Detecção de Anomalias em Logs de Sistemas

Fabrício A Silva[1] e Luis G A Diniz[2]

***Abstract*—**

I. Introdução

É fato que sistemas computacionais são usados em larga escala por pequenas e grandes empresas, nas mais diversas áreas. Tal utilização, em alguns casos, pode gerar um grande volume de informações relacionadas com a entidade que detém os dados, assim como pela entidade que os produziu. As relações das entidades envolvidas com dados podem ser críticas e, nesse caso, devem ser abordadas cautelosamente. Questões como a privacidade das informações são extremamente delicadas e têm relação direta com a segurança do sistema utilizado para armazená-las. A segurança torna-se uma questão ainda mais crítica se considerarmos o fato de que há um elevado número de sistemas computcionais nas nuvens, o que leva à maior vulnerabilidade.

Tendo isso em vista, destaca-se a importância do desenvolvimento de medidas contra a vulnerabilidade de sistemas capazes de armazenar grandes volumes de dados [20]. A prevenção e detecção de intrusos tem um importante papel neste cenário. Considerando-se um sistema em rede é possível, por meio da análise dos dados produzidos no log do sistema, detectar atividades suspeitas que devem ser, posteriormente ou em tempo real, investigadas para que estas sejam classificadas ou não como reais ameaças.

Tendo como fonte de informações logs, há técnicas para a detecção de intrusos. Um sistema capaz de realizar tal tarefa é conhecido com NIDS (Network Intrusion Detection System). Há dois importantes métodos para detectar atividades suspeitas [8]: *misuse detection* e *anomaly detection*.

Misuse detection busca o que não está previsto no conjunto de dados. Para que esta técnica funcione corretamente, é necessário que assinaturas (descrições) de ataques já conhecidos sejam disponibilizadas para que o método trabalhe baseado nelas. Por esta razão, pode-se dizer que esta técnica é limitada, já que não permite ao sistema identificar novos tipos de ataque. Por outro lado, a taxa de acertos com uso de assinaturas tende a ser alta.

Anomaly detection consiste na identificação de comportamento dos dados analisados com base em uma entrada, não são necessárias assinaturas para a identificação dos ataques. O método aprende quais atividades são suspeitas e quais não são. Sua principal vantagem é possibilitar a identificação de novos ataques devido ao fato de não precisar de assinaturas. Entretanto, a taxa de falsos positivos tende a ser alta.

Em aplicações reais, a técnica de detecção de anomalias se mostra mais interessante. Fato que se deve principalmente à possibilidade de detecção de ataques desconhecidos (novos tipos de ataque) sem a necessidade da inserção de suas assinaturas (descrições). Tendo isso em vista, há diversas maneiras de se implementar algoritmos e/ou sistemas capazes de identificar anomalias [2], dentre elas pode-se citar análise estatística, algoritmos de classificação, algoritmos de clusterização e grafos. Estas são apenas algumas estratégias utilizadas, mais sobre elas e outras pode ser encontrado em [6].

O presente trabalho dará especial atenção para clustering aplicado à detecção de anomalias. Clustering se mostra um método vantajoso pois é implementado de forma não supervisionada, ou seja, não há necessidade de um conjunto de dados classificado como livre de anomalias (conjunto de dados de treinamento) para que o algoritmo aprenda a identificar uma atividade suspeita. É evidente que, dado um conjunto de dados livre de anomalias, a implementação de outras técnicas apresentará bons resultados. Todavia, em aplicações do mundo real, é pouco frequente a disponilidade de um conjunto de dados de treinamento. [5] mostra que há diferentes maneiras de se aplicar clustering, cada um dos algoritmos mencionados por [5] aprensenta suas particularidades. Técnicas baseadas em análises estatísticas também são exploradas, considerando que se mostram relevantes na literatura.

O objetivo então é: explorar o uso de técnicas de clustering e análises estatísticas para detecção de anomalias em logs de sistemas. Resultado esperado: uma análise comparativa entre diferentes técnicas na base de dados NSL-KDD, em termos de desempenho computacional, precisão, atributos escolhidos, entre outros.

[INCLUIR PARÁGRAFO DESCREVENDO A OR-

GANIZAÇÃO DO TEXTO]

II. Trabalhos Relacionados

Diversas estratégias foram propostas para o desenvolvimento de sistemas de detecção de instrusos. Tais estratégias possuem inúmeras possíveis abordagens, cada uma delas apresenta suas particularidades. Esta seção descreve trabalhos com as abordagens mais recorrentes na literatura.

Há uma série de soluções, ditas supervisionadas, para aplicar a detecção de anomalias. Uma possível implementação de um IDS (Intrusion Detection System) pode ser realizada por meio de redes neurais. [19] mostra resultados promissores utilizando redes do tipo *feed-forward* com base no algoritmo de *back propagation*. Outra estratégia recorrente é a aplicação de métodos estatísticos para identificação de comportamentos anômalos (dados que desviam do padrão esperado), [11] executa sólida análise baseada em logs de servidores apache e obtêm resultados satisfatórios. O uso de técnicas de *machine learning* também é uma alternativa, [15] deixa claro que o uso dessa estratégia deve ter especial atenção já que não funciona de forma eficiente em todos os cenários de IDS. [21] explicita algumas razões que tornam o uso de *machine learning* um desafio na detecção de intrusos, mas ressalta que tal estratégia não é totalmente ineficiente e que deve, apenas, ser usada em situações adequadas. Todas as técnicas mencionadas acima são ditas supervisionadas, pois necessitam de um conjunto de dados de treinamento para que possam ser executadas. A aplicação de estratégias supervisionadas é vantajosa pois apresenta alto nível de precisão. Todavia, necessita de um conjunto de dados de treinamento, no caso específico um conjunto de dados livre de anomalias. Em aplicações reais, a obtenção de um conjunto de informações adequadas para treinamento não é tarefa trivial e nem sempre viável.

Há também, diversas soluções implementadas por meio de técnicas não supervisionadas, [16] utiliza o clássico algoritmo *K-means* para executar detecção de anomalias. [13] combina dois tipos de clustering (i.e. *grid e density*) e obtém resultados satisfatórios, todavia, a taxa de falsos positivos apresentada é alta. [18], por sua vez, implementa clustering hiperesférico para aplicar detecção de instrusos em redes sem fio. [23] combina o *K-means* com o *Naïve Bayes Classification* e apresenta resultados que comprovam significativa precisão. [1] desenvolve um sistema baseado no algoritmo dos K vizinhos mais próximos para executar a detecção de intrusos em *Supervisory Control and Data Acquisition* (SCADA). Todas estas técnicas não supervisionadas são interessantes em cenários reais levando-se em conta que não há a necessidade de um conjunto de dados livre de treinamento, ou seja, são soluções práticas. Em contrapartida, a precisão de tais soluções deixa a desejar quando comparada com estratégias supervisionadas ou, em alguns casos, híbridas.

A combinação de estratégias supervisionadas e não supervisionadas é promissora, pois é capaz de identificar ataques desconhecidos e ainda sim manter uma taxa de acerto dentro de limites aceitáveis. Tendo isso em vista, tem-se os chamados sistemas híbridos. [10] utiliza *misuse detection* e detecção de anomalias combinadas para identifcar intrusos, os resultados apresentados têm melhor tempo de execução do que os modelos convencionais. [3] segue a mesma estratégia que [10] e comprova qua a combinação dos algoritmos é mais eficiente que cada um deles isolado. [14] combina clustering com a técnica dos vizinhos mais próximos e compara seus resultados com soluções recorrentes na literatura. [17] implementa árvore de decisão combinada com *suport vector machine* (SVM) e obtem bons resultados. [24] utiliza o algoritmo *random-forests* tanto para aplicação de misuse detection quanto para detecção de anomalias, e mostra que *misuse detection* apresenta melhor desempenho do que detecção de anomalias mesmo que não seja possível a identificação de novos ataques.

É evidente que, IDSs capazes de detectar ataques conhecidos e desconhecidos são mais interessantes para aplicações do mundo real. Já que em sistemas supervisionados é necessário um conjunto de dados livre de anoamlias para que seja aprendido a diferença entre um registro potencialmente danoso e um registro regular. E mesmo que haja uma parte não supervisionada em sistemas híbridos, há também parte implementada de forma supervisionada, além de ser claramente mais complexa a implementação de sistemas que combinam os dois tipos de técnicas.

Tendo isso em vista, o presente trabalho tem o objetivo de comparar estratégias não supervisionadas para detecção de anomalias. Modelos recorrentes na literatura, assim como novas propostas, serão comparados para que direções de pesquisa em detecção de anomalias de forma não supervisionada sejam estabelecidas. [9] também compara diversas estratégias e abordagens mas não foca em práticas não supervisionadas. [12] realiza comparação similar mas com foco na base de dados DARPA 1998. Por sua vez, [7] compara 19

algoritmos não supervisionados em 10 diferentes bases de dados, todavia, a base de dados NSL-KDD (versão refinada do KDD99) não se encontra entre elas. Dessa forma, objetiva-se estudar diferentes algoritmos para detecção de anomalias não supervisionados na base de dados NSL-KDD fornecida pelo CIC (*Canandian Institute of Cybersecurity*) da Universidade de New Brunswick.

III. NSL-KDD

Para a comparação dos algoritmos uma base de dados de benchmark foi escolhida: NSL-KDD. Esta base de dados consiste no refinamento da KDD99, usada na Terceira Competição Internacional de Descoberta de Conhecimento e Ferramentas de Mineração de Dados (Third International Knowledge Discovery and Data Mining Tools Competition).

O objetivo desta competição é desenvolver um detector de intrusos em rede usando a base de dados disponibilizada como referência para testes. Após a competição diversos trabalhos foram elaborados com base nos dados disponibilizados (citar artigos), de forma a evidenciar que a KDD99 apresenta características não desejadas para uma base de dados de benchmark.

Tendo isso em vista a NSL-KDD foi escolhida pois consiste numa versão refinada da KDD99. Segundo [4] registros redundantes foram removidos, de forma a não influenciar nos resultados. [22] faz uma detalhada análise da base de dados. Uma quantidade suficiente de registros está disponível na base de testes, permitindo a execução de testes na base completa. Além disso, o número de registros selecionados para cada nível de dificuldade é inversamente proporcional à porcentagem de registros na base de dados original (KDD99). Permitindo assim que as taxas de classificação de diferentes algoritmos variem num intervalo maior, dessa forma é possível avaliar com mais precisão a eficiência dos métodos analisados.

A. Tipos de Ataque

IV. Algoritmos Selecionados

Ao todo cinco algoritmos foram selecionados para comparação. São eles:

- K-means: extrema relevância na literatura ao se tratar de clustering. For
- Local Outlier Factor - LOF:
- Histrogram-Based Outlier Score - HBOS: algoritmos baseado em análise estatística que apresentou bom desempenho segundo [7]
- Elliptic Envelope:
- Isolation Forest:

References

[1] Abdulmohsen Almalawi, Xinghuo Yu, Zahir Tari, Adil Fahad, and Ibrahim Khalil. An unsupervised anomaly-based detection approach for integrity attacks on scada systems. *Computers & Security*, 46:94–110, 2014.

[2] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):15, 2009.

[3] Ozgur Depren, Murat Topallar, Emin Anarim, and M Kemal Ciliz. An intelligent intrusion detection system (ids) for anomaly and misuse detection in computer networks. *Expert systems with Applications*, 29(4):713–722, 2005.

[4] L Dhanabal and SP Shantharajah. A study on nsl-kdd dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(6):446–452, 2015.

[5] Daniel Gomes Ferrari and Leandro Nunes De Castro. Clustering algorithm selection by meta-learning systems: A new distance-based problem characterization and ranking combination methods. *Information Sciences*, 301:181–194, 2015.

[6] Pedro Garcia-Teodoro, J Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, 28(1):18–28, 2009.

[7] Markus Goldstein and Seiichi Uchida. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, 11(4):e0152173, 2016.

[8] Richard A Kemmerer and Giovanni Vigna. Intrusion detection: a brief history and overview. *Computer*, 35(4):supl27–supl30, 2002.

[9] Kevin S Killourhy and Roy A Maxion. Comparing anomaly-detection algorithms for keystroke dynamics. In *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on*, pages 125–134. IEEE, 2009.

[10] Gisung Kim, Seungmin Lee, and Sehun Kim. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4):1690–1700, 2014.

[11] Christopher Kruegel and Giovanni Vigna. Anomaly detection of web-based attacks. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 251–261. ACM, 2003.

[12] Aleksandar Lazarevic, Levent Ertoz, Vipin Kumar, Aysel Ozgur, and Jaideep Srivastava. A comparative study of anomaly detection schemes in network intrusion detection. In *Proceedings of the 2003 SIAM International Conference on Data Mining*, pages 25–36. SIAM, 2003.

[13] Kingsly Leung and Christopher Leckie. Unsupervised anomaly detection in network intrusion detection using clusters. In *Proceedings of the Twenty-eighth Australasian conference on Computer Science-Volume 38*, pages 333–342. Australian Computer Society, Inc., 2005.

[14] Wei-Chao Lin, Shih-Wen Ke, and Chih-Fong Tsai. Cann: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-based systems*, 78:13–21, 2015.

[15] Yu-Xin Meng. The practice on using machine learning for network anomaly intrusion detection. In *Machine Learning and Cybernetics (ICMLC), 2011 International Conference on*, volume 2, pages 576–581. IEEE, 2011.

[16] Gerhard Münz, Sa Li, and Georg Carle. Traffic anomaly detection using k-means clustering. In *GI/ITG Workshop MMBnet*, 2007.

[17] Sandhya Peddabachigari, Ajith Abraham, Crina Grosan, and Johnson Thomas. Modeling intrusion detection system using hybrid intelligent systems. *Journal of network and computer applications*, 30(1):114–132, 2007.

[18] Sutharshan Rajasegarar, Christopher Leckie, and Marimuthu Palaniswami. Hyperspherical cluster based distributed anomaly detection in wireless sensor networks. *Journal of Parallel and Distributed Computing*, 74(1):1833–1847, 2014.

[19] Jimmy Shun and Heidar A Malki. Network intrusion detection system using neural networks. In *Natural Computation, 2008. ICNC'08. Fourth International Conference on*, volume 5, pages 242–246. IEEE, 2008.

[20] Uthayasankar Sivarajah, Muhammad Mustafa Kamal, Zahir Irani, and Vishanth Weerakkody. Critical analysis of big data challenges and analytical methods. *Journal of Business Research*, 70:263–286, 2017.

[21] Robin Sommer and Vern Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 305–316. IEEE, 2010.

[22] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani. A detailed analysis of the kdd cup 99 data set. In *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on*, pages 1–6. IEEE, 2009.

[23] Warusia Yassin, Nur Izura Udzir, Zaiton Muda, and Md Nasir Sulaiman. Anomaly-based intrusion detection through k-means clustering and naives bayes classification. In *Proc. 4th Int. Conf. Comput. Informatics, ICOCI*, number 49, pages 298–303, 2013.

[24] Jiong Zhang, Mohammad Zulkernine, and Anwar Haque. Random-forests-based network intrusion detection systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 38(5):649–659, 2008.