Esse trabalho descreve uma forma hibrida utilizando duas técnicas de inteligência artificial, redes neurais e algoritmos genéticos para detecção de intrusão em uma rede de computadores. Utilizando informações extraídas dos pacotes TCP/IP versão 4, o algoritmo vai procurar violações coletando informações e analisando em tempo real por sinais de intrusão e mau uso, assim classificando o pacote como normal ou em um dos tipos de ataque pré-definido que podem ser feitos remotamente: DoS, U2R, R2L e Probes. Para o treinamento do algoritmo, será usada a base de dados KDD Cup99.

Referencias

FUNAI-32.pdf

0031732.pdf