Classificação de tráfego de ataques em redes de computadores através de técnicas de mineração de dados

Gesiel Rios Lopes[1], **Alexandre C. B. Delbem**[1]

[1]Instituto de Ciências Matemática e de Computação (ICMC)
Universidade de São Paulo (USP)
Avenida Trabalhador São-carlense, 400 – Centro
CEP: 13566-590 – São Carlos - SP - Brasil

gesielrios@usp.br, acbd@icmc.usp.br

Abstract. *The growth in the number of elements and services in today's computer networks based on the integration of diverse technologies to provide connectivity and services all the time and everywhere has made the computing infrastructure complex and susceptible to various malicious activities. Therefore, efficiently detecting traffic on a computer network and identifying it quickly and accurately becomes essential. This article presents the use of the DAMICORE technique to promote TCP stream grouping of a computer network. The proposed system is evaluated through two sets of traffic: real network traffic, collected at a university, and synthetic laboratory-produced traffic. The results showed the feasibility of using the technique, allowing its application in a set of 5,530 TCP flows.*

Resumo. *O crescimento do número de elementos e serviços nas atuais redes de computadores baseados na integração de diversas tecnologias, de modo a proporcionar conectividade e serviços a todo tempo e em todo lugar, vêm tornando a infraestrutura computacional complexa e suscetível as diversas atividades maliciosas. Portanto, detectar com eficiência o tráfego de uma rede de computadores e identificar de forma rápida e precisa torna-se essencial. Este artigo apresenta o uso da técnica DAMICORE para promover agrupamento de fluxos TCP de uma rede de computadores. O sistema proposto é avaliado através de dois conjuntos de tráfego: tráfego real de uma rede, coletado em uma universidade e tráfego sintético produzido em laboratório. Os resultados gerados mostraram a viabilidade do uso da técnica, permitindo a sua aplicação em um conjunto de 5.530 fluxos TCP.*

1. Introdução

Ataques às redes de computadores constituem em uma das principais ameaças ao mundo amplamente conectado. O crescimento do número de elementos e serviços conectados à internet, traz consigo uma gama de atividades maliciosas e vulnerabilidades não exploradas [Sanz and Lopez 2018].

Portanto, mecanismos de segurança que detectem ataques de forma acurada são imprescindíveis para uma Internet do Futuro segura, no entanto, essa tarefa não é nada trivial [Ziviani and Duarte 2005, Barros et al. 2016]. A identificação da composição do

tráfego de uma rede é de extrema importância e utilidade para administradores e projetistas de redes de computadores que trabalham com o planejamento e aprovisionamento de recursos. A partir da identificação correta do tráfego de uma rede, possibilita a sua manipulação, distribuindo-o de acordo com os recursos disponíveis e também com os requisitos específicos que ele possa possuir, além de protegê-las contra eventuais atividades maliciosas [Ziviani and Duarte 2005, Barros et al. 2016].

No entanto, para tal tarefa é necessário um conhecimento prévio dos padrões de tráfego para que seja feito de forma correta a sua manipulação. Técnicas populares de identificação baseados em análise do número da porta e no conteúdo dos pacotes estão de alguma forma limitados. O reconhecimento do tráfego baseado no conteúdo de pacotes utiliza padrões específicos de *bytes* (assinaturas) [Davies et al. 1998, Moore and Zuev 2005]. Porém, essa abordagem possui um alcance limitado, já que, consegue identificar somente tráfego quando as assinaturas são conhecidas.

Neste artigo, o problema de detecção do tráfego de rede e de ataques é formulado como um problema de classificação de fluxos TCP. A classificação dos fluxos é feita através da utilização da técnica de mineração de dados (MD), DAMICORE (do inglês, *DAta MIning of Code REpositories*) [Sanches et al. 2011]. A abordagem proposta neste trabalho utiliza um conjunto de variáveis discriminantes estatísticas extraídas do fluxo TCP e a técnica DAMICORE que gera uma filogenia que descreve relações hierárquicas de similaridade entre os fluxos avaliados.

O restante deste trabalho está estruturado da seguinte forma. Na Seção 2 discute os trabalhos relacionados, enquanto que na Seção 3 é apresento os conceitos relacionados à técnica de mineração de dados utilizada neste trabalho, DAMICORE. Na Seção 4 é descrito todo o ambiente utilizado nos experimentos, além das descrições dos dados utilizados. A Seção 5 apresenta e discutes os resultados obtidos. Por fim, a Seção 6 são apresentadas as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

Ao longo dos anos, várias medidas vêm sendo criadas com o objetivo de garantir a segurança contra ataques em redes de computadores, tais como criptografia e autenticação. No entanto, tais medidas não são suficientes para lidar com a gama de ataques existentes e que vêm surgindo nos últimos anos. Dessa forma, faz-se necessário outros mecanismos de prevenção, tais como os Sistemas de Detecção de Intrusos (IDS, do inglês *Intrusion Detection System*), que, em geral, analisa o tráfego da rede tentando reconhecer comportamentos e/ou uma ações intrusivas para alertar o administrador, ou automaticamente disparar contramedidas [Ramos and dos Santos 2011, Debar et al. 2000].

Na literatura, em geral, as técnicas utilizadas para detecção de intrusão são classificadas em dois tipos: assinatura e anomalia [Ramos and dos Santos 2011]. Na detecção por assinatura, o tráfego é comparado com uma base de tráfego conhecido de ataques (assinaturas), já a detecção por anomalia realiza a comparação dos dados coletados com registros de atividades rotulados como normais. Qualquer desvio do que é considerado normal é considerado uma possível ameaça. Em ambas as abordagens existem desafios a serem superados, como, por exemplo, a atualização frequente dos registros para garantir uma boa detecção em abordagens baseadas em assinaturas e a taxa de falsos positivos e negativos em técnicas baseadas por anomalia [Lopes et al. 2011].

Várias abordagens baseadas em aprendizado de máquina como Redes Neurais Artificiais, Sistemas de Inferência Fuzzy e SVM (do inglês, *Support Vector Machine*), têm sido propostas na literatura para realizar detecção de intrusão. Em [Amudhavel et al. 2016] é apresentada uma revisão sobre as principais técnicas utilizadas nos IDS's. Já em [Chapaneri and Shah 2019] é apresentado uma revisão sobre IDS's de última geração baseada em aprendizado de máquina. E em [Amrita and Kant 2019] os autores apresentam os principais IDS's baseado em anomalia que utilizam técnicas de aprendizado de máquina empregando abordagens de seleção de características.

No trabalho descrito por [Ramos and dos Santos 2011], os autores propõem o uso de comitês de classificadores em três níveis para resolver problemas de detecção. Em cada nível são aplicados classificadores gerados por um mesmo algoritmo base e seus resultados são combinados nos níveis posteriores. O último nível de classificação forma um comitê de comitês, que tenta viabilizar uma maior precisão na detecção.

O trabalho de [Sanz and Lopez 2018], os autores apresentam um sistema de detecção, em linha (*online*), de ameaças distribuídas de rede baseado em aprendizagem enriquecida por grafos. É proposto uma arquitetura de detecção de intrusão para inferir características de análise de grafos a partir das amostras do tráfego coletado em uma janela de tempo. Para cada amostra recebida, um grafo do *snapshot* desta janela é gerado e repartido em subgrafos de componentes conexas. Um algoritmo percorre as componentes conexas inferindo 39 novas características a partir de métricas locais, de vértices e de arestas das componentes.

Em [Elejla et al. 2018], é proposto um IDS, baseado em fluxo, para detectar a presença de ataques DDoS baseados em ICMPv6 em redes habilitadas para IPv6. O IDS proposto consiste em três estágios consecutivos: coleta e pré-processamento dos dados, extração das características e construção de fluxo, e detecção de ataques DDoS baseados em ICMPv6.

Já em [Jyothsna et al. 2019] é proposto um IDS baseado em fluxo para redes de alta velocidade usando escala meta-heurística. Inicialmente, uma abordagem baseada em fluxo é aplicada no fluxo de solicitação para definir métricas de recursos. Em seguida, essas métricas de recurso são usadas para definir a escala, que é usada posteriormente para definir se o fluxo é normal ou malicioso.

O presente trabalho difere dos citados anteriormente em dois aspectos principais: (a) a utilização de variáveis discriminantes estatísticas extraídas dos fluxos TCP para caracterização do tráfego. (b) o uso de uma técnica de mineração de dados para descrever relações hierárquicas de similaridade entre objetos de dados não estruturados.

3. DAMICORE

O método DAMICORE (*DAta MIning of Code REpositories*) [Sanches et al. 2011, Pinto et al. 2017] consiste em um arcabouço teórico constituído pela combinação de várias técnicas visando fornecer relações hierárquicas entre objetos de dados não estruturados. O método consiste na realização de três passos: (1) construir uma matriz de distâncias comparando cada dois objetos do repositório de acordo com uma métrica de similaridade; (2) converter a matriz de distâncias em uma rede que conecta os objetos de acordo com suas similaridades; (3) aplicar um processo de detecção de comunidades para detecção de grupos de elementos similares dentro da rede. Originalmente

três algoritmos são utilizados nestes passos: *Normalized Compression Distance* (NCD) [Cilibrasi and Vitanyi 2005] para a construção da matriz de distâncias, *Neighbor Joining* (NJ) para produzir uma árvore filogenética a partir da matriz de distâncias e o método *Fast Newman* (FN) para detecção de comunidades na árvore gerada. O cálculo da NCD é o passo do DAMICORE que viabiliza sua aplicação a qualquer tipo de dado sem requerer informação semântica sobre o mesmo. A NCD é uma aproximação computável da complexidade de Kolmogorov, definida pela Equação 1 [Cilibrasi and Vitanyi 2005].

$$NCD_z(a,b) = \frac{C_z(ab) - min\{C_z(a), C_z(b)\}}{max\{C_z(a), C_z(b)\}} \quad (1)$$

Os dois objetos a serem comparados são denominados por a e b, sendo ab concatenação de ambos e $C_z(x)$ é o tamanho da versão compactada do objeto x obtido por meio de um algoritmo de compressão Z. Para um compressor ideal e dois arquivos idênticos, $C_z(ab) = C_z(a) = C_z(b)$ e, portanto, $NCDz(a,b) = 0$, enquanto para dois arquivos totalmente diferentes, $C_z(ab) = C_z(a) + C_z(b)$ e logo $NCD_z(a,b) = 1$. Uma vez que a compressão é efetuada em nível de cada byte dos dados, o método DAMICORE torna-se agnóstico quanto à semântica dos dados. A aplicação do algoritmo NJ na matriz de distâncias produz uma árvore filogenética dos objetos do repositório tornando visual relações não evidentes na matriz de distâncias. Por fim, o método é completado pela aplicação do FN para detecção de agrupamentos (comunidades) dos elementos semelhantes na árvore, destacando as relações mais fortes entre os objetos em estudo.

4. Experimentos

Para avaliar a aplicação da DAMICORE na caracterização do perfil de fluxos de tráfego TCP/IP foi utilizado o princípio de fluxo de dados, o qual pode ser definido como uma sequência de pacotes trafegando entre dois dispositivos através de um protocolo em comum e um par de portas específicas [Moore and Zuev 2005]. Os fluxos devem ter pelo menos um pacote em cada sentido de tráfego para serem considerados válidos.

Para avaliação e validação proposta neste trabalho foram utilizados apenas fluxos TCP, ou seja, aqueles que são iniciados com uma apresentação de três vias e são considerados finalizados se um *flag* FIN e/ou RST são vistos no cabeçalho TCP. Fluxos UDP, tráfego criptografado ou sem apresentar no mínimo um pacote contendo dados de aplicação não foram considerados.

Os fluxos de dados são criados a partir dos pacotes coletados por um analisador de pacotes (*Sniffer*). Para cada fluxo foi gerado um conjunto de 52 variáveis que foram obtidas a partir dos cabeçalhos dos pacotes capturados por um analisador de pacotes. Estas variáveis foram definidas a partir de um conjunto listado em [Filho et al. 2007, Moore and Zuev 2005] e demonstram informações tais como: tamanho do pacote e *flags* TCP/IP. Essas métricas descrevem o comportamento de um fluxo de dados tendo em vista às duas direções de um tráfego: do cliente para servidor e vice-versa. A Tabela 1 pode-se observar algumas das variáveis utilizadas neste trabalho.

4.1. Dados e medições

Para representar o tráfego considerado Normal, pacotes foram coletados a partir do *gateway* de uma rede pública, durante o período de 26 a 28 abril de 2019, nos períodos da

Tabela 1. Exemplos de variáveis candidatas a discriminantes

Variável Candidata
Número Mínimo do Total de Bytes em um Pacote IP cliente para servidor
Tamanho Máximo da Janela de Anúncio cliente para servidor
Média dos Bytes de Controle no Pacote cliente para servidor
Média do Tamanho do Segmento servidor para cliente
Tamanho Máximo da Janela de Anúncio servidor para cliente
Pacotes de Dados Atuais cliente para servidor
Tamanho Mínimo da Janela de Anúncio servidor para cliente
Tamanho Máximo do Segmento cliente para servidor

manhã (8:00 às 9:00) e tarde (14:00 às 15:00 e 16:00 às 17:00). Os pacotes capturados foram armazenados temporariamente e, em seguida, os fluxos foram reconstruídos. Após a captura dos pacotes e reconstrução dos fluxos, cada fluxo foi rotulado com uma classe de aplicação.

Com o intuito de tentar garantir que o fluxo coletado estaria desprovido de atividades maliciosas, todos os fluxos reconstruídos foram analisados pela ferramenta NIDS *Snort* [Roesch 1999], com todos os conjuntos de regras datadas de 29 de Novembro de 2018. Os fluxos que infringiram alguma das regras utilizadas pelo NIDS Snort foram separados dando origem a um conjunto de fluxos, aqui denominado de Alertas *Snort*. Não foram feitas investigações no conjunto Alertas *Snort* com o intuito de identificar os possíveis tipos de ataques.

Face às dificuldades para se obter amostras reais e recentes de tráfego malicioso, ao nível de pacote e com os dados dos cabeçalhos TCP/IP devidamente identificados, foram gerados ataques artificialmente, para que estes fossem inseridos no tráfego a ser analisado. Neste trabalho foram consideradas duas categorias de ataques de quebra de senha. O primeiro (*Dictionary attack*), que tem como objetivo a quebra de senhas de um mecanismo de autenticação utilizando um conjunto predeterminado de palavras. O segundo (*Brute Force*), realiza o ataque mesclando letras e dígitos de forma aleatória até conseguir a adivinhação da senha. A Figura 1 apresenta o ambiente utilizado para a geração do tráfego de ataque.

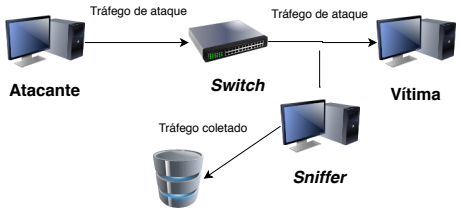

Figura 1. Topologia da rede para geração do tráfego de ataque.

Neste cenário foram utilizados três computadores: o atacante, a vítima, e um analisador de pacotes. O atacante possui o papel de enviar tráfegos de ataques contra os serviços, como FTP, SMTP e HTTP, de uma determinada vítima. Para a realização de ataques foram gerados pelos programas *Hydra* e *Brutus*.

A Tabela 2 descreve as classes, as aplicações e o total dos fluxos dentro de cada conjunto de dados utilizados.

Tabela 2. Descrição do conjunto de dados utilizado.

Classe	Número de Fluxos
Tráfego Normal (WWW, CHAT, MAIL e P2P)	1835
Alertas Snort	1345
Dicionário	1250
Força Bruta	1100

5. Resultados

A DAMICORE foi aplicado sobre todo o conjunto de fluxos descritos na Tabela 2 de forma aleatória. A Figura 2 apresenta a metodologia da aplicação da DAMICORE utilizada neste trabalho.

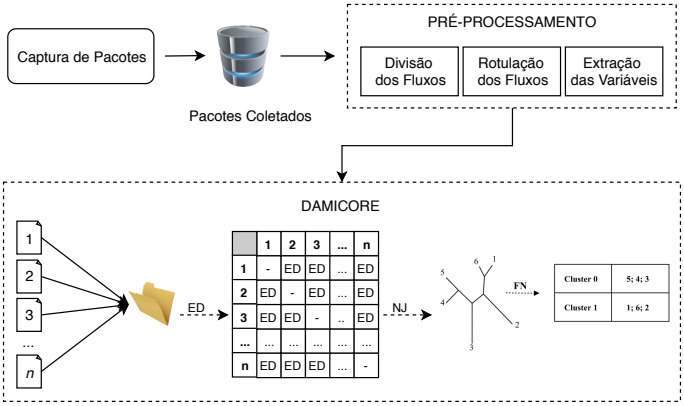

Figura 2. Esquema utilizado para aplicação da DAMICORE

Como resultado, foram geradas "árvores" que agrupam os fluxos de acordo com as suas características (Figura 3). A estrutura de cada "árvore" gerada é composta por "folhas" que representam cada um dos fluxos pela sua classe, e "ramos" (conjunto de folhas) que representam os agrupamentos dos fluxos de acordo com as características obtidas a partir dos discriminantes estatísticos extraídos dos fluxos.

A Figura 3 contém a árvore filogenética resultante da aplicação do DAMICORE em uma amostra de 40 fluxos escolhidos aleatoriamente, sendo 10 fluxos de cada classe (Tráfego Normal, Alertas Snort, Força Bruta e Dicionário). É importante notar que a árvore determina a filogenia dos fluxos TCP analisados, ou seja, fluxos com comportamentos semelhantes(no que tange os descriminantes estatísticos utilizados). Na área destacada em verde é possível observar os agrupamentos dos 10 fluxos rotulados como Tráfego Normal e em amarelo os 10 fluxos rotulados como Alerta Snort. Já em vermelho e em roxo, estão os 10 fluxos rotulados como Dicionário e Força Bruta respectivamente. É possível observar que na árvore gerada houve uma separação significativa para cada classe, evidenciando a viabilidade da utilização da DAMICORE para classificação do tráfego de rede a partir da captura das variáveis discriminantes utilizadas.

6. Conclusão

O objetivo desse trabalho é apresentar os resultados parciais de uma pesquisa que identificou, por meio de técnicas de MD, padrões relevantes de comportamentos fluxos TCP

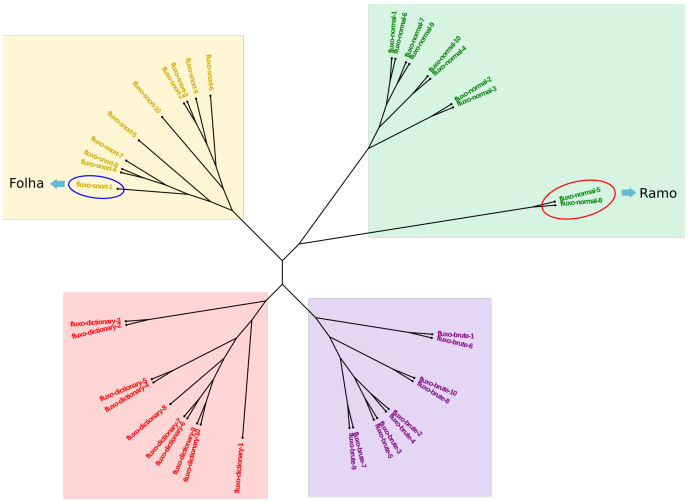

Figura 3. "Árvore" gerada pela DAMICORE para um subconjunto de 10 fluxos de cada classe de fluxo.

de tráfego que flui em uma rede de computadores. Tal conhecimento proporciona entendimento no que trafega em uma rede e quais medias ou precações podem ser tomada na medida em que surgem eventuais problemas. Os resultados preliminares obtidos e aqui apresentados foram satisfatórios e mostram que é possível identificar comportamentos para identificação do tráfego de ataque em uma rede baseada em variáveis discriminantes de fluxos TCP através da utilização da DAMICORE. Apesar dos resultados positivos alcançados, ainda é necessário validar a metodologia para um grupo maior de fluxos e outras classes de tráfego, além de aplicá-la em um ambiente totalmente *online*, de forma a identificar o comportamento do tráfego real de uma rede de forma mais efetiva.

A continuidade deste trabalho segue em três direções: investigar o desempenho da abordagem proposta para novas classes de aplicações e investigar o desempenho de outros classificadores com novas variáveis discriminantes para a classificação do tráfego.

Referências

Amrita and Kant, S. (2019). Machine learning and feature selection approach for anomaly based intrusion detection: A systematic novice approach. *International Journal of Innovative Technology and Exploring Engineering*, 8(6):434–443. cited By 0.

Amudhavel, J., Brindha, V., Anantharaj, B., Karthikeyan, P., Bhuvaneswari, B., Vasanthi, M., Nivetha, D., and Vinodha, D. (2016). A survey on intrusion detection system: State of the art review. *Indian Journal of Science and Technology*, 9(11):1–9.

Barros, M. T., de Alencar, M. S., Gomes, R., and Costa, A. F. (2016). Classificação de fluxos ip para engenharia de tráfego na internet. *Revista de Tecnologia da Informação e Comunicação*, 6(1):21–28.

Chapaneri, R. and Shah, S. (2019). A comprehensive survey of machine learning-based network intrusion detection. In Satapathy, S. C., Bhateja, V., and Das, S., editors, *Smart Intelligent Computing and Applications*, pages 345–356, Singapore. Springer Singapore.

Cilibrasi, R. and Vitanyi, P. M. B. (2005). Clustering by compression. *IEEE Transactions on Information Theory*, 51(4):1523–1545.

Davies, E., Carlson, M. A., Weiss, W., Black, D., Blake, S., and Wang, Z. (1998). An architecture for differentiated services.

Debar, H., Dacier, M., and Wespi, A. (2000). A revised taxonomy for intrusion-detection systems. In *Annales des télécommunications*, volume 55, pages 361–378. Springer.

Elejla, O. E., Anbar, M., Belaton, B., and Alijla, B. O. (2018). Flow-based ids for icmpv6-based ddos attacks detection. *Arabian Journal for Science and Engineering*, 43(12):7757–7775.

Filho, R., Maia, J., and F F Do Carmo, M. (2007). Seleção de discriminantes estatísticos para identificação de tráfego de ataques. *Workshop Gerência de Redes e Serviços - WGRS'2007*.

Jyothsna, V., Mukesh, D., and Sreedhar, A. N. (2019). A flow-based network intrusion detection system for high-speed networks using meta-heuristic scale. In Peng, S.-L., Dey, N., and Bundele, M., editors, *Computing and Network Sustainability*, pages 337–347, Singapore. Springer Singapore.

Lopes, G. R., Coelho, A. L., and Holanda Filho, R. (2011). An autonomic security mechanism based on novelty detection and concept drift. In *ICAS 2011 : The Seventh International Conference on Autonomic and Autonomous Systems*, pages 158–163. IARIA.

Moore, A. W. and Zuev, D. (2005). Internet traffic classification using bayesian analysis techniques. In *SIGMETRICS '05: Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, pages 50–60, New York, NY, USA. ACM.

Pinto, R. S., Delbem, A. C. B., and Monaco, F. J. (2017). Caracterização do perfil de carga a partir de programas binários. In *Anais Estendidos da Escola Regional de Alto Desempenho de São Paulo (ERAD-SP)*, pages 65–68, Porto Alegre, RS, Brasil. SBC.

Ramos, A. L. and dos Santos, C. N. (2011). Combinando algoritmos de classificação para detecção de intrusão em redes de computadores. In *SBSeg'11, XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. SBC.

Roesch, M. (1999). Snort - lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX Conference on System Administration*, LISA '99, pages 229–238, Berkeley, CA, USA. USENIX Association.

Sanches, A., Cardoso, J. M. P., and Delbem, A. C. B. (2011). Identifying merge-beneficial software kernels for hardware implementation. In *2011 International Conference on Reconfigurable Computing and FPGAs*, pages 74–79.

Sanz, I. J. and Lopez, M. A. (2018). Um sistema de detecção de ameaçãs distribuídas de rede baseado em aprendizagem por grafos. In *Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. SBC.

Ziviani, A. and Duarte, O. (2005). Metrologia na internet. *Minicursos do XXIII Simpósio Brasileiro de Redes de Computadores, SBRC*, pages 285–329.