Um Estudo Experimental em Análise, Caracterização e Predição de Tráfego Hostil

Rivalino Matias Jr[1], Patryck Ramos Martins[2]

[1] Faculdade de Computação – Universidade Federal de Uberlândia (UFU) – Brazil

[2] Secretaria do Estado de Saúde de Santa Catarina (DIVE) - Brazil

rivalino@facom.ufu.br, patryckrm@gmail.com

Abstract. *This paper describes a quantitative approach to predict hostile traffic based on traffic sampling and characterization using free software measurement tools. The research work used real traffic samples, collected from multiples network locations, during a three month period. The hostile traffic classification was based on a security policy created for the target network from the characterization study. The results from the forecast models comparison study shown that exponential smoothing family models had a higher performance in terms of prediction accuracy (over 80% on average) among the 14 evaluated models.*

Resumo. *Este artigo apresenta uma abordagem quantitativa para predição de tráfego hostil apoiada na coleta, análise e caracterização de amostras de tráfego obtidas com o uso de ferramentas de software livre. O estudo foi conduzido com amostras de tráfego real, representativas de três meses de coleta e provenientes de múltiplas fontes de dados. A tipificação do tráfego hostil, no ambiente investigado, teve como base uma política de segurança de tráfego criada a partir do estudo de caracterização da rede investigada. Dentre os modelos de predição avaliados, aqueles da família AE (alisamento exponencial) foram os de melhor desempenho (> 80% de acuracidade) dentre os 14 modelos considerados.*

1. Introdução

Considerando a grande dependência da sociedade moderna para com os sistemas computacionais, a segurança desses sistemas deixou de ser um tema tratado em nível operacional para ser considerado elemento estratégico dentro das políticas das organizações, sejam elas públicas ou privadas.

De acordo com [Deri e Suin 2000], a análise de tráfego de rede é considerada uma atividade indispensável para a gerência da segurança, haja vista a variedade de fluxos de tráfego existentes nas redes atuais, principalmente em função da integração de redes heterogêneas, o que propicia o surgimento de diversas formas de ameaças, vulnerabilidades e ataques. A coleta e análise de tráfego oferecem uma visão detalhada do que está sendo transportado pela rede, pois os dados capturados podem ser tratados em todos os níveis da pilha de protocolos. No entanto, sua aplicação exige um processo sistematizado, principalmente na escolha dos pontos de coleta, bem como na periodicidade da monitoração, tamanho das amostras e filtros utilizados.

No contexto da análise de tráfego em redes, destacam-se pesquisas voltadas para a caracterização (ex. [Brownlee e Claffy 2002], [Pedroso *et al*. 2008], [Maia *et al*. 2008]) e a predição de tráfego (ex. [Ilow 2000] ,[Feng et al. 2006], [Papadopouli et al. 2006]). Em ambos os casos, consultando a literatura fica claro o avanço destes estudos cada vez mais no sentido de se adotar métodos quantitativos para apoiar atividades de análise, caracterização e predição de tráfego em redes. Apesar desses avanços, em termos práticos a predição de tráfego de redes tem sido utilizada timidamente em ambientes de produção, seja para fins de planejamento ou gerenciamento/operação. Uma possível explicação seria a ausência de processos sistematizados que integrem o uso de ferramentas de coleta e medição de tráfego com procedimentos de teste e seleção de modelos de predição. Atualmente, diversas ferramentas, licenciadas como software livre (ver Seção 3), podem ser usadas para fins de medição, portanto sendo necessário a integração destas com métodos apropriados para a modelagem e predição de tráfego.

A fim de contribuir com o corpo de conhecimento nesta área, este trabalho apresenta um estudo experimental envolvendo a coleta e caracterização de tráfego visando avaliar modelos de predição para uso em análise de tráfego hostil. Para isso, estabeleceu-se um processo sistematizado que integrou o uso de ferramentas de livre distribuição com os métodos estatísticos adotados no estudo.

O restante do artigo está organizado como descrito a seguir. A Seção 2 apresenta a metodologia adotada no desenvolvimento do trabalho. Na Seção 3 o ambiente real onde o estudo foi realizado é descrito, bem como as tecnologias e as ferramentas de software livre utilizadas. A Seção 4 apresenta uma análise dos principais resultados obtidos. Finalmente, na Seção 5 são apresentadas as conclusões do estudo.

2. Metodologia

A primeira etapa do estudo foi analisar os serviços e o tráfego da rede investigada, objetivando entender o padrão e tipos de tráfego usuais nesse ambiente. Esse estudo preliminar foi necessário para a criação de uma política de segurança aplicada ao tráfego da rede, a qual regulou o que deveria ou não ser transportado pela rede analisada. Para [CAIDA 2001], a definição de tráfego hostil em um ambiente de rede não está associada a nenhum modelo ou padrão pré-estabelecido. Essa tipificação se dá em termos das políticas locais da organização. Portanto, com base na caracterização inicial foi possível identificar os fluxos de tráfego pertinentes ao ambiente investigado.

Com base na política de tráfego definida, iniciou-se a monitoração do tráfego da rede, em diversos pontos de coleta, para a obtenção de amostras visando identificar potenciais desvios (tráfego hostil) em relação à política estabelecida. A estratégia de amostragem considerou um período de coleta de 13 semanas em regime 24x7.

A partir da análise das amostras e sua caracterização, construiu-se uma série temporal com os dados representando aquelas atividades consideradas hostis ao ambiente investigado. A série contou com 91 valores representando o número de ataques diários. Com base nessa amostra foram ajustados 14 modelos de predição. Os modelos considerados neste trabalho foram, *naïve*, *naïve ajustado*, *regressão linear simples (RLS)*, *média móvel* (ordens 2 e 3) e *alisamento exponencial* ($0{,}1 \leq \alpha \leq 0{,}9$), onde α é o coeficiente de alisamento. Uma descrição detalhada destes modelos foge ao

objetivo do trabalho e pode ser encontrada em Brockwell e Davis (1996), Fox (1997) e Makridakis et al. (1997).

3. Estudo Experimental

O ambiente investigado foi uma sub-rede da rede local de uma IFES[1]. Os serviços servidores em operação nessa sub-rede foram: HTTP (Apache), SMTP/POP/IMAP (Qmail), SMB/CIFS (Samba), FTP (ProFTPD), SGBD (MySQL), Backup (Amanda) e Proxy/Cache (Squid). Para efetuar a caracterização do tráfego de entrada/saída desse ambiente, utilizou-se uma solução de captura de tráfego passiva baseada no analisador de protocolos ntop[2] integrado a uma *ethernet bridging* implementada via *kernel* FreeBSD. Essa solução foi instalada na entrada da sub-rede analisada. Uma segunda fonte de dados, esta específica para obtenção de assinaturas de ataques, foi criada com a implementação do NIDS snort na mesma localização do analisador de protocolos. Complementarmente, também foram usados os registros dos *logs* do *firewall* (ipfw) da sub-rede e dos servidores Apache. O sistema operacional usado para implementar as ferramentas citadas foi o FreeBSD. A Figura 1 ilustra o ambiente investigado.

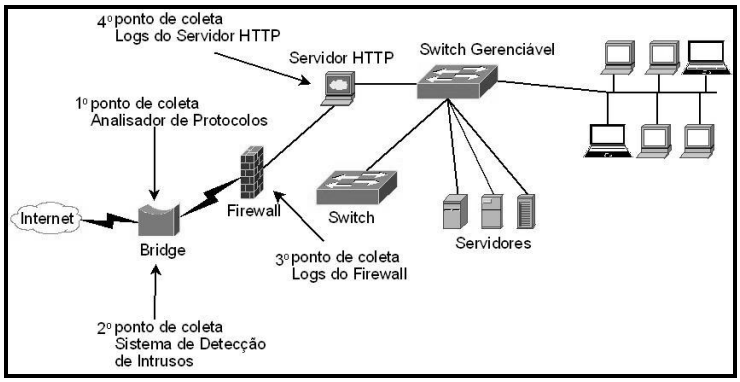

Figura 1. Pontos de coleta para caracterização do tráfego hostil.

Adotar uma única fonte de dados para análise de tráfego hostil não é adequado, haja vista que a atual sofisticação dos ataques exige uma análise a partir de múltiplos pontos da rede e sob diferentes perspectivas. Por exemplo, muitas assinaturas de ataques são transportadas criptografadas em conexões HTTPS, o que dificulta sua detecção via NIDS ou Firewall, mas sendo possível a partir dos logs do servidor web. Em função da adoção de múltiplas fontes de dados, cada qual com formato próprio, foi necessária uma etapa de pré-processamento dos dados para homogeneizar as informações antes de sua análise estatística. Nesse sentido, primeiramente foram desenvolvidos *scripts* para automatizar a extração de dados das diversas fontes (ntop, ipfw, Apache, snort) e padronizar seus formatos para uso posterior na etapa de caracterização e predição. A extração de dados do ntop se deu automaticamente pela sua interface web usando o software wget. Posteriormente, os dados de interesse do ntop foram transportados para

[1] Instituição Federal de Ensino Superior

[2] www.ntop.org

uma planilha onde foram realizadas diversas análises estatísticas (ver Seção 4). No caso do snort, usou-se a ferramenta *SnortSnarf* que permite o agrupamento de alertas por assinatura, origens dos ataques, entre outras funcionalidades. Para os *logs* do *firewall* desenvolveu-se uma ferramenta (usando PHP e MySQL) para importar e contabilizar as informações de interesse. Esse aplicativo também permite visualizar o total de ataques por dia, hora e mês, e lista os sistemas computacionais que mais originaram tráfego hostil. Quanto aos *logs* do Apache foi utilizada a ferramenta *LogSurfer* em virtude do seu alto grau de customização para processamento de arquivos ASCII.

4. Análise dos Resultados

Em função da quantidade de dados analisados e das caracterizações realizadas, aqui serão apresentados apenas os principais resultados com o intuito de demonstrar o potencial das ferramentas e abordagem utilizada. O período de estudo foi de três meses, totalizando 91 dias de amostra. A Figura 2 apresenta a distribuição do tráfego agregado por protocolos.

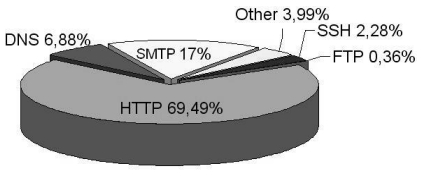

Figura 2. Percentual de utilização da banda da rede por protocolo.

Já com relação ao tráfego hostil, construiu-se um ranking das fontes de ataques (endereços IP) com maior freqüência em número de ataques provenientes de seus endereços. Analisando as trinta e duas primeiras entradas do ranking, aspectos interessantes foram identificados como, por exemplo, uma grande incidência de ataques provenientes de outras sub-redes da rede local do campus, o que corrobora com as atuais estatísticas de segurança que destacam a importância dos ataques internos e não apenas daqueles externos à organização. Diversos ataques provenientes de diferentes *hosts* de uma mesma rede classe C, o que é indicativo de um ataque coordenado. Esse ranking não será apresentado para evitar a exposição dos endereços em questão. A Tabela 1 apresenta um resumo das atividades hostis identificadas como de maior incidência no período da amostragem. Observa-se que o tráfego originado por atividades de *port scanning* destaca-se em comparação com os demais tipos de tráfego hostil.

Tabela 1. Distribuição dos ataques durante o período de coleta.

Ataques	%
Scans de Rede	64,17
Ataques Web	23,06
Exploits	6,38
IPSpoofing	3,82
Flood	2,16
Força Bruta	0,24
Buffer Overflow	0,16
DoS	0,01

Além da caracterização do tráfego hostil, foram testados modelos de predição (ver Seção 2) contra uma amostra organizada na forma de uma série temporal contendo o número de ataques e os dias de ocorrência. Objetivou-se com essa etapa avaliar o desempenho desses modelos para uso futuro em predição de tráfego hostil. Vale ressaltar que a avaliação dos modelos ocorreu utilizando duas séries, sendo uma contendo os dados observados e outra sendo a primeira "logaritmizada", o que significa que os dados da série original foram transformados ($\log_{10}$) antes da análise. Esta abordagem permitiu um melhor ajuste numérico dos modelos do que com os dados originais. Outras transformações (ln(y), 1/y, e^y) também foram testadas, porém não demonstrando melhores resultados. Dentre os modelos considerados, os cinco primeiros classificados estão listados na Tabela 2.

Tabela 2. Ranking dos modelos ajustados aos dados transformados

Modelos	MAPE	Acuracidade
AE(0,9)	15,76037	84,24%
Naïve	15,96394	84,04%
AE(0,8)	16,07929	83,92%
AE(0,7)	16,62296	83,38%
AE(0,6)	17,27656	82,72%

Pode-se verificar que a melhor acuracidade foi demonstrada pelo modelo de alisamento exponencial (α=0,9). É importante notar que para o uso dos valores preditos, foi necessário transformar os valores das predições para sua escala original, já que esses foram estimados com base na série transformada (logaritmizada). Nesse caso, foi necessário aplicar o *anti-log* para cada valor predito (y). Por exemplo, o próximo valor predito da série (92º dia) foi 2,4346, o que resultou em um valor estimado de 272 ataques após realizar o *anti-log* (2,4346). A Figura 3 apresenta uma visão gráfica do ajuste do modelo AE(0,9) aos dados observados, na sua escala original, onde o eixo y corresponde ao número de ataques diários para cada dia (eixo x) da série analisada.

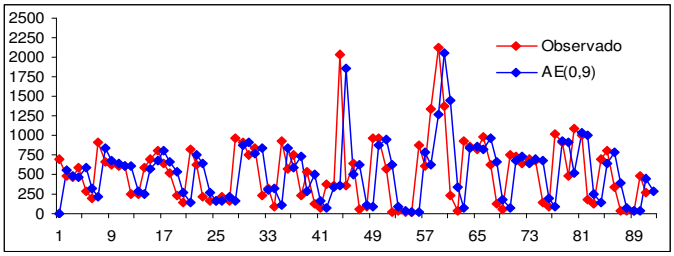

Figura 3: Ajuste do modelo AE (0,9) aos dados observados

5. Considerações Finais

A utilização de métodos quantitativos aplicados à caracterização e predição de tráfego de redes tem se mostrado de grande importância no contexto da engenharia de tráfego. Nesse trabalho verificou-se que modelos da família AE, apesar de simples, apresentaram resultados satisfatórios para as necessidades de um ambiente real. Essas são evidências que motivam aprofundar a investigação desses modelos frente a

diferentes padrões de tráfego hostil. Em termos práticos, a aplicabilidade do enfoque proposto (Seção 2) em ambientes de produção pode ser facilitada automatizando-se não só a coleta de dados, como foi feito, mas também o ajuste, verificação e seleção dos modelos de predição.

Desse modo, propõe-se como trabalho futuro o desenvolvimento de uma ferramenta para automatizar as etapas de ajuste e seleção dos modelos de predição com base em amostras de tráfego hostil. Para facilitar a integração dessa nova ferramenta com as diversas fontes de dados descritas nesse trabalho, os dados, depois de coletados e padronizados, serão armazenados em uma base de dados já no formato de uma série temporal, a fim de serem usados na seleção automática dos modelos. Nesse caso, planeja-se usar a tecnologia RRD (*round-robin database*) [Oetiker 1998] como repositório de integração, visto que essa tecnologia é especializada no armazenamento de séries de dados no tempo. A implementação dessa integração para operação *on-line* seria um passo importante no gerenciamento de segurança em redes, em especial no tocante à análise de tráfego hostil, apoiada por métodos estatísticos.

Referências

Brockwell, P. e Davis, R. (1996) "Introduction to Time Series and Forecasting", Springer.

Brownlee, N. e Claffy, K. (2002) "Understanding Internet traffic streams: Dragonflies and tortoises", IEEE Communications Magazine, 40(10):110-117.

CAIDA. Metrics Working Group. (2001) "Network measurement faq", http://www.caida.org/outreach/metricswg/faq.xml.

Deri, L. e Suin, S. (2000) "Effective Traffic Measurement Using ntop", IEEE Communication Magazine, v. 38, pp. 144-151.

Feng, H., Shu, Y., Wang, S., Ma, M. (2006) "SVM-Based Models for Predicting WLAN Traffic", IEEE Int'l Conference on Communications (ICC'06), Turkey.

Fox, J. (2007) "Applied Regression Analysis, Linear Models, and Related Methods", SAGE Publications, USA.

Ilow, J. (2000) "Forecasting Network Traffic Using FARIMA Models with Heavy Tailed Innovations", ICASSP 2000, Turkey, June 2000.

Maia, M., Almeida, V., Almeida, J. (2008) "Vídeos Gerados por Usuários: Caracterização de Tráfego", Simpósio Brasileiro de Redes de Computadores, Brazil.

Makridakis, G. S., Wheelwright, S. C., Hyndman , R. J. (1997) "Forecasting: Methods and Applications", 3rd Edition, Wiley, USA.

Oetiker, T. (1998) "MRTG - The Multi Router Traffic Grapher", Proceedings of the 12th USENIX conference on System administration, USA.

Papadopouli, M., Raftopoulos, E. e Shen, H. (2006) "Evaluation of short-term traffic forecasting algorithms in wireless networks", IEEE Conference on Next Generation Internet Design and Engineering (NGI'06)", Spain.

Pedroso, C. M., Caldeira, J., Fonseca, K. e Cruz, M. (2008) "Análise da Evolução de Características de Tráfego VoIP", Simpósio Brasileiro de Telecomunicações¸ Brazil.