundação TCP SYN

$$Y = P(X|C_A) - P(X|C_N)$$

$$X = (P_{SYN} - (P_{FIN} + P_{RST}))$$

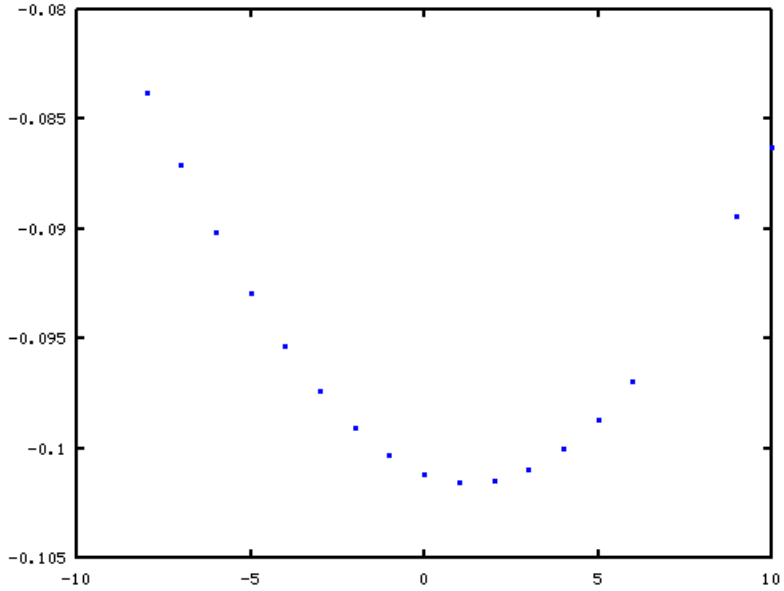


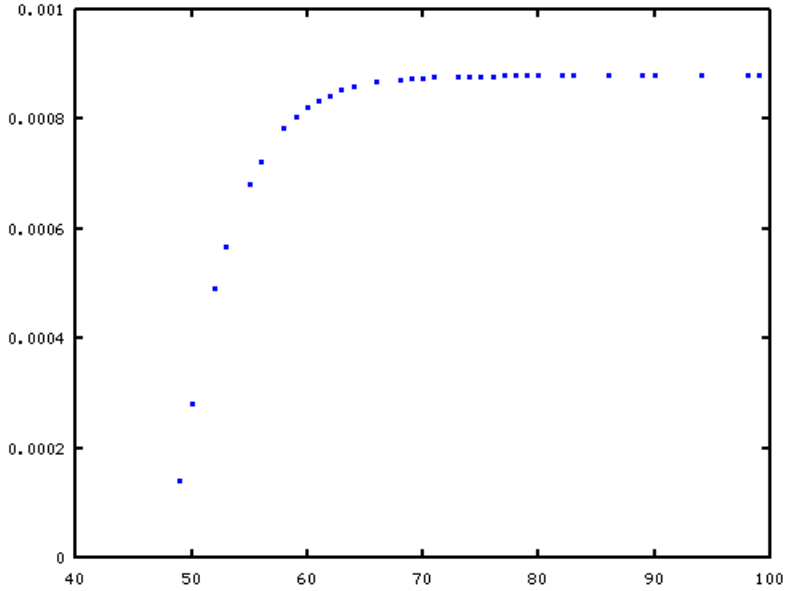
Resultados Experimentais

Classificador de ataques por inundação TCP SYN

$$Y = P(X|C_A) - P(X|C_N)$$

$$X = (P_{SYN} - (P_{FIN} + P_{RST}))$$



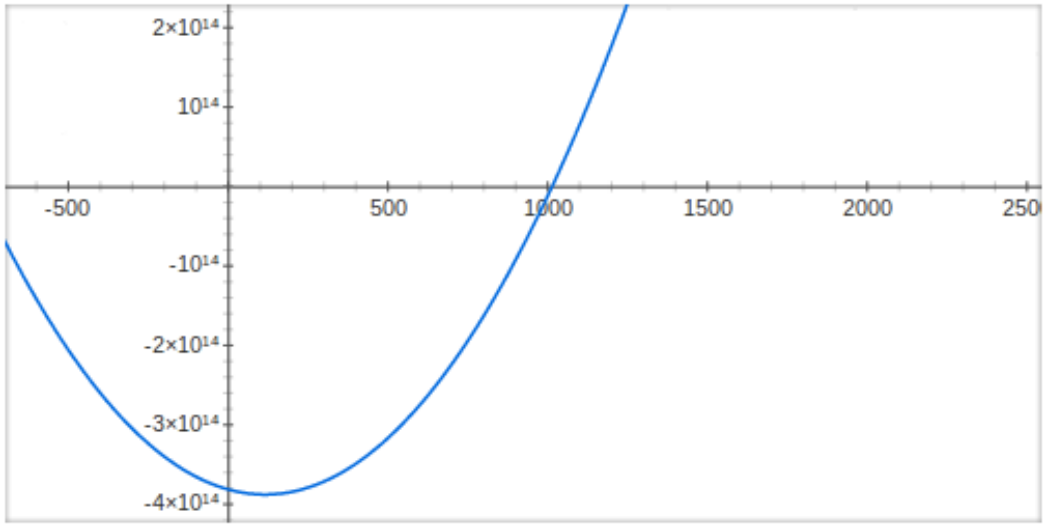


Avaliação Matemática

Classificador de ataques por inundação UDP

$$Y = P(X|C_A) - P(X|C_N)$$

$$X = (P_{UDP})$$

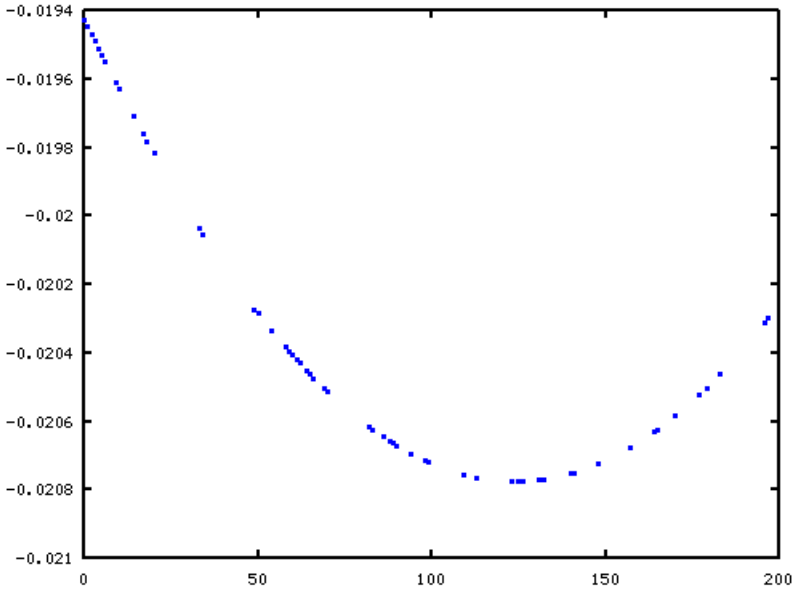


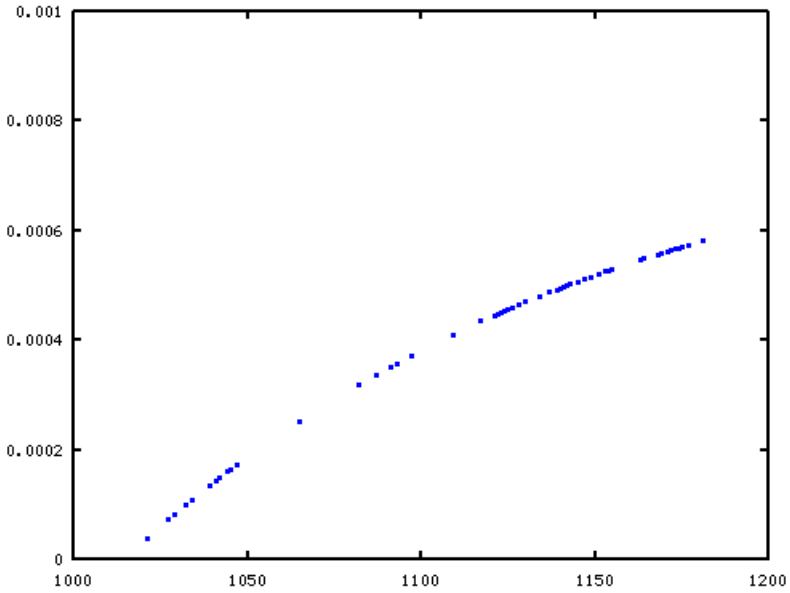
Resultados Experimentais

Classificador de ataques por inundação UDP

$$Y = P(X|C_A) - P(X|C_N)$$

$$X = (P_{UDP})$$

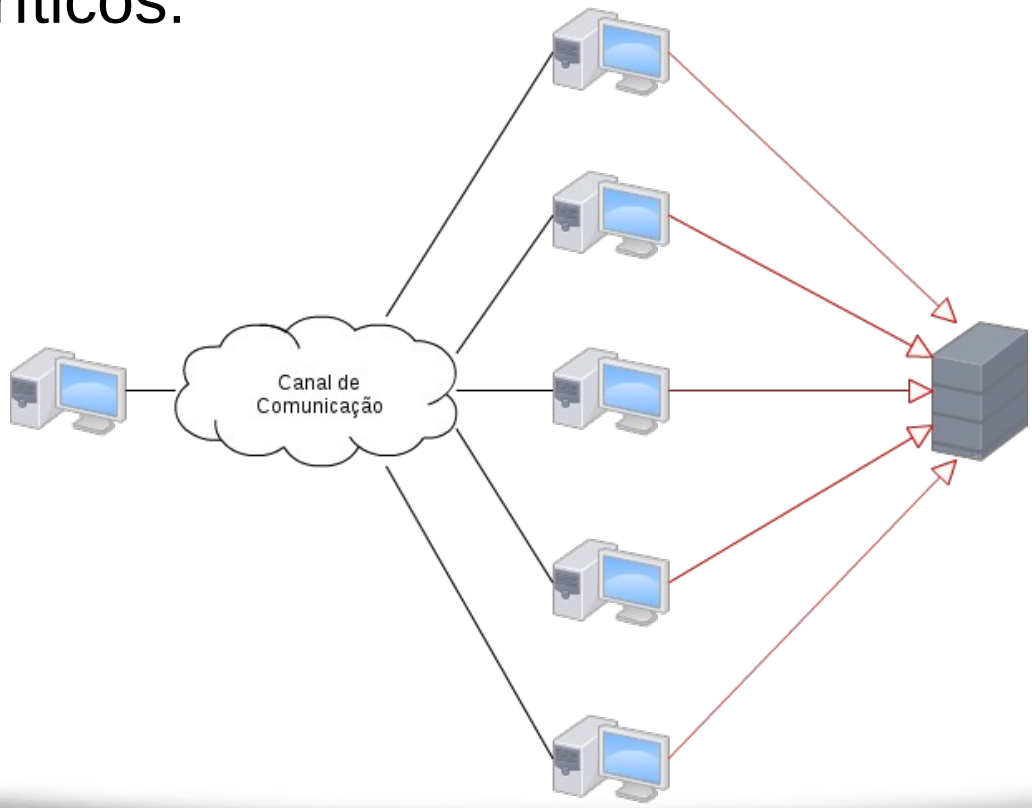




Conclusões

- Mecanismo eficaz quanto à detecção de ataques na rede origem.

- Casos críticos:



Obrigado pela atenção.

Perguntas?