Kappa-ARTMAP Fuzzy: uma metodologia para detecção de intrusos com seleção de atributos em redes de computadores

Nelcileno Virgílio de Souza Araújo[1], Ailton Akira Shinoda[2], Ruy de Oliveira[3], Ed'Wilson Tavares Ferreira[3], Valtemir Emerêncio do Nascimento[3]

[1]Instituto de Computação - Universidade Federal de Mato Grosso (UFMT) – Cuiabá, MT – Brasil

[2]Departamento de Engenharia Elétrica - Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP) - Ilha Solteira, SP – Brasil

[3]Departamento de Informática - Instituto Federal de Educação. Ciência e Tecnologia de Mato Grosso (IFMT) – Cuiabá, MT – Brasil

nelcileno@ic.ufmt.br,
shinoda@dee.feis.unesp.br,{ruy,ed,valtemir}@cba.ifmt.edu.br

Abstract. *The problem of intrusion detection in computer network has made several methodologies for intrusion detection systems that seek to reconcile two goals: high intrusion detection rate and low false alarm rate, but many of these techniques collide with the problem of dimensionality in worked training data, as a result, these solutions have a high computational cost. This paper introduces a methodology for intrusion detection with feature selection which applies Fuzzy ARTMAP network neural and Kappa coefficient to extract the most significant features from training data. The obtained results by our proposal can maintain a high rate of correct classification and face the problem of dimensionality using the Kappa coefficient, which is the main innovation this paper.*

Resumo. *O problema da detecção de intrusos numa rede de computadores tem produzido diversas metodologias para sistemas detectores de intrusão que procuram conciliar dois objetivos: alta taxa de detecção de intrusos e baixa taxa de falsos alarmes, mas muitas dessas técnicas esbarram no problema da dimensionalidade da base de treinamento a ser analisada, tornando essas soluções com um alto custo computacional. Neste artigo introduz-se uma metodologia de detecção de intrusos que emprega redes neurais ARTMAP Fuzzy e coeficiente Kappa por meio da seleção dos atributos mais significativos da base de treinamento. Os resultados obtidos pela nossa proposta consegue manter uma alta taxa de classificação correta e combate o problema da dimensionalidade por meio de um coeficiente de concordância para escalas nominais, sendo esta a principal inovação.*

1. Introdução

A detecção de intrusos tem sido utilizada em rede de computadores como uma ferramenta adicional no combate às ameaças de segurança [Wu e Banzhaf 2010]. Um conjunto de metodologias, que emprega redes neurais, computação evolucionária, conjuntos *fuzzy*, dentre outras técnicas, vem sendo desenvolvida nos sistemas detectores

de intrusão (IDS), mas o foco principal desses trabalhos são os algoritmos de detecção de intrusos. No entanto, devido ao crescimento da quantidade de informação trafegada numa rede, estes algoritmos de detecção sofrem com o problema do alto custo computacional para processá-los [Wu e Banzhaf 2010]. Este problema é comumente conhecido como a maldição da dimensionalidade, onde o conjunto de dados referente aos *logs* de rede coletados é representado por uma estrutura de dados muito dispendiosa para o processamento do dispositivo.

Neste sentido torna-se urgente a extração dos atributos mais representativos da base de treinamento para torná-la mais simples, contendo apenas as informações mais significativas para a detecção de ataques. Muitos trabalhos tem aplicado a técnica de seleção de atributos para pré-processar a base e dessa forma, torna a tarefa do algoritmo de detecção menos árdua, uma vez que a dimensionalidade da base é reduzida [Tsai *et al.* 2009].

A seleção de atributos procura extrair da base de treinamento os elementos mais significativos para a definição de um perfil, eliminando dos *logs* coletados aquelas características pouco representativas ou redundantes [Guyon e Elisseeff 2003]. Há três formas de implementação de seleção de atributos: filtro, que utiliza uma métrica independente para calcular a relevância dos atributos; envoltório, que explora algoritmos de aprendizagem de máquina para medir a importância de um ou vários atributos, com o objetivo de construir um subconjunto ótimo; e híbrido, que utiliza o método filtro na base de treinamento para selecionar os atributos candidatos e aplica o método envoltório para avaliar os atributos selecionados na criação do subconjunto ótimo. [Guyon e Elisseeff 2003].

Neste artigo apresenta-se uma metodologia de detecção de intrusos com seleção de atributos que aplica numa primeira fase o coeficiente Kappa [Cohen 1960] e o classificador ARTMAP *Fuzzy* [Carpenter *et al.* 1992] para avaliar e extrair os atributos mais representativos da base de treinamento e gerar um subconjunto ótimo que define dois tipos de comportamento no tráfego analisado: normal, tráfego gerado pelos clientes autorizados da rede, e anômalo, qualquer tráfego fora do comportamento considerado normal. A seguir, treina o classificador ARTMAP *Fuzzy* com o subconjunto ótimo gerado na primeira fase e aplica-o sobre uma base de teste para identificar os possíveis ataques existentes nos padrões de entrada submetidos.

O artigo está organizado da seguinte forma. Na segunda seção apresenta-se os principais artigos relacionados sobre seleção de atributos aplicado a detecção de intrusos. Na seção seguinte descreve-se a proposta de metodologia para pré-processamento e detecção de intrusos, evidenciando os conceitos téoricos sobre o coeficiente Kappa e as redes neurais ARTMAP *Fuzzy*. A terceira seção trata dos experimentos e resultados alcançados com a aplicação desta metodologia sobre a base de conhecimento KDD99 [Lippmann *et al.* 2000]. Por último, realizam-se as devidas conclusões obtidas com esta investigação e sugerem-se os trabalhos futuros na continuação dessa pesquisa.

2. Trabalhos Relacionados

Nesta seção abordam-se os principais trabalhos relacionados que empregam seleção de atributos para detecção de intrusos. As propostas apresentadas por [Alazab *et al.* 2012],

[Om e Kundu 2012], [Li *et al.* 2012] e [Sindhu, Geetha e Kannan 2012] foram realizadas sobre a base de conhecimento do KDD99 [Lippmann *et al.* 2000].

Em [Alazab *et al.* 2012], o ganho de informação é a métrica de relevância aplicada na seleção de atributos para gerar o subconjunto ótimo e emprega-se a árvore de decisão como algoritmo de detecção de intrusos. Na metodologia apresentada em [Om e Kund, 2012], os atributos mais representativos são selecionados por meio da Entropia, a seguir o algoritmo *k-means* é utilizado para agrupar os registros do subconjunto ótimo em cinco grupos e, então, submetê-los para o treinamento do classificador híbrido baseado nas técnicas *naives bayes* e *k-nearest neighboor* para a detecção de intrusos. Os autores da proposta [Li *et al.* 2012] desenvolveram uma série de estratégias de aprendizagem de máquina num único IDS, composto pelas técnicas de agrupamento *k-means*, otimização por colônia de formigas e máquinas de vetores de suporte (SVM). O subconjunto ótimo de atributos é extraído pela aplicação do algoritmo de remoção de atributos gradual. A estratégia relatada em [Sindhu, Geetha e Kannan 2012] utiliza um IDS com classificação multiclasse. A arquitetura trabalha em cima de três perspectivas. Em primeiro lugar, os padrões de tráfego de entrada são pré-processados e os atributos redundantes são removidos. A seguir, um algoritmo de seleção de atributos baseado em algoritmos genéticos é aplicado para que tenha um maior impacto na minimização da complexidade computacional do classificador. Por último, um modelo de árvore neural é empregado como máquina de classificação.

Nas propostas de IDS apresentadas em [Alazab *et al.* 2012], [Om e Kundu 2012], [Li *et al.* 2012] e [Sindhu, Geetha e Kannan 2012] observam-se a tendência em classificar os ataques no modo multi-classe, bem como o uso de técnicas de aprendizado de máquina em série. A principal diferença da nossa proposta é aplicar o coeficiente Kappa como métrica de relevância do atributo. Além disso, procura-se no trabalho dar um enfoque em detectar as anomalias na base de treinamento e não na classificação por ataque, por isso trabalha-se apenas com dois perfis de tráfego: normal e anomalia. O enfoque na detecção de intrusos tem como principal objetivo tornar o IDS mais rápido, uma vez que a classificação por ataque exige um custo computacional mais alto devido ao emprego de uma série de técnicas de aprendizado de máquina [Wu e Banzhaf 2010] [Tsai *et al.* 2009].

3. Metodologia proposta para detecção de intrusos

Nesta seção relata-se a arquitetura proposta para tratar o problema da detecção de intrusos, mas primeiramente é descrito um levantamento teórico sobre as técnicas envolvidas no desenvolvimento dessa metodologia.

3.1. Seleção de atributos

Em domínios mais complexos de classificação de padrões, algumas características podem ser redudantes, visto que a informação contida nelas podem já existir em outros atributos. Esta redudância de informação pode aumentar o custo computacional do IDS, uma vez que a quantidade de atributos existentes na base de treinamento influencia o número de processamentos necessários para executá-la [Tsai *et al.* 2009]. A seleção de atributos enfrenta este problema, buscando um subconjunto de atributos que melhor representa os padrões de comportamento existente na base de treinamento.

Neste artigo propõe-se uma metodologia de seleção de atributos que, primeiramente, avalia cada atributo da base de treinamento (S) por meio do classificador ARTMAP *Fuzzy* e gera uma matriz de confusão contendo as amostras (normal e anomalia) identificadas corretamente e incorretamente. No passo seguinte calcula o coeficiente Kappa de cada matriz de confusão gerada pela avaliação dos atributos e armazena num vetor chamado de vetor dos coeficientes Kappa (V_{Kappa}). A seguir, emprega a estratégia de busca SFS (*Sequential Forward Search*) [Guyon e Elisseeff 2003] para remover a cada iteração do vetor V_{Kappa} o atributo com maior coeficiente Kappa e adiciona-o no subconjunto de atributos candidatos ($S_{candidatos}$). Logo após, o classificador ARTMAP *Fuzzy* e o cálculo do coeficiente Kappa são aplicados, novamente, para avaliar a taxa de classificação correta e incorreta conseguida pelo subconjunto de atributos candidatos. Na próxima etapa verifica se o coeficiente Kappa de $S_{candidatos}$ é o maior valor alcançado dos subconjuntos avaliados. Caso a resposta seja afirmativa, o subconjunto ótimo ($S_{ótimo}$) armazena os atributos de $S_{candidatos}$. A condição de parada da busca SFS ocorre quando o V_{Kappa} estiver vazio. Após esse processamento, o subconjunto ótimo ($S_{ótimo}$) contém o agrupamento de atributos candidatos que possui o maior coeficiente Kappa entre os subconjuntos testados no algoritmo. A Figura 1 descreve os passos executados nesta metodologia proposta.

3.2. Rede neural ARTMAP *Fuzzy*

O classificador ARTMAP *fuzzy* é uma rede neural artificial incremental onde aplica-se a teoria da ressonância adaptativa para que não seja necessário recomeçar o treinamento para cada novo padrão de entrada e que o conhecimento previamente obtido seja conservado e estendido [Carpenter *et al.* 1992].

A arquitetura da rede ARTMAP *fuzzy* é composta por dois módulos ART_a nebuloso e ART_b nebuloso, que possuem a mesma estrutura da rede neural ART1 usando as operações envolvidas na lógica *fuzzy* [Carpenter, Grossberg e Rosen 1991]. Eles são interligados por um módulo conhecido como inter-ART que controla o treinamento de um mapa associativo de categorias de reconhecimento da ART_a para categorias de reconhecimento da ART_b. O inter-ART combina os parâmetros de entrada com os parâmetros de saída através do *match tracking*, de forma a maximizar a generalização das categorias de reconhecimento e minimizar o erro da rede [Carpenter *et al.* 1992] [Carpenter, Grossberg e Rosen 1991].

O algoritmo desta rede neural consiste nos seguintes passos [Carpenter *et al.* 1992][Carpenter, Grossberg e Rosen 1991]:

Passo 1: Normalizar os vetores de entrada ART_a e de saída ART_b, se necessário: Inicialmente, todos os valores dos neurônios devem ser normalizados se não estiverem entre 0 e 1.

Passo 2: Codificar os vetores dos módulos ART_a e ART_b: Um novo padrão de entrada deve sofrer uma codificação complementar preliminar para se preservar a amplitude da informação.

Passo 3: Iniciar os pesos e parâmetros dos módulos ART_a, ART_b e Inter-ART: Deve-se iniciar os pesos (valor 1 = todas as categorias desativadas), taxa de treinamento (β entre 0 e 1), parâmetro de escolha ($\alpha > 0$) e parâmetro de vigilância (ρ_a, ρ_b e ρ_{ab} entre 0 e 1);

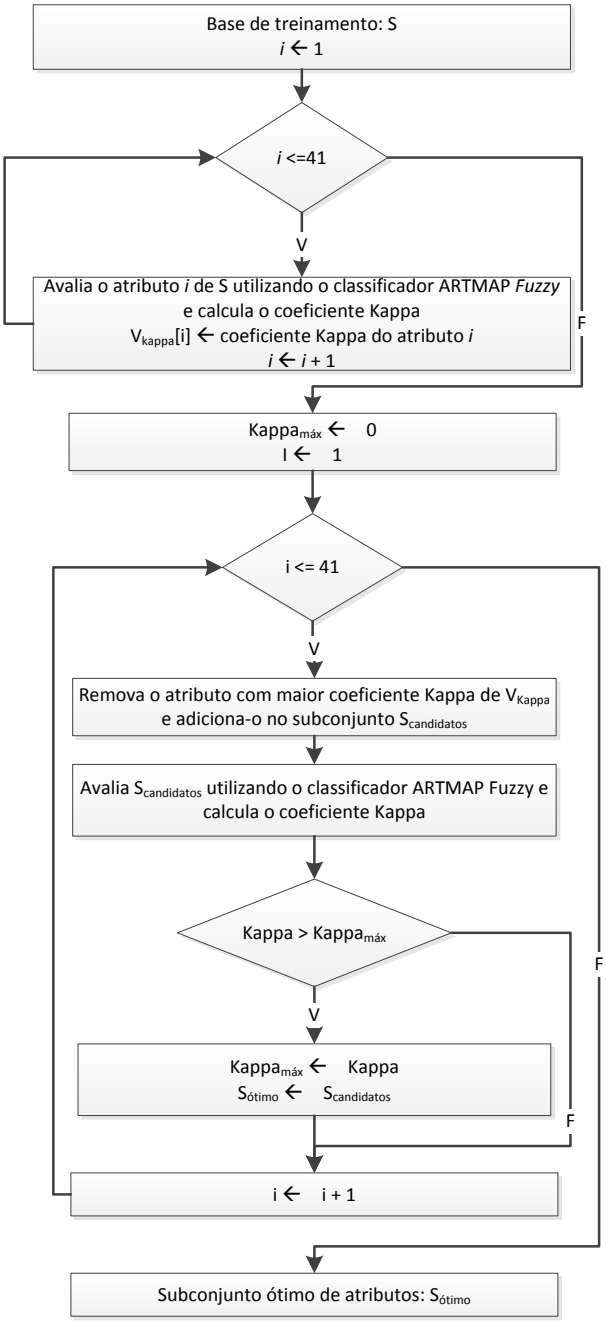

Figura 1. Fluxograma da metodologia de seleção de atributos proposta

Passo 4: Escolha da categoria para os módulos ART_a e ART_b: Se mais de um neurônio está ativo, é escolhido aquele com o maior índice de ordenação (maior valor).

Passo 5: Teste de vigilância dos módulos ART_a e ART_b: A ressonância ocorre se é satisfeito o critério de vigilância. Caso contrário, se o critério de vigilância falhar para a categoria escolhida, ocorre o *reset* e um novo índice é escolhido (retornar ao passo 4). O processo de busca se repete até que o índice escolhido satisfaça o teste de vigilância.

Passo 6: *Match tracking* (teste de ressonância) entre os módulos ART_a e ART_b: Verificação se houve associação da entrada com a saída. Se não houver associação deve-se procurar outro índice que satisfaça o teste;

Passo 7: Adaptação dos pesos: O vetor dos módulos ART_a, ART_b e inter-ART são atualizados com os novos pesos.

Passo 8: Repetir passos 4 à 7 para todos os pares a serem treinados.

3.3. Coeficiente Kappa

A avaliação dos atributos da base de treinamento aplicando o classificador ARTMAP *Fuzzy* gera uma estrutura conhecida como matriz de confusão. A matriz de confusão [Wu e Banzhaf 2010] apresenta informações sobre as classificações corretas e previstas realizadas pelo sistema de classificação. O desempenho do classificador, normalmente, é avaliado usando os dados contidos nesta matriz. A Tabela 1 é uma representação da matriz de confusão do problema de detecção de intrusos.

As entradas da matriz de confusão possuem os seguintes significados no contexto do nosso estudo: Verdadeiro Positivo (TP) - identifica uma atividade intrusiva corretamente; Verdadeiro Negativo (TN) - identifica uma atividade não-intrusiva corretamente; Falso Positivo (FP): identifica uma ação não-intrusiva como sendo intrusiva; Falso Negativo (FN): identifica uma atividade intrusiva como sendo não-intrusiva.

Tabela 1 - Matriz de confusão do problema de detecção de intrusos

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Classe prevista</td><td rowspan="2">Total</td></tr>
<tr><td>Classe negativa (Normal)</td><td>Classe positiva (Anomalia)</td></tr>
<tr><td rowspan="2">Classe real</td><td>Classe negativa (Normal)</td><td>Verdadeiro Negativo (TN)</td><td>Falso Positivo (FP)</td><td>l_1 = TN+FP</td></tr>
<tr><td>Classe positiva (Anomalia)</td><td>Falso Negativo (FN)</td><td>Verdadeiro Positivo (TP)</td><td>l_2 = FN+TP</td></tr>
<tr><td colspan="2">Total</td><td>c_1 = TN+FN</td><td>c_2 = FP+TP</td><td>Total de unidades classificadas (N)</td></tr>
</table>

Para avaliar o desempenho do classificador na detecção de intrusos, diversas métricas têm sido calculadas a partir das entradas oferecidas pela matriz de confusão, entre as mais empregadas na área de sistemas detectores de intrusão [Wu e Banzhaf 2010] pode-se citar:

- Taxa de detecção ($\frac{TP}{FN+TP}$) - proporção de atividades intrusas classificadas corretamente;
- Taxa de falsos alarmes ($\frac{TN}{TN+FP}$) - proporção de atividades normais classificadas incorretamente como intrusas;
- Exatidão global ($\frac{TN+TP}{N}$) – proporção da quantidade de previsões que foram classificadas corretamente;

- Precisão ($\frac{TP}{FP+TP}$) – proporção de atividades intrusas previstas que foram corretamente identificadas.

Contudo, este artigo adota uma nova métrica de avaliação conhecida como coeficiente de correlação Kappa.

O coeficiente Kappa é uma métrica de concordância introduzida, primeiramente, entre observadores da área de psicologia [Cohen 1960]. A intenção original de Kappa era medir o nível de concordância ou discordância de um grupo de pessoas observando um mesmo fenômeno [Cohen 1960].

Para o problema da detecção de intrusos, o coeficiente Kappa mede a proporção de concordância observada (P_o) entre as classes de comportamentos existentes (classe real) e calculadas (classe prevista) sobre a base de treinamento após ser removida a proporção de concordância devido ao acaso (P_a), representada pelas Equações (1), (2) e (3).

$$k = \frac{P_o - P_a}{1 - P_a} \quad (1)$$

$$P_o = \frac{TN+TP}{N} \quad (2)$$

$$P_a = \frac{(c_1 * l_1)+(c_2 * l_2)}{N} \quad (3)$$

A interpretação do valor calculado *k* dar-se-á da seguinte forma: quanto mais próximo de zero for *k*, significa que as unidades classificadas ocorreram ao mero acaso, por outro lado quando *k* aproxima-se de 1, a concordância entre as classes corretas e previstas tende ao exato [Cohen 1960].

A escolha pelo coeficiente Kappa como métrica para selecionar os atributos mais relevantes da base de treinamento e para avaliar a qualidade da classificação do IDS deve-se as métricas, exatidão global e precisão, serem inapropriadas em aplicações onde as classes são desigualmente representadas na base de treinamento [Kubat, Holte e Matwin 1998]. A Tabela 2 mostra esta situação onde a quantidade de amostras normais contida na base de treinamento representa 98% do espaço amostral e o restante, corresponde as amostras anômalas. Pode-se observar que apesar de uma taxa de detecção de 2%, as métricas exatidão global e precisão apresentam valores os quais demonstram, equivocadamente, o sucesso do classificador avaliado, diferentemente do coeficiente Kappa que evidencia a ineficiência do classificador.

3.4. Modelo proposto para o Sistema de Detecção de Intrusos

A Figura 2 mostra o diagrama de blocos da metodologia de detecção de intrusos proposta neste trabalho. Na primeira fase ocorre o pré-processamento de dados, onde aplica-se a seleção de atributos para extrair as características mais significativas da base de treinamento, utilizando o coeficiente Kappa como métrica de relevância, o classificador ARTMAP *Fuzzy* para avaliar os atributos selecionados e a busca SFS para gerar o subconjunto ótimo.

Tabela 2 - Matriz de confusão e métricas de avaliação para uma base de treinamento com espaço amostral desigualmente dividido entre as classes de comportamento

		Classe prevista		Total
		Classe negativa (Normal)	Classe positiva (Anomalia)	
Classe Real	Classe negativa (Normal)	2450	0	$l_1 = 2450$
	Classe positiva (Anomalia)	49	1	$l_2 = 50$
Total		$c_1 = 2499$	$c_2 = 1$	2500

Taxa de detecção = 2%
Taxa de falsos alarmes = 0%
Exatidão global = 98,04%
Precisão = 100%
Kappa = 0,038

Após os dados serem pré-processados inicia-se a fase de reconhecimento de intrusão, onde o subconjunto ótimo de atributos é submetido para treinar o classificador ARTMAP *Fuzzy*, que detecta se as atividades apresentadas ao classificador são atividades de tráfego dos clientes pertencente à rede (classe normal) ou atividades não autorizadas criadas por clientes maliciosos (classe anomalia). Por fim, avalia-se o IDS com a base de teste.

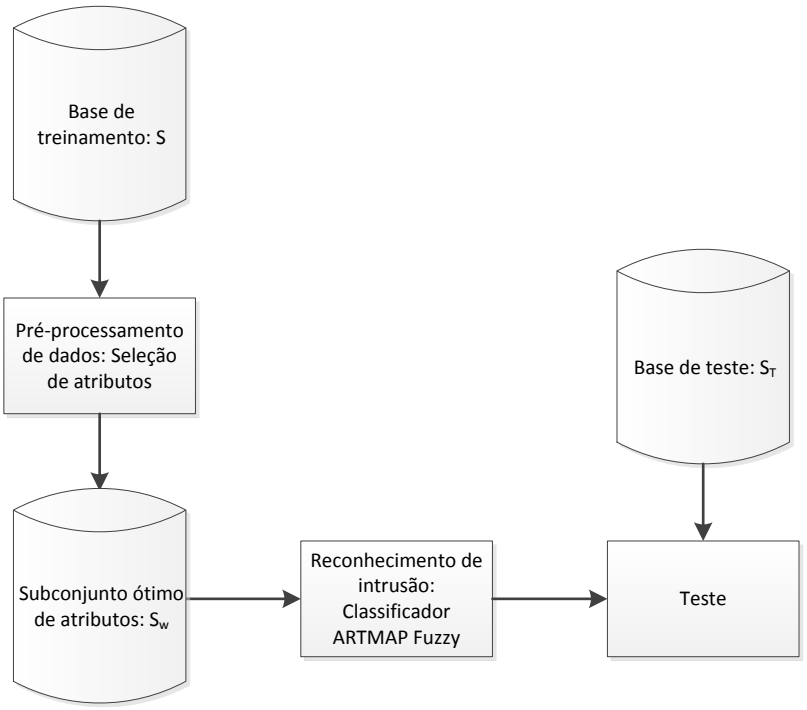

Figura 2. Diagrama de blocos da solução proposta.

4. Experimentos e Resultados

Na primeira parte desta seção relata-se a metodologia utilizada para realizar a avaliação do IDS Kappa-ARTMAP *Fuzzy* e, logo após, apresentam-se os resultados obtidos nos experimentos e suas respectivas análises.

4.1. Metodologia

O banco de dados escolhido para os experimentos é a base de dados KDD99 [6]. Apesar de ser relativamente antiga, e incluir poucos ataques contra sistemas baseados em UNIX e em roteadores CISCO, a KDD99 [Lippmann *et al.* 2000] é uma base de dados amplamente utilizada por pesquisadores para avaliar algoritmos de detecção de intrusão e aprendizagem de máquina [Wu e Banzhaf 2010].

A Tabela 3 apresenta a composição da base KDD99. O subconjunto 10%KDD99, normalmente, desempenha o papel de base de treinamento numa avaliação de IDS, possui uma maioria de amostras representando atividades intrusivas e representa uma versão concisa da base completa *Whole* KDD99 [Lippmann *et al.* 2000]. A base *Corrected* KDD99 tem como principal característica a inserção de novos padrões de ataques que não aparecem nas outras bases de detecção do KDD99 [Lippmann *et al.* 2000].

A base de treinamento empregada nos experimentos é um conjunto de 10000 amostras retiradas da base 10%KDD99, respeitando a representatividade das 22 classes de ataques existentes e a classe normal.

Tabela 3 – Classes de comportamentos dos subconjuntos de detecção de intrusos da base KDD99 em termo do número de amostras

Base de Dados	Normal	Anomalia	Total de amostras
10% KDD99	97277	396743	494020
Corrected KDD99	60593	250436	311029
Whole KDD99	972780	3925650	4898430

Para analisar o desempenho do IDS proposto aplica-se o método de exatidão preditiva *10 fold cross-validation* [Fielding e Bell 1997] sobre a base de treinamento, onde ocorre um particionamento da base em 10 subconjuntos com 1000 amostras. Em cada iteração, uma das 10 partições geradas representa a base de teste e as 9 partições restantes representam a base de treinamento. A exatidão preditiva é calculada pela média dos percentuais de acerto das 10 iterações.

Os parâmetros do classificador ARTMAP *fuzzy* empregado na arquitetura de detecção de intrusos concebida são apresentados na Tabela 4. A utilização destes valores deve-se por empregar na rede neural um treinamento rápido (β=1), bem como, configurar o classificador para ser bastante sensível a alterações nos padrões de entrada que levam a uma boa decisão de classificação (ρ próximo de 1) [Huang, Georgiopoulos e Heileman 1995].

Todas as simulações foram realizadas por meio da ferramenta de programação MATLAB [The Mathworks 2008] que mostrou-se bastante eficiente no desenvolvimento da solução proposta.

Tabela 4 – Parâmetros de configuração usados no classificador ARTMAP Fuzzy.

Parâmetros	Valor
Parâmetro de escolha (α)	0,001
Taxa de treinamento (β)	1
Parâmetro de vigilância da rede $ART_a(\rho_a)$	0,99
Parâmetro de vigilância da rede $ART_b(\rho_b)$	0,9
Parâmetro de vigilância do módulo inter-ART(ρ_{ab})	0,99

4.2. Resultados obtidos

Primeiramente, aplica-se a técnica de seleção de atributos Kappa-ARTMAP *Fuzzy* na base de treinamento para extrair as características mais significativas. A Figura 3 mostra a avaliação do subconjunto de atributos candidatos, após cada busca SFS, até atingir a dimensão original (41 atributos). O subconjunto ótimo de atributos é atingido quando o subconjunto de atributos candidatos contém os 3 atributos mais significativos da base de treinamento.

Além disso, na Figura 3 fica bem evidenciado que a utilização do coeficiente Kappa, como métrica de relevância, na extração dos elementos para o subconjunto ótimo, mostra-se bastante efetiva, pois consegue processar uma base de treinamento desequilibrada nas classes de comportamento representadas e gera um subconjunto ótimo bem reduzido (3 atributos), que resultará uma diminuição no custo computacional do IDS. O subconjunto ótimo extraído é formado pelos atributos: *logged in*, *dst bytes* e *src bytes*.

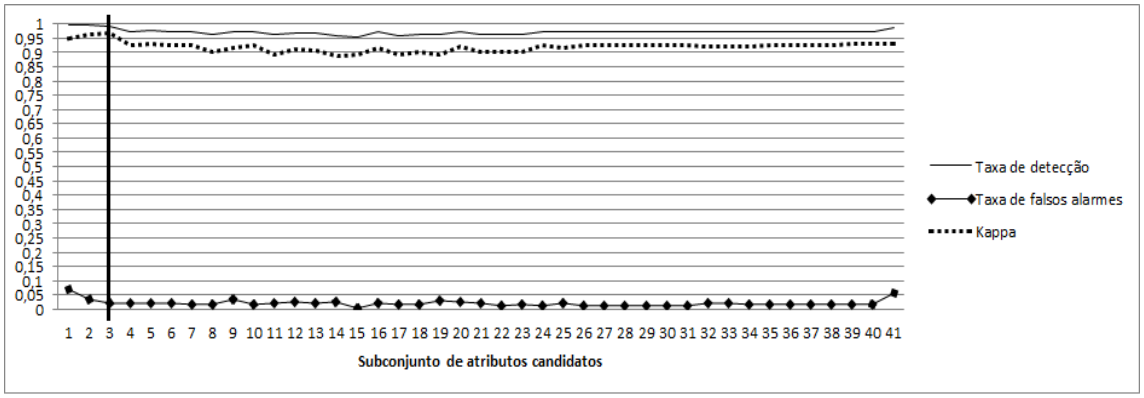

Figura. 3. Avaliação do subconjunto de atributos candidatos após cada busca SFS na base de treinamento

A Tabela 5 reitera a importância de aplicar seleção de atributos na base de treinamento, pois os resultados obtidos entre a base original e a base pré-processada mostram que uma base de dados sem pré-processamento prejudica a capacidade de detecção do IDS.

Na Tabela 6 avalia-se o desempenho da solução proposta comparando-a com as arquiteturas de IDS com seleção de atributos empregadas em [Alazab *et al.* 2012], [Om e Kundu 2012], [Li *et al.* 2012] e [Sindhu, Geetha e Kannan 2012], uma vez que são os autores estudados no levantamento dos trabalhos produzidos nesta aréa. Os valores apresentados demonstram a viabilidade da nossa proposta, pois as métricas de desempenho (taxa de detecção, taxa de falsos alarmes e exatidão geral) obtem

resultados muito próximos das outras soluções, com a vantagem de utilizar uma quantidade de atributos mais reduzida do que os outros modelos estudados.

Tabela 5 – Avaliação de desempenho do classificador ARTMAP *Fuzzy* para 41 atributos e os 3 atributos do subconjunto ótimo.

Nº de atributos	Taxa de Detecção (DR)	Taxa de Falsos Alarmes (FPR)	Exatidão Global	Precisão	Kappa
41 atributos	98,79%	5,91%	97,86%	98,54%	0,9323
3 atributos	99,24%	2,27%	98,94%	99,43%	0,9667

A principal deficiência da técnica Kappa-ARTMAP *Fuzzy* expressa-se na taxa de falsos alarmes, onde o valor alcançado é o maior do grupo de modelos avaliados. Uma possível razão para este problema pode ser o uso de parâmetros da rede neural ARTMAP *Fuzzy* que tornam a sintonia do reconhecimento de intrusão bastante sensível, gerando um número maior de falsos alertas. Apesar disso, devido à taxa de detecção ser bastante alta, a exatidão global obtida é a segunda maior dos IDS analisados.

Tabela 6 – Comparação de desempenho de arquiteturas IDS com seleção de atributos.

Modelo	Nº de atributos	Taxa de Detecção (DR)	Taxa de Falsos Alarmes (FPR)	Exatidão Global
J48 [Alazab *et al.* 2012]	12	98,04%	1,53%	98,22%
K-means+K-NN+Bayes [Om e Kundu 2012]	-	98,18%	0,83%	99,00%
GFR [Li *et al.* 2012]	19	97,06%	0,49%	98,62%
NeuroTree [Sindhu, Geetha e Kannan 2012]	16	97,91%	1,3%	98,38%
Kappa-ARTMAP *Fuzzy*	3	99,24%	2,27%	98,94%

5. Conclusões

Os resultados apresentados demonstram a viabilidade da técnica Kappa-ARTMAP *Fuzzy*, tanto na seleção de atributos mais relevantes da base de treinamento como na tarefa de detecção de intrusos. A dimensão do subconjunto ótimo, contendo apenas 3 atributos, produz uma redução considerável no custo computacional, bem como, o índice Kappa apresenta-se como uma métrica de relevância bastante interessante pois consegue conciliar uma base de treinamento reduzida sem afetar as métricas de desempenho do IDS.

Como continuação desse trabalho, pretende-se investigar técnicas que possam reduzir a taxa de falsos alarmes do IDS e estender essa arquitetura de detecção de intrusos para outras bases de treinamento que englobem outras tecnologias de rede, tais como: redes sem fio, redes sensores sem fio, redes móveis.

Agradecimentos

Esta pesquisa foi parcialmente apoiada pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e pela Fundação de Amparo à Pesquisa do Estado de Mato Grosso (FAPEMAT).

Referências

Alazab, A., Hobbs, M., Abawajy, J. e Alazab, M. (2012) "Using feature selection for intrusion detection system", Proceedings of International Symposium on Communications and Information Technologies (ISCIT), p.296-301.

Carpenter, G. A., Grossberg, S., Markuzon, N., Reynold, J. H. e Rosen, D. B. (1992) "Fuzzy ARTMAP: A neural network for incremental supervised learning of analog multidimensional maps", IEEE Transactions on Neural Network, vol. 3, n. 5, p. 689-713.

Cohen, J. (1960) "A coefficient of agreement for nominal scales", In *Educational and Psychological Measurement*, vol. 20, no. 1, p. 37-46, 1960.

Fielding, A. H. e Bell, J. (1997) "A review of methods for the assessment of prediction errors in conservation presence/absence models", In *Environmental Conservation*, vol. 24, n. 1, p. 38-49.

Guyon, I. e Elisseeff, A. (2003) "An introduction to variable and feature selection", Journal of Machine Learning Research, vol.3, p.1157–1182.

Huang, J., Georgiopoulos, M. e Heileman, G. (1995) "Fuzzy ART Properties", In *Neural Networks*, vol. 8, n. 2, p. 203-213.

Kubat, M., Holte, R. C. e Matwin, S. (1998) "Machine learning for the detection of oil spills in satellite radar images", In *Machine Learning*, vol. 30, n. 2-3, p. 195–215.

Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X. e Dai, K. (2012) "An efficient intrusion detection system based on support vector machines and gradually feature removal method", In *Expert Systems with Applications*, vol. 39, n. 1, p. 424-430.

Lippmann, R., Haines, J. W., Fried, D. J., Korba, J. e Das, K. (2000) "The 1999 DARPA off-line intrusion detection evaluation", In *Computer Networks*, vol.34, n.4, p. 579-595.

Om, H. e Kundu, A. (2012) "A hybrid system for reducing the false alarm rate of anomaly intrusion detection system", Proceedings of the 1st International Conference on Recent Advances in Information Technology (RAIT), p.131-136.

Sindhu, S. S. S., Geetha, S. e Kannan, A. (2012) "Decision tree based light weight intrusion detection using a wrapper approach", In *Expert Systems with Applications*, vol. 39, n. 1, p. 129-141.

The Mathworks (2008) "Matlab 7 Getting Started Guide".

Tsai, C., Hsu, Y., Lin, C. e Lin, W. (2009) "Intrusion detection by machine learning: A review", In *Expert Systems with Applications*, vol. 36, n. 10, p. 11994-12000.

Wu, S. e Banzhaf, W. (2010) "The Use of Computational Intelligence in Intrusion Detection Systems: A Review", In *Applied Soft Computing*, vol.10, p. 1-35.