Avaliação da Sensibilidade de Preditores de Suavização Exponencial na Detecção de Ataques de Inundação

Nícolas R. e Silva[1], Ronaldo M. Salles[1]

[1] Seção de Engenharia de Computação
Instituto Militar de Engenharia (IME) – Rio de Janeiro, RJ – Brazil

nicolasime@gmail.com, salles@ime.eb.br

Abstract. *This paper analyzes the sensitivity of typical exponential smoothing predictors used to detect Distributed Denial of Service (DDoS) flooding attacks. We compare two predictors (EWMA and Holt-Winters) and evaluate their detection accuracy within different settings and scenarios. The performance is investigated in terms of false positive and false negative ratios. We insert attacks on real IP traces (MAWILab) and on real traffic samples from RNP's WAN backbone to perform simulations with different levels of flooding. Simulations show that to optimize the parameters of predictors provide better results.*

Resumo. *Este artigo analisa a sensibilidade de preditores de suavização exponencial usados para detectar ataques distribuídos de negação de serviço (DDoS). Comparou-se a capacidade de detecção de dois preditores (EWMA e Holt-Winters) com diferentes configurações e cenários. Foi verificado o desempenho através das taxas de falsos positivos e falsos negativos gerados. Foi inserido ataques em traces reais do MAWILab e em amostras reais de tráfego de backbone da RNP com o intuito de realizar simulações de ataques com diferentes volumes de inundação. As simulações mostram que a otimização de parâmetros dos preditores trazem melhores resultados.*

1. Introdução

Cada vez mais, ataques distribuídos de negação de serviço (DDoS) se tornam mais sofisticados e difíceis de detectar. Por isso, desenvolver métodos para combatê-los é uma tarefa desafiadora. Embora existam estudos desde o ano de 2000, ainda não há uma resposta definitiva para a solução deste problema.

Apesar dos avanços na detecção deste tipo de anomalia, especialmente sobre *backbones* de alta velocidade, muitas das abordagens apresentam um custo computacional elevado, requerem mudanças na infraestrutura ou mesmo apresentam baixa sensibilidade a mudanças de comportamento. Por isso, a demanda por métodos mais eficientes justifica o desenvolvimento de estudos nessa área.

Soluções baseadas na correlação de dados e agregação do tráfego em fluxos, parecem ser a tendência para soluções futuras [Feitosa et al, 2008], possibilitando uma detecção antecipada. Essa antecipação pode ser alcançada através da distribuição de detectores em pontos que, embora não sejam objetivos do ataque, constituem vias por onde passam os fluxos destinados à vítima. A eficiência e viabilidade desse tipo de solução depende de uma abordagem colaborativa, onde o esforço conjunto de instituições, através do compartilhamento de dados, pode proteger um número muito

maior de redes e fortalecer o sistema como um todo.

Neste caso, a escolha de métricas mais sensíveis parece ser a mais adequada, já que a concentração esperada de tráfego malicioso é relativamente baixa nesses pontos.

Neste artigo, foi comparado o desempenho de dois estimadores de suavização exponencial bastante empregados, *Exponential Weighted Moving Average* (EWMA) e *Holt-Winters* (HW), aplicados à série temporal formada por medidas de entropia de Shannon, considerando-se diferentes configurações, para a detecção de ataques de inundação. Foi verificado o desempenho através dos índices de falsos positivos (FPOS) e falsos negativos (FNEG) observados em cada cenário, com a inserção de pacotes maliciosos em diferentes níveis de concentração.

Uma série temporal de predição, gerada com o auxílio de estimadores, pode servir como referência para o cálculo das margens de segurança que seriam ultrapassadas após o início do ataque. Normalmente, utiliza-se um fator multiplicativo que determina a amplitude dessas margens. Neste trabalho, verificou-se, também, a influência desse fator multiplicativo, que determina a amplitude dos limites de segurança, na sensibilidade destes estimadores.

No presente trabalho, pode-se destacar as seguintes contribuições:

- proposta de uma metodologia simples para inserção de ataques de inundação, com volume ajustável, para a avaliação de técnicas de detecção baseadas na identificação de anomalias, sem a necessidade de alterar o trace original;
- uma análise da sensibilidade de estimadores de suavização exponencial através da inserção de ataques com diferentes volumes;
- uma análise do desempenho destes estimadores com o emprego de parâmetros otimizados.

O restante do artigo está organizado da seguinte forma: na Seção 2, são discutidos os trabalhos relacionados. Os métodos empregados no corrente trabalho são apresentados na Seção 3. Na Seção 4, é destacada a arquitetura do sistema utilizada. A Seção 5, por sua vez, traz os resultados obtidos através de simulações. Finalmente, na Seção 6, são apresentadas as conclusões.

2. Trabalhos Relacionados

De maneira geral, o combate aos ataques DDoS requer a execução de 3 etapas: (i) identificar a ocorrência de um ataque; (ii) rastrear a origem dos pacotes maliciosos; e (iii) acionar contramedidas que contribuam para a mitigação ou eliminação dos danos causados pelo ataque, tais como filtragem e bloqueio de pacotes [Castelúcio et al 2009].

No que diz respeito à detecção, são propostos diferentes mecanismos baseados em *wavelet* [Kaur et al, 2010], entropia [Lakhina et al, 2005], [Lucena e Moura, 2008], tabela de roteamento [Park e Lee, 2000], *defense by ofense* [Walfish et al, 2010], caracterização do tráfego [Feng e Liu, 2009], marcação de pacotes [Law et al, 2002], que podem adotar uma abordagem *single-link* [Lucena e Moura, 2008], [Demir e Khan, 2010] ou *network-wide* [Chen e Hwang, 2006]. Algumas arquiteturas independem de base histórica [Lin e Uddin, 2005], enquanto que outras têm seus parâmetros adaptados de acordo com uma *baseline* para melhor se ajustar a fatores sazonais [Kline et al, 2008].

Diversos pesquisadores sugerem que a detecção deste tipo de anomalia seja realizada junto à vítima, e que os alertas, bem como o rastreamento e as contramedidas, sejam realizados no sentido contrário do fluxo, como ocorre nos sistemas COSSACK [Papadopoulos et al, 2003] e DefCOM [Mirkovic e Reiher, 2005]. Neste caso, o intuito dos gerentes de rede é proteger a sua própria rede. Entretanto, mesmo com a detecção, o ataque já pode ter comprometido a vítima de alguma maneira e a execução de qualquer medida torna-se mais difícil devido à inundação de dados. Sendo assim, é altamente desejável que a detecção de ataques DDoS ocorra o mais rápido possível, antes que a inundação torne-se generalizada [Chen et al, 2007].

Para conseguir uma detecção antecipada alguns autores recomendam realizar a inspeção de pacotes nos roteadores de borda de Sistemas Autônomos, já que constituem pontos de concentração de fluxo [Park e Lee, 2000], [Lin e Uddin, 2005].

O percentual de pacotes maliciosos que passa por estas interfaces costuma ser relativamente baixo, de forma que as mudanças de comportamento são mais brandas e, por isso, mais difíceis de detectar. Métricas mais sensíveis, como a entropia de Shannon, aplicadas nas distribuições estatísticas dos endereços IP ou dos tamanhos dos pacotes, têm sido consideradas eficazes na detecção de tráfego anormal [Xiang et al, 2011].

Neste artigo, foram testadas configurações otimizadas de dois estimadores a fim de verificar se há uma melhora significativa na precisão da detecção, particularmente em cenários cujo tráfego de ataques DDoS seja mais ameno.

3. Métricas Empregadas para Detecção de Ataques

3.1. Entropia

Em Shannon (1948), foi desenvolvida uma teoria da comunicação com o intuito de tornar melhores os projetos de sistemas de telecomunicações. Trata-se de uma medida da informação contida numa mensagem que Shannon chamou de entropia, e pode ser definida como:

$$E_S = -\sum_{i=0}^{N} p_i \log_2\left(p_i\right) \quad (1)$$

Onde N é o número de diferentes ocorrências no espaço amostral e p_i é a probabilidade associada a cada ocorrência i. O resultado varia entre *zero* e $\log_2 N$, onde *zero* indica concentração máxima na distribuição medida, quando ocorre um único valor de i, e $\log_2 N$ indica máxima dispersão na distribuição medida, quando todas as ocorrências têm a mesma probabilidade de ocorrência. No corrente trabalho, esta medida foi aplicada ao conjunto de endereços IP em cada intervalo considerado, a fim de identificar mudanças bruscas de padrão com o passar do tempo.

3.2. Estimadores

Uma série temporal de predição, gerada com o auxílio de estimadores, pode servir como referência para o cálculo das margens de segurança que seriam ultrapassadas após o início do ataque. No presente trabalho foram aplicados dois estimadores à série temporal dos valores de entropia referente ao tráfego observado.

1) Exponentially weighted moving average (EWMA) - Como o próprio nome diz,

trata-se de um método que faz o cálculo da média móvel exponencialmente ponderada, também conhecido como suavização exponencial simples (*simple exponential smoothing*). Pode ser expressa da seguinte maneira:

$$x_{t+1} = \alpha X_t + (1 - \alpha) x_t \quad (2)$$

Onde x_t representa a média estimada no instante t e X_t é o valor atual real. O valor de α reflete o peso conferido ao valor mais recente, e assume valores entre 0 e 1.

Não é difícil perceber que, a cada iteração, as estimativas mais antigas perdem a influência no resultado calculado de maneira exponencial, de forma que quanto mais recente o valor, maior o peso creditado a ele. Dessa forma, o valor estimado representa uma média ponderada cujos valores mais recentes têm maior peso. Por conta disso, o traçado da série de estimativa gerada se assemelha ao traçado obtido com os valores reais. Quanto menor o valor de α, maior a suavidade no traçado da série.

2) Holt-Winters (HW) - Trata-se de um método de suavização exponencial tripla (*triple exponential smoothing*), que costuma ser empregado quando os dados da série apresentam tendência e sazonalidade. Para lidar com essas duas características, são utilizados mais dois parâmetros além daquele empregado na suavização exponencial simples em três equações que formam um conjunto resultante denominado *Holt-Winters* (HW). Existem dois modelos principais de HW, aditivo e multiplicativo, que tratam a sazonalidade de maneiras ligeiramente distintas [Kalekar et al, 2004]. No corrente trabalho, foi utilizado o modelo aditivo, que é calculado a partir das seguintes expressões:

$$a_t = \alpha (X_t - c_{t-m}) + (1 - \alpha)(a_{t-1} + b_{t-1}) \quad (3)$$

$$b_t = \beta (a_t - a_{t-1}) + (1 - \beta) b_{t-1} \quad (4)$$

$$c_t = \gamma (X_t - a_t) + (1 - \gamma) c_{t-m} \quad (5)$$

$$x_{t+1} = a_t + b_t + c_{t+1-m} \quad (6)$$

Onde x_t representa a média estimada no instante t e X_t é o valor atual real. a_t denota a componente residual, b_t, a componente de tendência de crescimento, c_t, a componente de periodicidade da série e m representa o tamanho do período. Os parâmetros α, β e γ refletem a importância conferida a cada componente.

4. Arquitetura do Sistema

A ocorrência de um DDoS causa uma mudança acentuada na distribuição de endereços IP de destino, de forma que a entropia desta informação sofre uma queda abrupta.

Sendo assim, para identificar esta anomalia, a arquitetura utilizada prevê a montagem de séries temporais contendo medidas de entropia obtidas nas distribuições estatísticas dos endereços IP de destino, extraídas a cada intervalo de tempo considerado. A partir dos valores reais de entropia, monta-se a série temporal de predição, gerada com o auxílio dos estimadores.

Após montar essas séries, as margens de segurança podem ser calculadas. Para

isso foi utilizada uma expressão de suavização exponencial simples para o erro de estimativa.

$$e_t = \gamma |X_t - x_t| + (1 - \gamma) e_{t-m} \quad (7)$$

Onde e_t representa o erro de estimativa no instante t. A componente é atualizada a cada erro calculado, levando em conta os erros do período anterior.

De acordo com Brutlag (2000), baseando-se na teoria de distribuição estatística e em algumas suposições, este erro deve ser multiplicado por um valor de escala δ para poder compor as margens de segurança. Valores normalmente empregados para δ estão entre 2 e 3, de acordo com Ward et al (1998).

Sabe-se que a largura das margens de segurança influencia no índice de FPOS e FNEG, e que esta largura é diretamente proporcional ao valor atribuído a δ. Sendo assim, verificou-se, também, os resultados obtidos com limites mais largos, que aqui chamamos de AMPLOS, e mais ajustados, que aqui chamamos de RIGOROSOS. No primeiro caso, atribuiu-se o valor 3 a δ, enquanto que no segundo, atribuiu-se o valor 2.

Dessa forma, quando o valor real ultrapassa os limites, um alerta é emitido. Os limites superior e inferior podem ser calculados a partir das seguintes expressões:

$$lim_{Sup} = x_t + \delta . e_{t-m} \quad (8)$$

$$lim_{Inf} = x_t - \delta . e_{t-m} \quad (9)$$

Na Figura 1, pode-se observar dois exemplos de resultados obtidos com a utilização da arquitetura empregada. A linha azul representa os valores de entropia, calculados a partir dos dados extraídos dos traces e ataques inseridos. A linha laranja, por sua vez, representa as estimativas de HW, calculadas a partir dos valores reais, enquanto que as linhas vermelha e ocre indicam os limites inferior e superior, respectivamente.

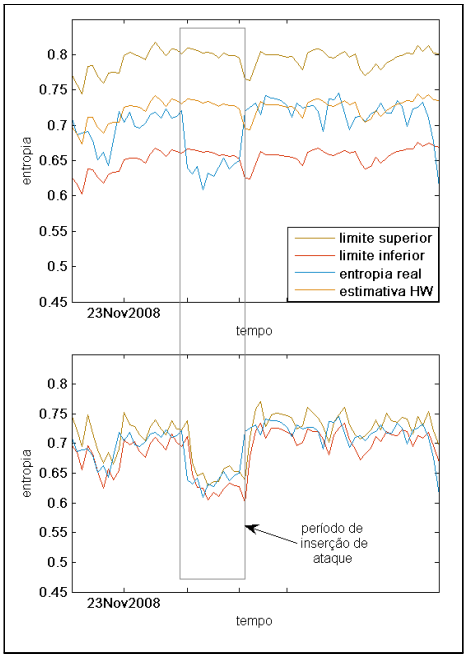

Figura 1. Exemplos de resultados com estimativas de Holt-Winters

Destaca-se nos gráficos da Figura 1 um período de inserção de ataque que foi identificado em ambos os casos. Quando o valor real ultrapassa o limite inferior, emite-se um alerta, que pode caracterizar a ocorrência de um FPOS, caso não haja um ataque, ou a detecção do DDoS, caso haja.

Pode-se perceber, também, alguns pontos com violações do limite inferior que ocorreram fora do período de ataque, particularmente no segundo gráfico desta Figura, quando foram empregados parâmetros otimizados. Estes eventos caracterizam a ocorrência de FPOS.

5. SIMULAÇÕES

Foram realizadas diversas simulações com o intuito de comparar os índices de FPOS e FNEG obtidos com cada configuração de parâmetros. Duas configurações foram empregadas: na primeira, aqui chamada de PADRÃO, foram utilizados os valores dos parâmetros α, β e γ baseados em Brutlag (2000); na segunda, aqui chamada de ÓTIMA, utilizou-se valores que garantiam o menor erro de estimativa sem a presença de ataques. Estes valores foram obtidos empiricamente, como descrito na Seção 5.2.

Para obter os resultados necessários, foi implementado em C++ um programa capaz de realizar todos os cálculos referentes à montagem das séries temporais, desde a agregação dos endereços contidos no mesmo intervalo considerado até a contabilização de FPOS e FNEG.

5.1. Bases de dados

Foram utilizadas as informações de traces reais (MAWILab), coletados pelo *WIDE Project* e disponibilizados em: http://www.fukuda-lab.org/mawilab/, e de amostras reais de tráfego oriundas do backbone da RNP, gentilmente cedidas pelo Centro de Engenharia e Operações da RNP, mediante solicitação. Na Tabela 1 são apresentadas algumas características desses traces, que também podem influenciar nos resultados finais.

Tabela 1. Características dos traces utilizados

		Base de dados	
		RNP	**MAWILab**
Período de observação	**Datas**	De 20Nov08, 0:00h, a 27Nov08, 0:00h	07Jun10, de 14:00h às 14:15h e 06Dez10, de 14:00h às 14:15h
	Tempo por dia	24 horas	15 minutos
	Total	7 dias (ininterruptos)	30 min (07Jun10 e 06Dez10)
Intervalo		5 minutos	1 segundo
Capacidade do enlace		2.5 Gbps	150 Mbps
Amostragem		1:100	Sem amostragem
Formato		NetFlow versão 5	.dump
Taxa média real		30 Kpps	48 Kpps

Devido ao pequeno período de observação disponibilizado nos traces do MAWILab, 15 minutos por dia, foi necessário realizar o estudo com séries temporais de 1 segundo. Além disso, verificou-se uma sazonalidade nos traces do RNP, não presente

nos traces do MAWILab. A partir desses traces, foram montadas séries temporais das entropias dos endereços de destino em intervalos fixos de 5 minutos, para RNP, e de 1 segundo, para MAWILab.

5.2. Obtenção de Parâmetros Otimizados

Procurou-se pelos parâmetros dos estimadores EWMA e Holt-Winters que fornecessem os menores somatórios de erros de estimativa num período de tráfego livre de ataques. Para fins de estudo, considerou-se que os traces estudados estariam livres de ataques.

A partir desses traces, foram montadas séries temporais das entropias dos endereços de origem e destino para intervalos fixos de 5 minutos, para RNP e de 1 segundo, para MAWILab. Essas séries serviram de base para a montagem das estimativas, que variam de acordo com a escolha dos parâmetros α, β e γ. Foram testados valores entre 0 e 1 e com precisão de três casas decimais. O mesmo foi feito para o parâmetro da EWMA. A combinação que forneceu o menor somatório de erros foi eleita como a mais adequada para os traces estudados, de acordo com a Tabela 2.

Tabela 2. Parâmetros otimizados para estimadores HW e EWMA

Trace	ESTIMADOR			
	Holt-Winters			EWMA
	α	β	γ	α
RNP	0.775	0.005	0.035	0.690
MAWILab	0.630	0.010	0.058	0.653

Pode-se perceber na Tabela 2 que os valores de β e γ são bem menores que os de α. Esses valores evidenciam o peso de cada componente de suavização exponencial na estimativa. Sendo assim, as componentes ligadas à sazonalidade e à tendência de crescimento, apresentam menor influência na estimação dos próximos valores.

5.3. Inserção de Ataques

Para validar os métodos de detecção foi necessária a inserção de ataques gerados artificialmente. Para tanto, alguns pressupostos foram assumidos:

- Traces originais livres de ataques ou com percentual irrelevante de fluxos maliciosos;
- Volume máximo de tráfego suportado pelos roteadores desprezado;
- Descartes e atrasos de pacotes, devido ao volume de tráfego inserido, não implementados.

As anomalias são identificadas já no início dos ataques, quando há uma mudança de comportamento do tráfego, por isso as considerações acima não invalidam as simulações realizadas, já que parte dos efeitos colaterais causados pelo tráfego adicional, e que foram desconsiderados durante a inserção, ocorre após a detecção. Essa abordagem permite uma implementação mais simples, uma vez que basta acrescentar ao tráfego original as informações dos pacotes maliciosos.

Outros fatores foram considerados para determinar a metodologia de inserção:

- Foco na detecção de ataques DDoS caracterizados por grande volume de tráfego;
- Anomalias presentes na distribuição de probabilidade de endereços de destino.

Optou-se pela inserção de ataques com taxa fixa de pacotes, destinados a uma mesma vítima, e número fixo de atacantes. Foram inseridos 15 ataques com duração fixa de 10 unidades de tempo, e espaçados entre si em 50 unidades. Dessa forma, foi possível avaliar a capacidade de detecção em diferentes instantes do período observado.

Para cada trace, foram seguidos os seguintes passos para a inserção:

Passo 1: Cálculo do número médio de pacotes por intervalo de tempo para todo o período;

Passo 2: Cálculo do percentual a ser acrescentado;

Passo 3: Seleção dos intervalos para inserção;

Passo 4: Seleção de número de atacantes;

Com o intuito de verificar a sensibilidade de cada métrica, foram realizadas simulações com a inserção de 50, 25, 20, 15, 10 e 5% do volume médio de pacotes transitado no período, de acordo com a Tabela 3.

Tabela 3. Número de Pacotes acrescentados na inserção de ataque

Volume Médio Inserido	Número de pacotes por janela	
	RNP (5 min)	MAWILab (1 seg)
50%	42.336	23.743
25%	21.168	11.872
20%	16.935	9.497
15%	12.701	7.123
10%	8.467	4.748
5%	4.234	2.374

Na Tabela 4 são apresentados alguns valores referentes aos ataques 7.7 e 3.4, para fins de comparação com os ataques inseridos neste trabalho. Nota-se que 10% do volume médio do trace do MAWILAb, por exemplo, representa um valor 128 vezes menor que o número de pacotes por segundo (PPS) por vítima observado no ataque 7.7. Percebe-se, também, que o número de PPS por vítima deste ataque é aproximadamente 1.825 vezes maior do que 100% do volume médio do trace da RNP. Desta forma, pode ser inferido que os valores utilizados nas inserções de ataque do corrente trabalho poderiam ser observados em pontos afastados de vítimas de ataques de inundação.

Tabela 4. Características dos ataques 7.7 e 3.4. Fonte (Ahnlab, 2011)

	Ataque 7.7 (07/07/2009)	Ataque 3.4 (04/03/2011)
Tráfico por zumbi	103 PPS	389 PPS
Número de zumbis	115.044	116.299
PPS total	11.849.532	45.240.311
Número de vítimas	23	40
PPS por vítima	515.197	1.131.007

A inserção foi realizada durante a extração dos dados, de acordo com a Figura 2, sem a necessidade de alterar o trace original.

Inicialmente, os endereços IP de destino dos pacotes presentes em cada intervalo são extraídos do trace, de forma a se obter as distribuições de probabilidade para este parâmetro. Em seguida, uma rotina verifica se deve ou não ocorrer a inserção de pacotes, de acordo com os períodos de ataque escolhidos antes da simulação. Caso seja um período de ataque, altera-se o número de pacotes destinados à vítima, adicionando-se o valor listado na Tabela 3. A escolha da vítima que recebe os 15 ataques é realizada na primeira inserção através de sorteio. Após isso, calcula-se a entropia deste parâmetro no intervalo considerado, com ou sem inserção de dados, e atualiza-se a série temporal acrescentando-se o valor calculado.

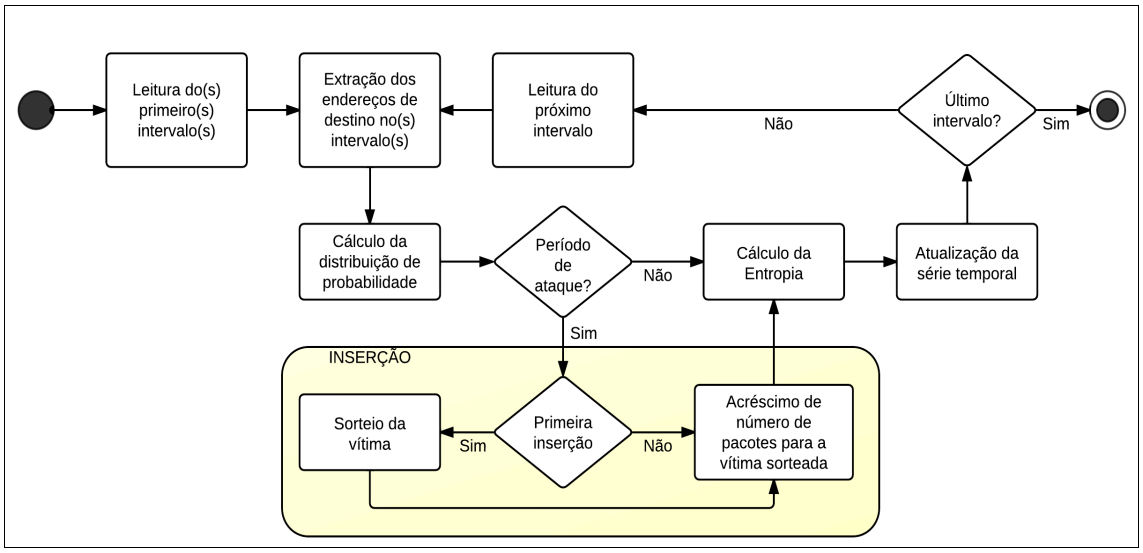

Figura 2. Algoritmo para inserção de ataques em tempo de execução

5.4. Resultados MAWILab

Observando-se a Figura 3, pode-se verificar que, com a inserção de 15%, 10% e 5% do volume médio transitado, fica mais evidente a capacidade de detecção de cada métrica. Como os ataques são menos expressivos, as mudanças de comportamento são mais brandas e, por isso, mais difíceis de detectar.

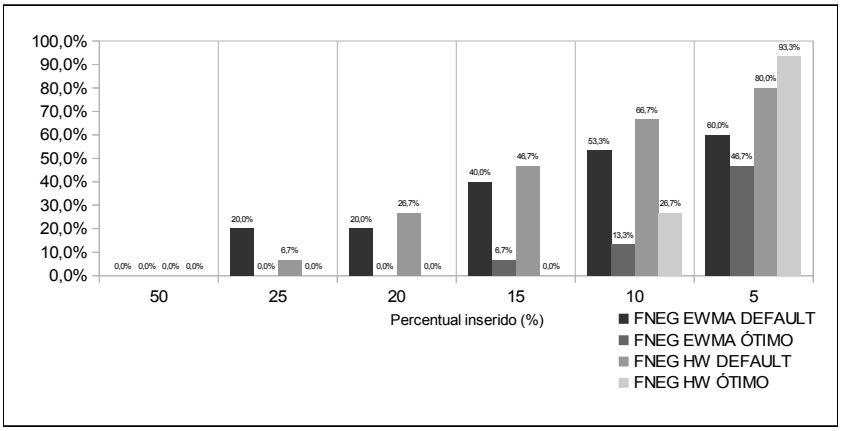

Figura 3. Índice de FNEG no MAWILab com limites amplos

Na inserção de 5%, tanto com limites rigorosos (Figura 4) quanto com limites amplos (Figura 3), observou-se o menor índice de FNEG com o emprego do estimador

EWMA e parâmetros otimizados, cujos índices de erro alcançaram 20% e 46,7%, respectivamente. Para limites rigorosos, o segundo melhor resultado foi obtido com o estimador HW e parâmetros ótimos. Entretanto, para limites amplos, observou-se para o HW com parâmetros ótimos um crescimento exponencial do número de FNEG na inserção de 5%, quando 93,3% de ataques não são detectados.

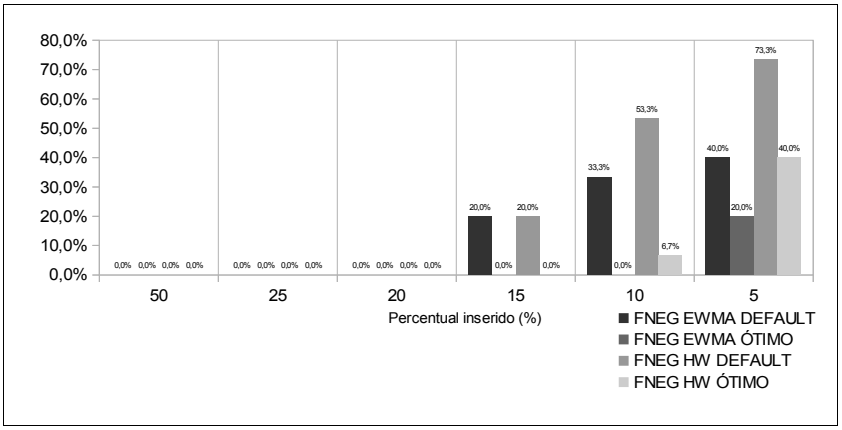

Figura 4. Índice de FNEG no MAWILab com limites rigorosos

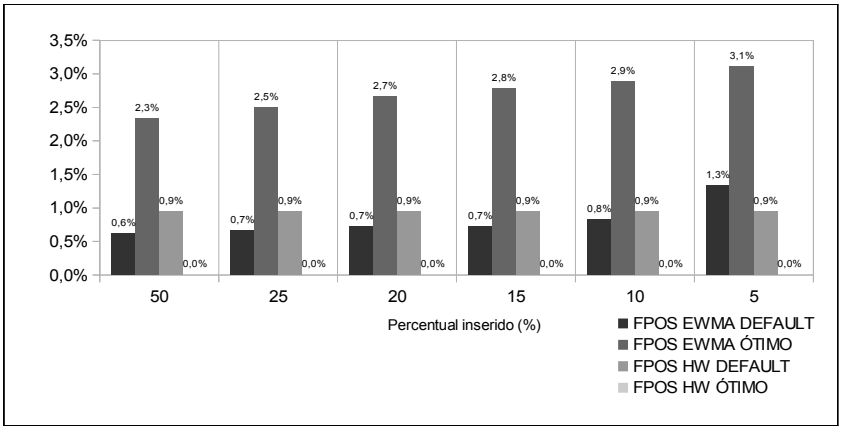

Figura 5. Índice de FPOS no MAWILab com limites amplos

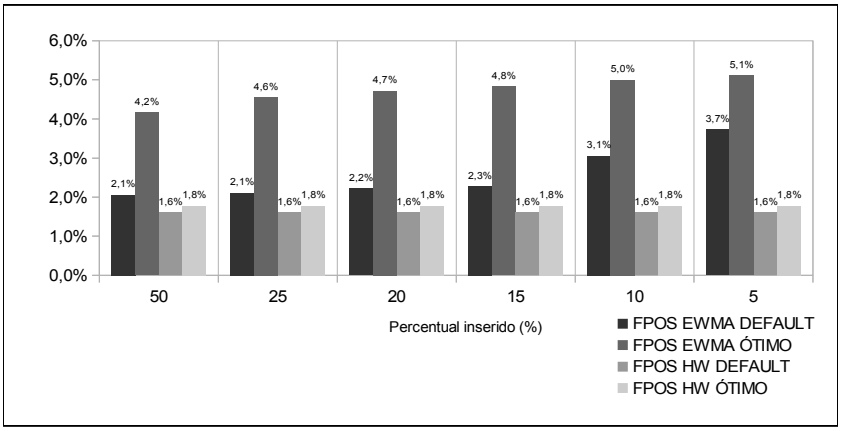

Figura 6. Índice de FPOS no MAWILab com limites rigorosos

No que diz respeito ao índice de FPOS, observou-se valores relativamente baixos nas simulações. A variação desse índice, devido à mudança do volume de ataque inserido

e ao tipo de limite adotado, também foi relativamente pequena, como pode ser visto na Figura 5 e na Figura 6. Observa-se que o valor máximo obtido foi de 5,11%, quando se utilizou o EWMA com parâmetros otimizados e limites rigorosos. As menores taxas de FPOS foram obtidas com o emprego do HW.

Dessa forma, particularmente para ataques menos volumosos, o estimador que apresentou melhor desempenho na detecção de ataques neste enlace, foi o EWMA com parâmetros otimizados. Quanto aos limites, fica evidente a vantagem de se empregar os rigorosos, dado o pequeno aumento dos índices de FPOS, e a grande diminuição nos índices de FNEG. Esta vantagem foi maior para o HW com parâmetros ÓTIMOS, dado o alto índice de FNEG obtido com o limites amplos.

5.5. Resultados RNP

Pode-se perceber pela Figura 7 que, nos traces do RNP, os menores índices de FNEG foram obtidos com o emprego de parâmetros otimizados. Pode-se observar, também, que nas simulações com limites amplos, o número de FNEG cresce mais rapidamente com o EWMA, de forma que, a 10% e 5% de inserção, o HW com parâmetros otimizados apresentou menores índices de erro.

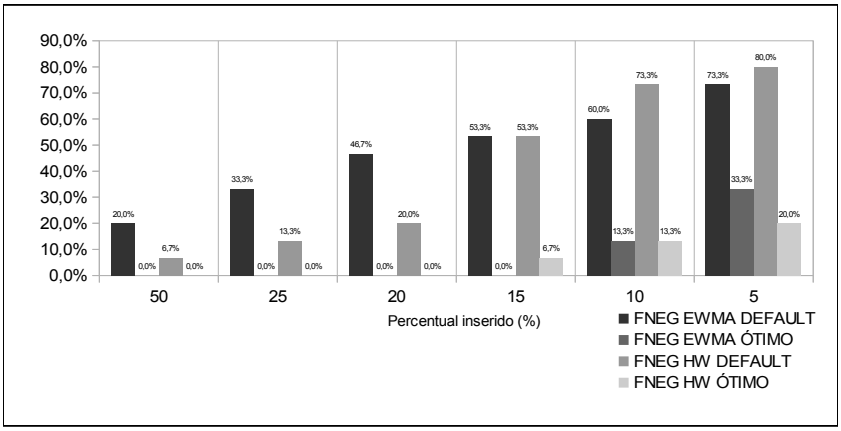

Figura 7. Índice de FNEG no RNP com limites amplos

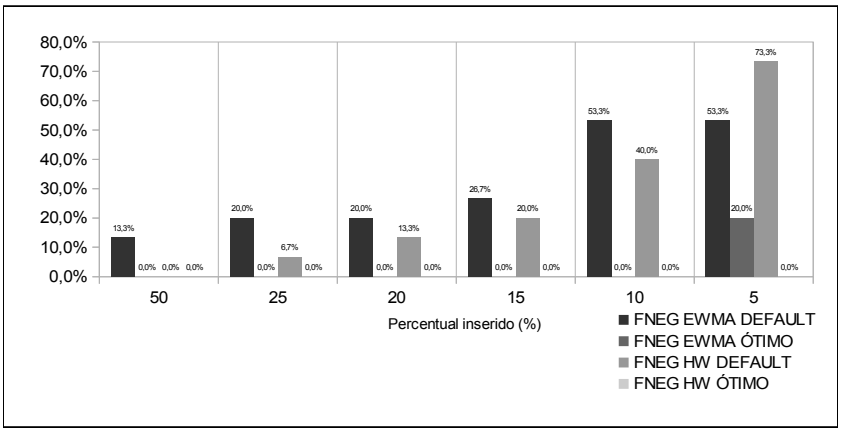

Figura 8. Índice de FNEG no RNP com limites rigorosos

Além disso, verificou-se que, mesmo a 5% de inserção, o índice de FNEG do HW com parâmetros otimizados foi de 0% (Figura 8). Dessa forma, pode-se dizer que, para esse enlace, o estimador que apresentou o melhor desempenho foi o HW com parâmetros otimizados, tanto para limites amplos como para rigorosos.

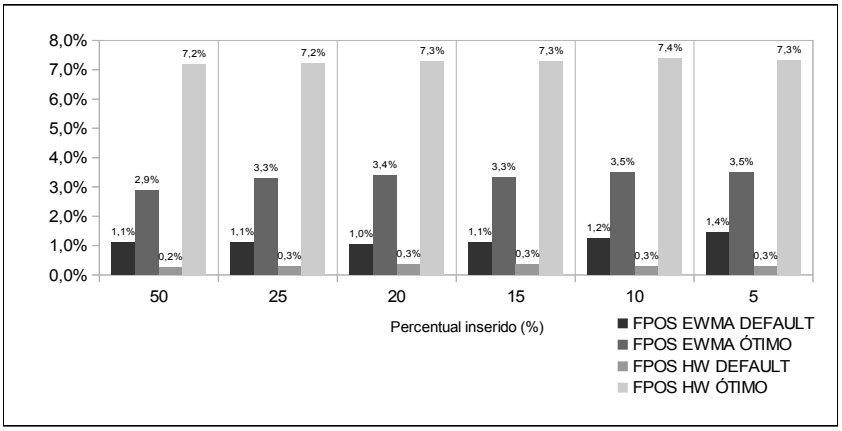

Figura 9. Índice de FPOS no RNP com limites amplos

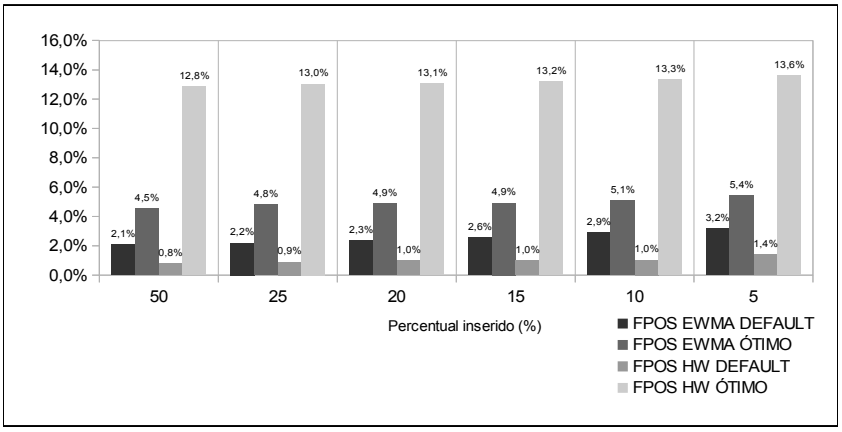

Figura 10. Índice de FPOS no RNP com limites rigorosos

Assim como ocorre com o MAWILab, o índice de FPOS muda muito pouco com a variação do volume de ataque inserido. Entretanto, a utilização de limites mais rigorosos quase que duplica o número de FPOS, que, ainda assim, não alcança percentuais muito expressivos. No pior caso, observado com o HW otimizado e limites rigorosos, o índice de FPOS alcançando foi de 13,64%. Com limites mais amplos, esse valor cai para 7,32%. Pode-se observar na Figura 9 e na Figura 10 que o índice de FPOS obtido com o HW equivale a pouco mais que o dobro daquele alcançado com o EWMA, onde os valores não ultrapassam 5,43%, com limites rigorosos, e 3,48%, com limites amplos.

6. CONCLUSÃO

Neste artigo, foram avaliados dois métodos de detecção de anomalias de tráfego de rede, baseados na extração de entropias de endereços IP e no uso de estimadores (EWMA e HW). Foram verificados dois tipos de configuração (PADRÃO e ÓTIMA), com o intuito de encontrar qual a combinação mais adequada para a detecção de ataques em pontos afastados da vítima, onde o volume de tráfego malicioso ainda é baixo,

considerando-se um cenário colaborativo. Verificou-se, também, o desempenho dessas métricas com o uso de limites AMPLOS e RIGOROSOS.

De maneira geral, pode-se observar que o desempenho dos estimadores diminui a medida em que o volume do ataque inserido é reduzido (de 50% até 5%). Embora não haja alterações significativas nos índices de FPOS, os índices de FNEG aumentam expressivamente a medida em que o volume do ataque diminui.

Diante do exposto, conclui-se que a utilização de parâmetros otimizados e limites mais ajustados aumenta expressivamente a sensibilidade das duas métricas estudadas, trazendo melhores taxas de detecção em ambos os traces. Foi observado um aumento nos índices de FPOS, devido ao maior ajuste dos limites de segurança, embora essa alteração tenha sido relativamente pequena. Por outro lado, os índices de FNEG diminuíram significativamente com parâmetros ÓTIMOS. Por essa razão, a utilização dos estimadores com parâmetros ÓTIMOS em ambientes colaborativos, ou mesmo naqueles onde se deseja identificar volumes menos expressivos de ataque, apresentam uma relação custo-benefício mais vantajosa. Vale salientar que o estimador HW trouxe melhores índices de FNEG apenas para o trace do RNP, devido ao comportamento sazonal identificado neste.

7. Referências

Ahnlab, INC. “Analytical report on 3.4 DDoS attack, White Paper”, (2011), http://www.ahnlab.com , April.

Feitosa, E. L., Souto E. J. P. e Sadok D. (2008) “Tráfego Internet não Desejado: Conceitos, Caracterização e Soluções”, Livro-Texto dos Minicursos do VIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, p. 91-137.

Castelúcio, A. O., Salles, R. M. e Ziviani, A. (2009) “An AS-Level Overlay Network for IP Traceback”, IEEE Network, Vol. 23, pp. 36-41.

Kaur, G., Saxena, V. e Gupta, J. P. (2010) “Anomaly Detection in network traffic and role of wavelets”, 2nd International Conference on Computer Engineering and Technology (ICCET), v.7, p.46-51.

Lakhina, A., Crovella, M. e Diot, C. (2005) “Mining anomalies using traffic feature distributions”, Proceedings of the ACM SIGCOMM'2005, Philadelphia, PA, USA.

Lucena, S. C. e Moura, A. S. (2008) “Detecção de Anomalias Baseada em Análise de Entropia no Tráfego da RNP”, XIII Workshop de Gerência e Operação de Redes e Serviços (WGRS), Rio de Janeiro. Anais do XIII Workshop de Gerência e Operação de Redes e Serviços, p. 163-176.

Park, K. e Lee, H. (2000) “A Proactive Approach to Distributed DoS Attack Prevention using Route-Based Packet Filtering”, Technical Report CSD-TR-00-017, Purdue University, Dept. of Computer Sciences.

Walfish, M., Vutukuru, M., Balakrishnan, H., Karger, D. R. e Shenker S. (2010) “DDoS defense by offense”, ACM Transactions on Computer Systems (TOCS), Journal Vol. 28, Issue 1.

Feng, J. e Liu, Y. (2009) "The Research of DDoS Attack Detecting Algorithm Based on the Feature of the Traffic", Networking and Mobile Computing 5th International Conference on Wireless Communications (WiCom'09).

Law, K. T., Lui, J. C. S. e Yau, D. K. Y. (2002) "An Effective Methodology to Traceback DDoS Attackers", X IEEE Int'l Symp, MASCOTS'02.

Demir, O. e Khan, B. (2010) "Quantifying Distributed System Stability through Simulation: A Case Study of an Agent-Based System for Flow Reconstruction of DDoS Attacks", IEEE, 2010 ISMS, Liverpool, England, January.

Chen, Y. e Hwang, K. (2006) "Collaborative Change Detection of DDoS Attacks on Community and ISP Networks", IEEE Networks, pp. 401 - 410.

Lin, B. P. e Uddin M. S. (2005) "Synmon Architecture for Source-based SYN-flooding Defense on Network Processor", IEEE, 2005 Asia-Pacific Conference on Communications, Perth, Western Australia.

Kline, J., Nam, S., Barford, P., Plonka, D. e Ron, A. (2008) "Traffic Anomaly Detection at Fine Time Scales with Bayes Nets", The Third International Conference on Internet Monitoring and Protection, ICIMP'08, PP. 37-46.

Papadopoulos, C., Lindell, R., Mehringer, J., Hussain, A. e Govindan, R. (2003) "COSSACK: Coordinated Suppression of Simultaneous Attacks", Proc. Third DARPA Information Survivability Conf. and Exposition (DISCEX-III'03), pp.2-13.

Mirkovic, J. e Reiher, P. (2005) "D-WARD: A Source-End Defense against Flooding DoS Attacks", IEEE Trans. Dependable and Secure Computing, pp. 216-232.

Chen, Y., Hwang, K. e Ku, W. S. (2007) "Collaborative Detection of DDoS Attacks over Multiple Network Domains", IEEE Transactions on Parallel and Distributed Systems, Vol. 18, Issue 12, pp. 1649 - 1662.

Xiang, Y., Li, K., e Zhou, W. (2011) "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 2.

Shannon, C. E. (1948) "A mathematical theory of communication", Bell System Technical Journal, 27:379-423 and 623-656.

Kalekar, P. S. e Rekhi, K. (2004) "Time series Forecasting using Holt-Winters Exponential Smoothing", School of Information Technology, December 6.

Brutlag, J. D. (2000) "Aberrant Behavior Detection in Time Series for Network Monitoring". Proceedings of the 14th Systems Administration Conference (LISA 2000).

Ward, A., Glynn, P. e Richardson, K. (1998) "Internet Service Performance Failure Detection", ACM SIGMETRICS Performance Evaluation Review, Vol. 26, No. 3.

