SBSEG'08 1 a 5 de setembro Gramado - RS

Uma Proposta de Utilização da Transformada de Wavelet e Redes Neurais para Detecção de Ataques em Redes Ad Hoc Sem Fio

Ed' Wilson Tavares Ferreira (CEFETMT)
Ruy de Oliveira (CEFETMT)
Gilberto Arantes Carrijo (UFU)
Nelcileno Virgílio de Souza Araújo (UFMT)

Transformadas de Wavelet

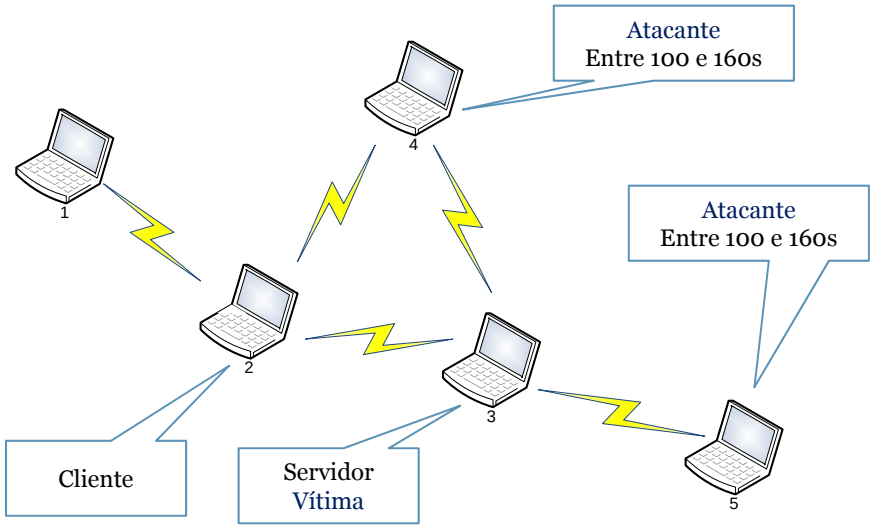
- Definição
- Descrever o comportamento característico
- Atualização de perfil
- Detecção de descontinuidade e variações bruscas
  - Comportamentos anômalos
- Métricas
  - Banda disponível/utilizada
  - Conexões
  - Fluxos
  - Pacotes transmitidos/recebidos/descartados

Simulação

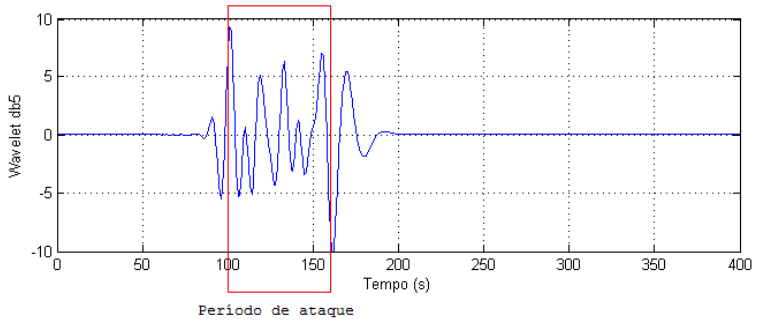
- NCTUns

Parâmetro	Valor
Tempo de simulação	400s
Número de dispositivos	5
Distância média entre os dispositivos	200m
Rede sem fio	IEEE 802.11b
Alcance da transmissão	250m

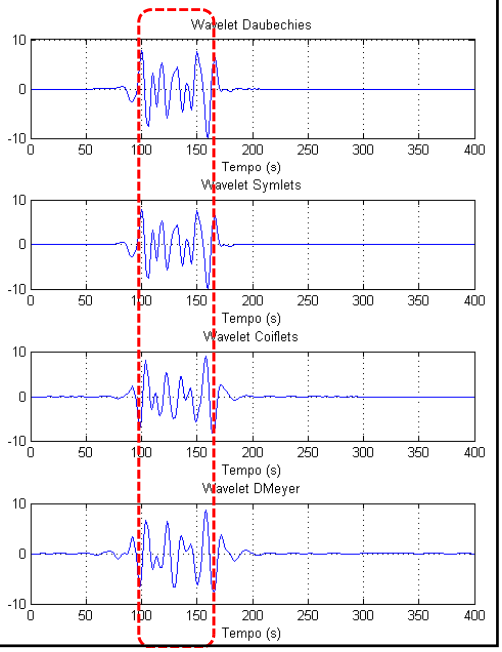
Topologia simulada



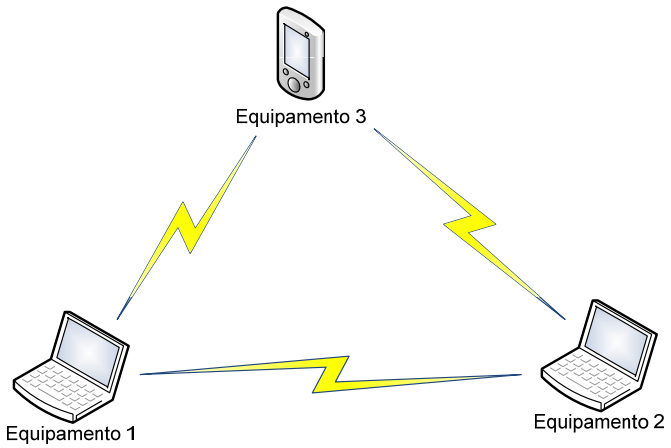
Aplicação da Wavelet de Daubechies



Coeficientes de Algumas Wavelets



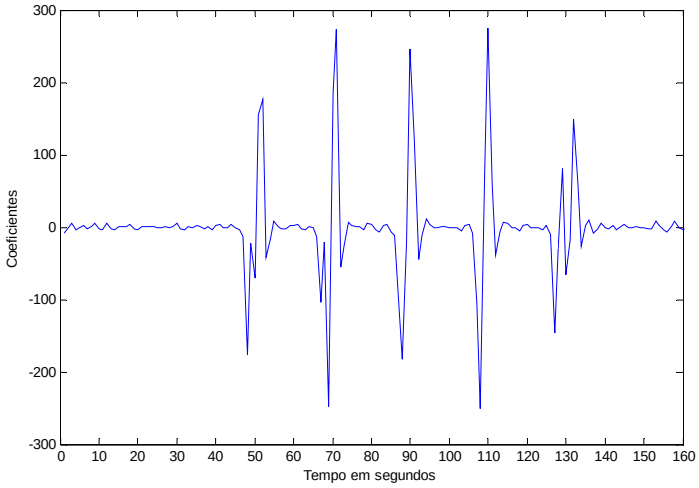
Topologia do Ambiente de Testes



Ataques TCP-RPC (Ambiente de Testes)

Ataques	Período (em segundos)
Primeiro	Entre 47 a 50
Segundo	Entre 67 a 69
Terceiro	Entre 86 a 89
Quarto	Entre 106 a 108
Quinto	Entre 126 a 130

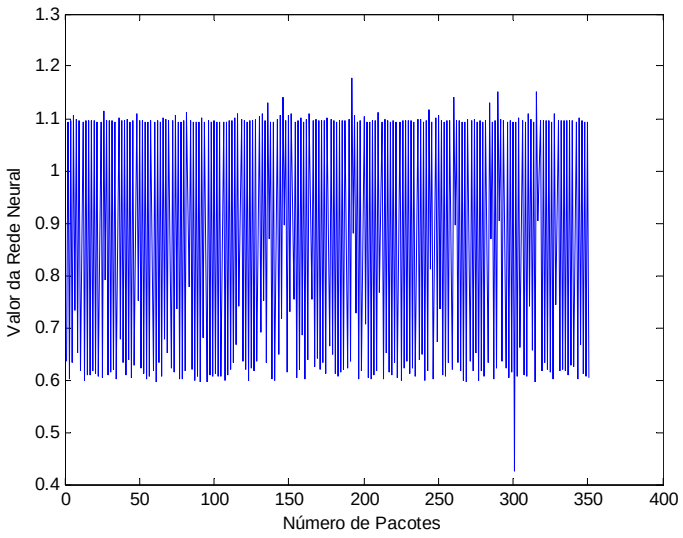
Coeficientes de Daubenchies (db5)



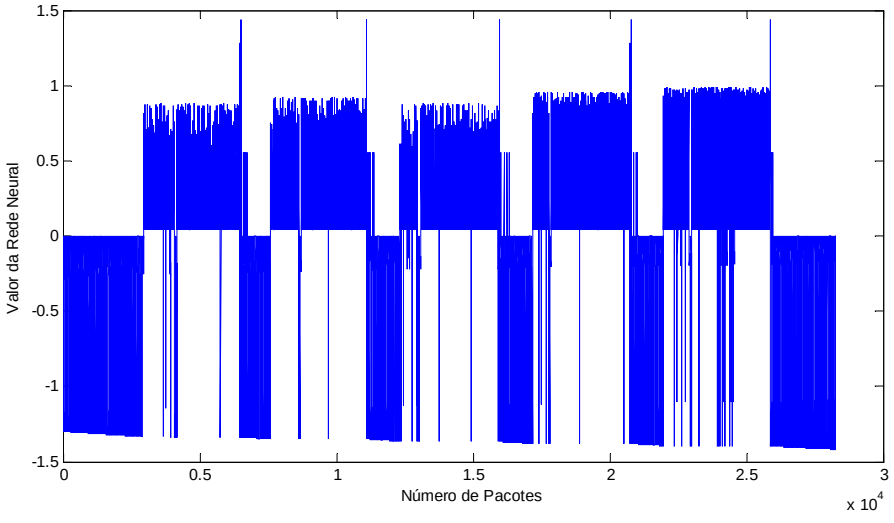
Redes Neurais

- Funcionamento
  - Dados de auditoria
  - Treinamento
- Classificação de ataques

Testes De Validação



Classificação Dos Ataques



Comentários Finais

- Sistema
  - Wavelet => Detecção
  - Redes Neurais => Classificação
- O algoritmo detectou mudança abrupta na rede
- A rede neural classificou o ataque efetuado
- Wavelets
  - Vantagem
  - Desvantagem
- Redes Neurais
  - Vantagem
  - Desvantagem

Trabalhos Futuros (ou Continuação)

- Integrar wavelet com redes neurais
- Criar e atualizar perfis de comportamento
- Medir
  - Falsos positivos
  - Falso negativos
- Comparar com outros trabalhos