Em uma trabalho em conjunto do Departamento de Automação e Sistemas da Universidade Federal de Santa Catarina (UFSC) (Paulo M. Mafra,Joni da Silva Fraga,Vinícius Moll,2008)[1] e com a Pontifícia Universidade Católica do Paraná (PUC-PR)(Altair Olivo Santin,2008)[1], foi desenvolvido um sistema multicamadas chamado de POLVO-IIDS, utilizando redes neurais de Kohonen, que classifica os dados de forma genérica comportamentos considerados normais ou anômalo e para cada classe de ataque foi utilizada uma rede neural do tipo Support Vector Machine(SVM) especializada na detecção da classe correspondente e tendo como saída a indicação de trafego normal ou atividade maliciosa. A ideia de utilizar outra rede neural é utilizada para minimizar o número de falsos positivos, pois com apenas um tipo de ataque para classifica, aumenta a precisão para identificar apenas duas categorias trafego normal ou anomalia. O valor de cada neurônio pode variar de 0 a 1, normalmente em redes neurais de Kohonen algum neurônio deve estar de 0,1 a 0,9, mas no POLVO-IIDS, foi utilizado de 0,2 a 0,8 para evitar erro de algum possível ataque. O trabalho indica de teve uma melhora nos resultados obtidos relacionados a outras literaturas, mostrando que o modelo POLVO-IIDS é um modelo eficiente.

Um trabalho feito na Pontifícia Universidade Católica do Rio de Janeiro (Renato Maia Silva,Marco Antonio Grivet M. Maia)[2], demostra um teste de desempenho para algumas diferentes entradas para o treinamento de Redes neurais artificiais, utilizando 4 redes, apenas uma utiliza as 41 categorias diferentes, as outras 3 utilizam apenas 9 categorias básicas do TCP-IP, usando um intervalo de -1 a 1. A primeira rede utilizando todas as 41 categorias e a segunda rede com apenas 9 categorias com apenas uma saída, identificando como 1 ataque ou -1 normal, a terceira com apenas uma saída e 9 categorias, indicando como -1 normal, 0 neptune ou 1 smurf e a última com 4 saídas e 9 categorias, indicando (-1 1 1 1) normal, (1 -1 1 1) neptune, (1 1 -1 1) back e (1 1 1 -1) smurf. As taxas de acertos foram acima de 90% para todas as configurações testadas, a rede que teve um melhor resultado foi a terceira rede, tendo 97,5% na sua taxa de acertos.

Referencias

[1] http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st02\_02\_artigo.pdf

[2] Art019\_ssi04.pdf