Comparando Seleção de Atributos na Detecção de Ataques DoS Hulk e DoS GoldenEye

Marcos G. Barbosa[1], Matheus R. Sapata[1], André Riker[2], Bruno L. Dalmazo[1]

[1] Centro de Ciências Computacionais
Universidade Federal do Rio Grande (FURG) – Rio Grande, RS – Brasil

[2]Universidade Federal do Pará (UFPA) – Belém, PA – Brasil

marcosgabriel@furg.br, matheussapata@furg.br, ariker@ufpa.br, dalmazo@furg.br

Abstract. *Computer networks are essential for performing a wide range of indispensable activities in daily life. However, they are subject to vulnerabilities arising from the transmission of unprotected data and the inadequate implementation of security protocols, leading to risks such as unauthorized data disclosure and interruption of critical services. In light of this reality, the present study proposes a comparative analysis of attribute selection for the detection of DoS Hulk and DoS GoldenEye attacks through a MultiClass Classifier. The goal is to determine the effectiveness of each technique in identifying these attacks, which are considered network anomalies.*

Resumo. *Redes de computadores são fundamentais para a realização de uma ampla gama de atividades indispensáveis no cotidiano. No entanto, estão sujeitas a vulnerabilidades derivadas da transmissão de dados não protegidos e da implementação inadequada de protocolos de segurança, levando a riscos como a divulgação não autorizada de dados e a interrupção de serviços críticos. Diante dessa realidade, esse estudo propõe uma análise comparativa de seleção de atributos para a detecção de ataques DoS Hulk e DoS GoldenEye através de um Classificador MultiClass. O objetivo é determinar a eficácia de cada técnica em identificar esses ataques, que são considerados anomalias na rede.*

1. Introdução

A ubiquidade das redes de computadores na vida cotidiana é inegável, abrangendo desde momentos de entretenimento até atividades de trabalho. No entanto, essa constante transmissão de dados pode resultar em sérios problemas se não estiver devidamente protegida, incluindo vazamentos de dados pessoais e interrupções nos serviços [Dalmazo et al. 2018, Dalmazo et al. 2021]. Para aprimorar a eficácia dos classificadores na detecção de ataques, a seleção de atributos é uma abordagem valiosa. Ela envolve a escolha dos atributos mais relevantes para melhorar o desempenho dos sistemas de segurança da rede. Este estudo explora e compara diversas técnicas de seleção de atributos na detecção de ataques DoS Hulk e DoS GoldenEye, usando um Classificador Multiclasse, visando aprimorar a segurança de redes contra essas ameaças.

O objetivo deste estudo é avaliar a eficácia das técnicas de seleção de atributos na detecção de anomalias na rede, usando o conjunto de dados CICIDS2017 [Sharafaldin et al. 2018]. O foco é identificar quais técnicas oferecem melhor desempenho e economia de tempo, sem comprometer significativamente a capacidade de detecção

de ataques. As próximas seções detalham os trabalhos relacionados, a proposta, a implementação, algumas considerações finais e perspectivas de trabalhos futuros.

2. Trabalhos Relacionados

No trabalho proposto por [Jabez and Muthukumar 2015], o objetivo principal é desenvolver um Sistema de Detecção de Intrusão (IDS) que faça uso da detecção de outliers, especialmente através da avaliação do conjunto de dados de anomalias utilizando o Neighbourhood Outlier Factor (NOF). O IDS foi projetado para lidar com grandes conjuntos de dados distribuídos, visando melhorar seu desempenho. Os resultados dos testes realizados com o conjunto de dados KDD revelaram que o IDS proposto superou abordagens anteriores, conseguindo identificar a maioria das anomalias de forma eficiente.

Em [Kasongo and Sun 2019], um Sistema de Detecção de Intrusão (IDS) com foco em sistemas sem fio. A abordagem incluiu a normalização de recursos, convertendo características em valores numéricos e ajustando-os para melhorar o desempenho. Além disso, utilizou-se a técnica Information Gain para selecionar recursos relevantes na detecção de intrusões em sistemas wireless.

Em [Vinayakumar et al. 2019], foi utilizado o método DNN, um tipo de modelo de aprendizagem profunda, com o intuito de desenvolver um IDS flexível para detectar e classificar ataques cibernéticos imprevisíveis e previsíveis. O modelo proposto foi testado em mais de um *dataset* como por exemplo o KDD Cup 99 e o CICIDS2017, um dos grandes diferenciais desta proposta é a escalabilidade e a possibilidade da detecção de ataques em tempo real ou não.

Em [Thaseen and Kumar 2017], um modelo de detecção de intrusão foi proposto, utilizando seleção de características do qui-quadrado e SVM multiclasse, otimizado por ajustes nos parâmetros do kernel da Função de Base Radial. Esta inovação resultou em redução do tempo de treinamento e testes e aumento da precisão na detecção de ataques, comprovado pelo desempenho superior no conjunto de dados NSL-KDD.

3. Proposta

Este estudo avalia a eficácia de três técnicas de seleção de atributos na detecção de anomalias: Information Gain, OneR e Análise de Componentes Principais (PCA). O primeiro atribui pesos com base na entropia para avaliar a relevância das features. Já o OneR elabora regras individuais para cada atributo e seleciona aqueles que minimizam o erro [Novakovic et al. 2011]. A Análise de Componentes Principais (PCA) gera novas features para compreender dados complexos. O estudo compara essas técnicas, considerando sua eficácia na detecção de anomalias e sua relação com o ganho de tempo e precisão.

3.1. Modelo Conceitual

Realizamos um estudo em sete etapas para avaliar a eficácia das técnicas de seleção de atributos na detecção de anomalias em redes. Na Etapa 1, escolhemos um conjunto de dados diversificado, enfatizando sua qualidade e diversidade. Na Etapa 2, eliminamos recursos redundantes após uma análise detalhada. A Etapa 3 envolveu a divisão dos dados em treinamento (70%) e teste (30%) para garantir uma análise eficaz. As Etapas 4 e 5 consistiram na aplicação de técnicas de seleção de recursos e na coleta de resultados. Na Etapa 6, aplicamos os resultados a um classificador MultiClassClassifier, obtendo

métricas valiosas. Finalmente, na Etapa 7, analisamos as métricas em tabelas e gráficos, comparando as técnicas de seleção de atributos para identificar as mais eficazes, considerando a relação entre precisão na detecção e tempo de processamento. A Figura 1 ilustra a base fundamental deste modelo de avaliação, oferecendo uma visão detalhada de seus estágios. Ela expõe todas as etapas deste processo, seus principais componentes e interações.

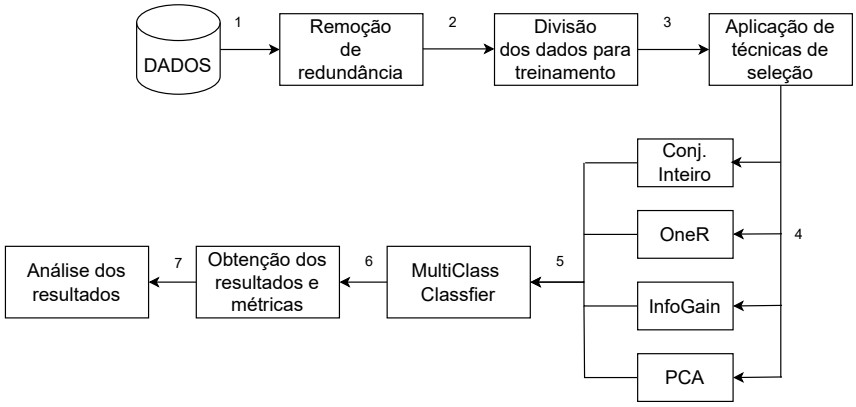

Figura 1. Modelo conceitual

3.2. Dataset Utilizado

O conjunto de dados CICIDS2017 [Sharafaldin et al. 2018] é notável por sua inclusão de ataques atualizados e benignos, mimetizando com precisão as condições do mundo real com dados em formato PCAP. Este conjunto é enriquecido com resultados analíticos derivados do tráfego de rede.

Para o modelo proposto, utilizamos o conjunto de dados MachineLearningCSV, composto por 77 features e uma label, extraídas dos arquivos de DUMP do Dataset CICIDS2017 [Sharafaldin et al. 2018]. Este conjunto abrange 8 sessões de monitoramento ao longo de uma semana, com tráfego normal (“Benigno”) e tráfego de ataques, incluindo 14 tipos diferentes de ataques. Focamos nos ataques DoS Hulk e DoS GoldenEye, que se destacaram nesse conjunto de dados, registrado em 5 de julho de 2017, contendo aproximadamente 640 mil instâncias. A Tabela 1 ilustra o conjunto de ataques no dia analisado.

Tipo de Ataque	Data	Número de Instâncias
DoS slowloris	05/07/2017	5.796
DoS slowhttptest	05/07/2017	5.499
DoS Hulk	05/07/2017	231.073
DoS GoldenEye	05/07/2017	10.293
Heartbleed	05/07/2017	11

Tabela 1. Tabela de tipos de ataques, datas de registro e número de instâncias

4. Avaliação

Para demonstrar a viabilidade técnica da proposta, avaliamos o classificador e as técnicas de seleção de atributos escolhidas. No primeiro cenário, utilizamos o conjunto de dados

completo e aplicamos um script em Python para remover as features redundantes identificadas. Posteriormente, aplicamos esses dados ao classificador. Os resultados dessa avaliação estão resumidos na Tabela 2.

Tipo de Ataque	TP	FP
Benigno	0.996	0.002
DoS Hulk	0.999	0.004
DoS GoldenEye	0.988	0.000

Tabela 2. Resultados sem seleção de atributos

Os resultados indicam que ao utilizar o conjunto de dados completo, alcançamos taxas de verdadeiros positivos superiores a 98% e taxas de falsos positivos inferiores a 1%, demonstrando um desempenho excepcional na detecção de ataques à rede.

4.1. Classificador com InfoGain

No segundo cenário, aplicamos a técnica de seleção de atributos InfoGain, que atribui pesos às features para classificá-las por relevância. Selecionamos as 15 features mais relevantes, e os resultados obtidos foram satisfatórios, como evidenciado a seguir.

Tipo de Ataque	TP	FP
Benigno	0.981	0.225
DoS Hulk	0.800	0.018
DoS GoldenEye	0.699	0.001

Tabela 3. Resultados com InfoGain

Observa-se que ao aplicar esta técnica de seleção de atributos, já não obteve-se resultados tão satisfatórios em comparação ao conjunto sem seleção de atributos. Obteve-se taxas de verdadeiro positivo de 80% e 69.9% para os ataques Hulk e GoldenEye respectivamente.

4.2. Classificador com OneR

No terceiro cenário, ao usar o MultiClassClassifier no conjunto de atributos selecionados, obtivemos os resultados apresentados abaixo.

Tipo de Ataque	TP	FP
Benigno	0.990	0.137
DoS Hulk	0.873	0.010
DoS GoldenEye	0.839	0.001

Tabela 4. Resultados com OneR

Neste contexto, é notável que, comparado com a técnica anterior, já alcançamos resultados promissores. Registramos taxas de verdadeiro positivo de 87,3% para ataques do tipo Hulk e 83,9% para GoldenEye, enquanto as taxas de falso positivo foram contidas em 1% e 0,1%, respectivamente.

4.3. Classificador com PCA

Por fim, uma técnica que é considerada das mais modernas e eficazes foi usada para seleção de atributos: PCA.

Tipo de Ataque	TP	FP
Benigno	0.978	0.071
DoS Hulk	0.951	0.031
DoS GoldenEye	0.321	0.000

Tabela 5. Resultados com PCA

Observa-se que ao utilizarmos o PCA como aliado na classificação, obteve-se taxas de verdadeiro positivo bem distintas entre os tipos de ataque, sendo uma taxa de 95.1% para os ataques do tipo Hulk e uma taxa de 32.1% para ataques do tipo GoldenEye, sendo esta última bem inferior a todas apresentadas neste estudo.

4.4. Métricas de Precisão

Ao aplicarmos o classificador com a utilização dos atributos, é possível obter métricas de desempenho que nos auxiliam a avaliar quão bem o classificador está executando sua tarefa. Uma das métricas mais importantes é a precisão, que nos indica a proporção de instâncias classificadas corretamente em relação ao total de instâncias. Na tabela a seguir, apresentamos as precisões obtidas para as classes “Benigno”, “DoS Hulk” e “DoS GoldenEye” utilizando diferentes conjuntos de dados e técnicas de classificação:

	Benigno	DoS Hulk	DoS GoldenEye
Sem seleção de atributos	0.999	0.993	0.990
InfoGain	0.884	0.956	0.905
OneR	0.927	0.978	0.945
PCA	0.960	0.939	0.936

Tabela 6. Precisões para as classes Benigno, DoS Hulk e DoS GoldenEye

Analisando os resultados da tabela, podemos observar que o conjunto de dados “Sem seleção de atributos” proporciona as melhores precisões, atingindo valores próximos a 99%. Isso sugere que usar todas as informações disponíveis nos atributos resulta em um desempenho superior. No entanto, é interessante notar que, mesmo ao utilizar técnicas de redução de dimensionalidade, como OneR, ainda é possível obter precisões bastante elevadas, o que indica a eficácia dessas técnicas em preservar as informações essenciais para a classificação.

Além disso, destaca-se um redução no tempo de processamento, chegando a 98,25%, como demonstrado na tabela abaixo. Este comparativo evidencia de forma nítida a economia de tempo obtida ao empregar técnicas de seleção de atributos.

Abordagem	Tempo de Execução (s)
Sem seleção de atributos	6941
InfoGain	97
OneR	121
PCA	95

Tabela 7. Tempo de execução por abordagem

5. Considerações Finais

Ao empregarmos técnicas de seleção de atributos antes de realizar a classificação dos dados, é evidente que diversos fatores podem influenciar a precisão e, portanto, devem ser considerados na implementação de um IDS. Os resultados indicam que ao adotarmos a seleção de atributos prévia à classificação, conseguimos notáveis ganhos em eficiência na detecção de ataques, sem comprometer de forma substancial a precisão. Destaca-se drástica redução em tempo de processamento, chegando a uma economia de 98,25%. Este comparativo demonstra claramente a economia de tempo alcançada ao utilizar técnicas de seleção de atributos. Dito isso, nota-se que técnicas de seleção de atributos desempenham um papel fundamental na implementação de sistemas de detecção de intrusão. Isso se deve, em grande parte, à necessidade crescente de eficiência e economia de recursos, especialmente para a detecção em tempo real de ataques.

Referências

Dalmazo, B. L., Marques, J. A., Costa, L. R., Bonfim, M. S., Carvalho, R. N., da Silva, A. S., Fernandes, S., Bordim, J. L., Alchieri, E., Schaeffer-Filho, A., Paschoal Gaspary, L., and Cordeiro, W. (2021). A systematic review on distributed denial of service attack defense mechanisms in programmable networks. *International Journal of Network Management*, 31(6):e2163.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2018). Triple-similarity mechanism for alarm management in the cloud. *Computers & Security*, 78:33–42.

Jabez, J. and Muthukumar, B. (2015). Intrusion detection system (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science*, 48:338–346.

Kasongo, S. M. and Sun, Y. (2019). A deep learning method with filter based feature engineering for wireless intrusion detection system. *IEEE Access*, 7:38597–38607.

Novakovic, J., Strbac, P., and Bulatović, D. (2011). Toward optimal feature selection using ranking methods and classification algorithms. *Yugoslav Journal of Operations Research*, 21:119–135.

Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A. (2018). Intrusion detection evaluation dataset (cic-ids2017). *Proceedings of the of Canadian Institute for Cybersecurity*.

Thaseen, I. S. and Kumar, C. A. (2017). Intrusion detection model using fusion of chi-square feature selection and multi class SVM. *Journal of King Saud University-Computer and Information Sciences*, 29(4):462–472.

Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., and Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7:41525–41550.