A Evolução do Parâmetro de Hurst e a Destruição da Auto-Semelhança Durante um Ataque de Rede Intenso

Pedro R. M. Inácio[1,2,a], Mário M. Freire[1,b],
Manuela Pereira[1,c], Paulo P. Monteiro[2,3,d]

[1]IT-Networks and Multimedia Group
Departamento de Informática
Universidade da Beira Interior
Rua Marquês de Ávila e Bolama
6201-001 Covilhã, Portugal
{[b]mario,[c]mpereira}@di.ubi.pt

[2]Nokia Siemens Networks Portugal S.A.,
Rua Irmãos Siemens, no. 1,
2720-093 Amadora, Portugal
[a]pedro.inacio@nsn.com, [d]paulo.1.monteiro@nsn.com

[3]Instituto das Telecomunicações - Pólo de Aveiro,
Universidade de Aveiro,
3810-193 Aveiro, Portugal

Resumo

A propriedade matemática conhecida como *auto-semelhança* tem sido o assunto de inúmeras contribuições científicas na área das redes de computadores. Por definir parcialmente a natureza do tráfego em nós onde este é agregado, a referida característica pode tornar-se num potencial factor de diferenciação na presença de algumas anomalias. Este artigo resume um estudo ao comportamento do parâmetro que mede o grau de auto-semelhança (o parâmetro de Hurst) face a um ataque com expressão significativa ao nível do tráfego de rede, e avalia a resiliência da propriedade em função da intensidade daquele. A análise é conduzida recorrendo à simulação de tráfego auto-semelhante e a versões modificadas de dois estimadores do parâmetro Hurst, que permitem processamento do sinal de entrada de modo computacionalmente eficiente e ponto-a-ponto, para uma janela de valores fixa. A perca da auto-semelhança é avaliada através de dois testes estatísticos. Os resultados obtidos provam que a presença de um ataque não resulta necessariamente na destruição da auto-semelhança e que, independentemente disso, os valores devolvidos pelos dois estimadores aumentam assim que o tráfego relativo ao ataque entra na janela de observação.

1 Introdução

A propriedade matemática conhecida como *auto-semelhança* tem sido o assunto de inúmeras contribuições científicas na área das redes de computadores. A sua popularidade deve-se sobretudo ao facto de esta explicar a razão do tráfego chegar por *rajadas* a pontos de agregação, produzindo um efeito directo sobre os parâmetros de *Qualidade de Serviço* das ligações. Por definir parcialmente a natureza do tráfego de rede [8; 11; 16], alguns investigadores encontraram na auto-semelhança uma oportunidade para modelar tráfego *bem comportado*, propondo a sua análise como um meio para detectar intrusões ou anomalias [2; 5; 9; 14].

O presente documento visa descrever o impacto de um ataque no grau de auto-semelhança do tráfego de rede. Ao longo da descrição ficará mais claro que o tipo de ataques referidos recaí naqueles cuja execução adquire alguma expressão estatística ao nível da largura de banda ocupada num ponto de agregação da rede. Esses ataques são aqui designados de *ataques de rede intensos*. O estudo aqui reportado fez uso de dois estimadores do parâmetro de Hurst (que é considerada a medida do grau de auto-semelhança), que foram alterados de maneira a devolver estimativas ponto-a-ponto, e para uma janela de valores com tamanho fixo e ambulante. A evolução da propriedade pode assim ser investigada para um contexto local e de modo contínuo. O funcionamento dos dois métodos modificados é inovador, assim como a perspectiva por eles produzida. A análise é desprovida de quaisquer pressupostos iniciais acerca da preservação ou perda daquela propriedade estatística, sendo esse um dos aspectos apurados ao longo da descrição que se segue.

A parte restante deste documento está organizada da seguinte forma. A secção 2 apresenta matematicamente os principais conceitos relativos à auto-semelhança, e discute brevemente a sua expressão no tráfego de rede. A secção 3 contém uma análise crítica às referências que se debruçaram de modo mais vincado sobre o tema deste artigo. A secção 4 apresenta os métodos usados durante o trabalho de investigação na estimação do grau de auto-semelhança, e descreve brevemente o procedimento de geração de tráfego de rede. A mesma secção relata a forma de simular e injectar ataques nos registos de tráfego *legítimos*. Na secção 5 incluem-se e interpretam-se os resultados obtidos por simulação. A secção 6 apresenta as principais conclusões deste documento.

2 Auto-Semelhança e sua Expressão no Tráfego de Rede

Esta secção formaliza a propriedade da auto-semelhança e discute em que aspecto do tráfego de rede esta se manifesta.

2.1 Auto-Semelhança e Parâmetro de Hurst

A auto-semelhança é definida em termos de condições estatísticas. Um determinado processo estocástico $\{X(t)\}_{t\geq 0}$, definido para $t \geq 0$ é dito *auto-semelhante*, com *parâmetro de Hurst* H, se a equação (1) for verdadeira para qualquer valor positivo de $a \epsilon \mathbb{R}$. Note-se que o símbolo $\stackrel{d}{=}$, na referida equação, denota *igualdade em distribuição*.

$$X(t) \stackrel{d}{=} a^{-H} X(at). \tag{1}$$

Considere a particularização da definição anterior para processos com domínio temporal discreto. Nesses termos, a definição que melhor serve o propósito da explicação da auto-semelhança na área da análise de tráfego é baseada no chamado *processo das diferenças de primeira ordem* $\{Y(t)\}_{t\geq 0}$, dado por $Y(t) = X(t+1) - X(t)$. O processo $\{X(t)\}_{t \epsilon \mathbb{N}}$ é dito auto-semelhante se o seu processo das diferenças de primeira ordem respeitar a condição (2), para qualquer m positivo e inteiro. Por vezes, também se diz que $\{Y(t)\}_{t \epsilon \mathbb{N}}$ é auto-semelhante no sentido dado pela condição (2), e m é normalmente designado por *escala de agregação* [8].

$$Y(t) \stackrel{d}{=} m^{1-H} Y^{(m)}(i), \text{ onde } Y^{(m)}(i) = m^{-1} \left(X(i.m) + ... + X((i+1).m) \right). \tag{2}$$

Se a correlação de $\{Y(t)\}_{t \epsilon \mathbb{N}}$ e de $\{Y^{(m)}(i)\}_{i \epsilon \mathbb{N}}$ for a mesma para todo o $m \epsilon \mathbb{N}$, então $\{Y(t)\}_{t \epsilon \mathbb{N}}$ é dito ser *exactamente auto-semelhante de segunda ordem*. Se, por outro lado, a correlação de $\{Y(t)\}_{t \epsilon \mathbb{N}}$ e a de $\{Y^{(m)}(i)\}_{i \epsilon \mathbb{N}}$ só coincidirem para $m \rightarrow \infty$, o processo é dito ser *assimptoticamente auto-semelhante de segunda ordem*. Quando o parâmetro de Hurst é superior a 0.5 e inferior a 1, $\{X(t)\}_{t \epsilon \mathbb{N}}$ (ou $\{Y(t)\}_{t \epsilon \mathbb{N}}$ no sentido dado por (2)) exibe a propriedade da *persistência* ou da *dependência de longo-alcance*.

2.2 Expressão da Auto-Semelhança no Tráfego de Rede

O estudo que chamou a atenção da comunidade cietífica para a relação entre auto-semelhança e o tráfego de rede foi levado a cabo por Leland et al. e reportado exaustivamente em [8], publicado em 1994. O artigo entitulado *On the Self-Similar Nature of Ethernet Traffic* apresenta os resultados do estudo conduzido para registos de tráfego de uma rede de área local, implementada sobre *Ethernet*. Segundo a referida análise, a *dependência de longo-alcance* é fruto da agregação de processos com memória curta, mas cuja função de distribuição de probabilidades é uma curva com cauda alargada. Em [8; 16], cada fonte de tráfego (cada nó terminal) é modelada como uma variável independente que toma o valor 1 (=ON), sempre que o terminal está a transmitir, e o valor 0 (=OFF) quando está em silêncio. O número de bits por unidade de tempo que chegam a um determinado ponto de rede meeiro é então o resultado da agregação (soma) de diversos processos concorrentes, independentes e identicamente distribuídos, e é precisamente nessa métrica do tráfego que a auto-semelhança se revela. O *processo do número de bits por unidade de tempo* é assimptoticamente auto-semelhante de segunda ordem e a sua fisionomia é parecida com a do *ruído Gaussiano fraccionário* (rGf), um processo exactamente auto-semelhante no sentido dado por (2), com distribuição Gaussiana.

3 Trabalhos Relacionados

Dado a auto-semelhança definir parcialmente a natureza do tráfego em pontos de agregação, alguns estudos [2; 5; 9; 14] encontraram nessa propriedade uma oportunidade de categorizar o tráfego, e de detectar anomalias relacionadas com intrusões. A maior parte desses estudos [2; 5; 14] partem do pressuposto de que a auto-semelhança é perdida durante um ataque de rede intenso.

No início do artigo de Ming [9], a análise parece direccionada ao entendimento do comportamento do parâmetro de Hurst durante um ataque, mas acaba por concretizar um trabalho confuso, cujas conclusões colidem com as dos outros, e mesmo com as deste trabalho. A conclusão de que o parâmetro de Hurst decresce durante uma intrusão é fruto de uma análise ao *tamanho das unidades de dados*, ao invés de ter sido conduzida para o *processo da quantidade de informação por unidade de tempo*.

O trabalho relatado em [5] é mais vocacionado para a descoberta do melhor tamanho da janela de observação, que para a análise da auto-semelhança. O artigo é construído à volta do que os seus autores chamaram de *método de optimização*, cujo racional se resume à análise sucessiva do mesmo processo para tamanhos amostrais cada vez maiores, e à identificação do volume de pontos da melhor taxa de detecção. Após escassa discussão, e sem apresentarem quaisquer razões teóricas para o facto, o tamanho amostral de 1400 segundos (s) é indicado como aquele que onde a taxa de detecção de intrusões com duração superior a 500s é melhor.

O trabalho descrito em [14] faz referência ao estudo de [9], parecendo apoiar as suas conclusões mas, contrariamente ao esperado, no seu conteúdo é demonstrado que os valores do parâmetro de Hurst aumentam durante as anomalias investigadas. No artigo são usadas janelas de observação de 30 minutos, e os registos de tráfego são agregados para unidades de tempo que variam entre os 10ms e os 1000ms. A perca de auto-semelhança é sinalizada por desvios médios superiores a 10^{-3} entre a função de auto-correlação empírica e teórica, mas nada é dito acerca da intensidade ou duração das anomalias que podem provocar esses desvios.

O tipo de ataques que Allen et al. se propõem detectar em [2] corresponde ao tipo de ataques abrangidos pelo presente estudo. O tamanho das janelas de observação varia entre os 10 e os 30 minutos, dependendo do tamanho dos registos disponíveis e da carga de tráfego, e o valor do parâmetro de Hurst é calculado de 5 em 5 minutos. Um *ataque de exploração de tráfego* (designação usada na referência) é sinalizado quando o valor do parâmetro de Hurst

é superior a 1.0, ou inferior a 0.5. O artigo não contém um estudo à evolução do parâmetro de Hurst, nem refere a possibilidade de existirem *ataques de exploração de tráfego* que não resultem na perca da auto-semelhança.

Em nenhum dos artigos mencionados é mostrada uma evolução contínua dos valores do parâmetro de Hurst, sendo esse um dos principais factores de diferenciação do estudo aqui descrito. As simulações levadas a cabo durante este trabalho de investigação permitiram verificar uma panóplia mais abrangente de cenários de anomalia, e tirar conclusões daí. De igual modo, a implementação dos estimadores aqui proposta permitiu estudar o comportamento do grau de auto-semelhança para janelas temporais muito mais pequenas (na ordem dos 8s) que em qualquer outra contribuição científica. A interpretação teórica dos resultados não só explica fielmente os valores observados, como permite generalizar as conclusões para qualquer cenário de rede que se coadune com a simples condição do tráfego ser auto-semelhante.

4 Estimação do Parâmetro de Hurst e Simulação de Tráfego Auto-Semelhante

Esta secção apresenta os meios usados na estimação do parâmetro de Hurst, e relata brevemente o modo como o *tráfego legítimo* foi simulado computacionalmente. Note-se que no âmbito deste trabalho, a noção de *tráfego legítimo* é a mesma de *tráfego auto-semelhante*, de acordo com o que antes foi dito.

4.1 Estimação Móvel do Parâmetro de Hurst

Existem vários métodos de estimação do parâmetro de Hurst [3; 7]. A maior parte desses métodos é normalmente utilizado de modo retrospectivo, para análises conduzidas para registos de tráfego previamente capturados. Por muitas vezes se fundamentarem em estatísticas do processo auto-semelhante e das suas respectivas agregações, os estimadores dependem do processamento recorrente da mesma série de dados, pelo que apresentam uma complexidade computacional nunca inferior a $O(n \times \log(n))$ e requerem elevadas quantidades de memória.

Neste trabalho foram utilizados o método *Variância Tempo (VT)* (descrito, por exemplo, em [3]) e o método do *Processo Ramificado Embutido (PRE)* [7], por serem os que melhor se deixam moldar aos objectivos do estudo. Os dois métodos foram modificados e implementados de maneira a devolverem estimativas para uma janela de valores fixa, denominada aqui por *janela de observação*. Por motivos de falta de espaço, a formalização matemática das alterações sofridas pelos dois métodos não é aqui contida. Contudo, o conjunto de equações que formalizam as modificações para o VT pode ser encontrado em [6]. Os métodos modificados são aqui designados por VT (ou PRE) *móvel* ou *incremental*, assim se trate da versão que implementa o conceito da janela de observação, ou aquela que devolve o valor histórico (ponto-a-ponto) do parâmetro de Hurst.

Do ponto de vista conceptual, a filosofia dos estimadores móveis é simples. À instância que executa um desses métodos é pedido que devolva uma estimativa do parâmetro de Hurst cada vez que um ponto do processo em análise se torna disponível. No caso do VT, as variâncias das várias agregações do processo são actualizadas à medida que os valores do processo da *quantidade de bits por unidade de tempo* se tornam disponíveis, através da adição do efeito do valor de chegada, e da elimição do efeito do valor mais antigo na janela de observação. O valor cujo efeito foi eliminado dos cálculos é então substituido na memória pela mais recente ocorrência do processo. Contudo, deixa-se a ressalva de que o conceito da janela de observação não é directamente aplicável a todos os estimadores do parâmetro de Hurst, e que mesmo a implementação do VT ou do PRE na supramencionada filosofia, implica um efémero desvio ao seu racional inicial. Este desvio pode traduzir-se em ligeiras

instabilidades nas estimativas, que foram resolvidas pelos autores, mas cuja discussão está fora do âmbito deste artigo.

As modificações impostas ao VT e ao PRE permitiram não só construir autênticos histogramas dos valores do parâmetro de Hurst (ver secção 5), como também a abstracção ao problema levantado pela *lei dos grandes números*, que limitava fortemente a sensibilidade dos estimadores a alterações provocadas por mudanças nas propriedades do tráfego. Os estimadores retrospectivos, ainda que aplicados de maneira a devolver valores ponto-a-ponto, rapidamente perdem a capacidade de notar pequenas alterações, penalizados pelo peso estatístico da história da análise.

4.2 Simulação de Tráfego Auto-Semelhante

Os resultados contidos na secção 5 foram obtidos através de simulação computacional. Dado a especificidade do problema não requerer mais do que emulação do tráfego ao nível inferior da camada de ligação de dados, todos os registos de tráfego foram modelados como sequências de *tamanhos de pacotes* e *intervalos entre chegadas*. Convencionou-se que os tamanhos de pacotes eram incidências de uma variável aleatória com distribuição empírica conhecida (por exemplo de [10]) e que, por conseguinte, o seu valor esperado $E(P_t)$ era sabido à priori. A simulação de uma *Carga* de rede efectiva C (dada em relação a uma Largura de Banda total de LB) é conseguida através da geração de n_p *tamanhos de pacotes* e n_p *intervalos entre chegadas* por unidade de tempo, em que n_p é dado por:

$$n_p = \frac{LB \times C}{E(P_t)}. \tag{3}$$

Nestas circunstâncias, a média dos tempos entre chegadas $E(IC_t)$ é necessariamente descrita por (4) e, dado $\{IC_t\}_{t\epsilon\mathbb{N}}$ ser inferiormente limitada por um valor mínimo positivo IC_{min}, decidiu-se que o seu intervalo de variação se devia confinar a $[IC_{min}, 2 \times (E(IC_t) - IC_{min})]$.

$$E(IC_t) = \frac{LB \times (1 - C)}{n_p}. \tag{4}$$

A impressão da estrutura fractal (auto-semelhança) no *processo da quantidade de informação por unidade de tempo* foi conseguida através da modelização dos tempos entre chegadas como sendo incidências de rGf, de acordo com a expressão (5), onde rGf_t^H denota a ocorrência t de um rGf com parâmetro de Hurst H. Note-se que o desvio padrão do processo ($\sigma = (E(IC_t) - IC_{min})/3$) foi escolhido de modo a que, 99.7% das vezes, o valor produzido pela implementação de (5) esteja contido no intervalo de variação definido. O gerador de tráfego usado neste trabalho de investigação trunca automaticamente todos os valores que estejam fora do referido intervalo, para evitar inconsistências. A simulação de rGf é feita através de um método baseado em *Onduletas*, descrito em [3].

$$IC_t = rGf_t^H \times \frac{E(IC_t) - IC_{min}}{3} + E(IC). \tag{5}$$

4.3 Simulação de Ataques de Rede Intensos

Antes de prosseguir com a descrição do modo de como os ataques foram simulados, é pertinente o comentário ao tipo de anomalias que um método baseado em auto-semelhança tem possibilidades de detectar. Dado a princípal estatística em análise estar dependente de uma quantidade amostral necessariamente grande (o parâmetro de Hurst reflecte *dependências de longo-alcance*), qualquer ataque constituido por um número de pacotes expressivamente pequeno tem poucas hipóteses de ser detectado por este tipo de análise. O interesse incide, portanto, naqueles ataques que, a determinada altura da sua investida, ocupam uma

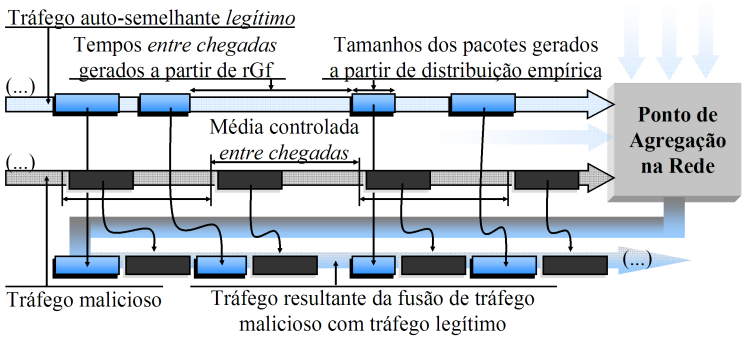

Figura 1: Representação gráfica do procedimento usado para *injectar* as unidades de dados de um ataque simulado no registo de tráfego auto-semelhante.

quantidade de largura de banda não negligenciável. São estes os ataques que aqui são denominados de *ataques de rede intensos*. Várias instâncias de ataques de negação de serviço (ataques a protocolos ou de inundação, distribuídos ou não) [13; 15] recaem precisamente na categoria indicada. Note-se que a definição destes ataques vai de encontro ao que foi dito sobretudo em [2; 9]. Em [9] é aliás enfatizada e utilizada a designação de *ataques de largura de banda*, sugerida pela *Computer Emergency Response Team* (CERT) [4].

A simulação dos ataques de rede intensos foi feita recorrendo à especificação do parâmetro de Intensidade (I), que determina a quantidade de pacotes que chega ao nó fictício, por unidade de tempo e em função da largura de banda disponível. Depois de se escolher o tamanho do pacote malicioso (por exemplo, o tamanho de um pacote SYN do *Transmission Control Protocol* (TCP)), calcula-se a média do ritmo de geração dos pacotes maliciosos. Devido ao facto do gerador de tráfego legítimo apresentado permitir a sua representação conceptual em termos de sequências de unidades de dados, a injecção do tráfego relativo ao ataque pode ser conseguida pela implementação directa do procedimento ilustrado pela figura 1. As unidades de dados do tráfego malicioso são simplesmente inseridas no tráfego legítimo por ordem de chegada, podendo isso incorrer no atraso de ambos os tipos de tráfego. A análise da auto-semelhança é feita para o fluxo resultante da fusão do tráfego malicioso com o legítimo. Na figura 1, esse fluxo está representado em baixo, ilustrado como o único que *sai* do equipamento de agregação.

5 Análise dos Resultados

Esta secção está dividida em quatro partes. As duas primeiras partes são dedicadas à análise da evolução do parâmetro de Hurst durante ataques de rede intensos. Os dois cenários estudados exploram a possibilidade da duração do ataque ser ou não superior à janela de observação dos estimadores móveis utilizados. A terceira parte é dedicada aos testes estatísticos de resiliência da auto-semelhança. A última subsecção elabora numa possível interpretação dos resultados.

5.1 Duração do Ataque Menor que o Tamanho da Janela de Observação

Um dos primeiros cenários observados com as ferramentas antes mencionadas foi aquele em que a duração do ataque é menor do que o tamanho da janela de observação. A representação gráfica do lado esquerdo da figura 2 mostra um dos cerca de 150 histogramas construídos e analisados empiricamente durante esta parte do trabalho de investigação. O cenário simulado é o de um ponto de agregação capaz de operar a 1Gbps, mas cuja carga

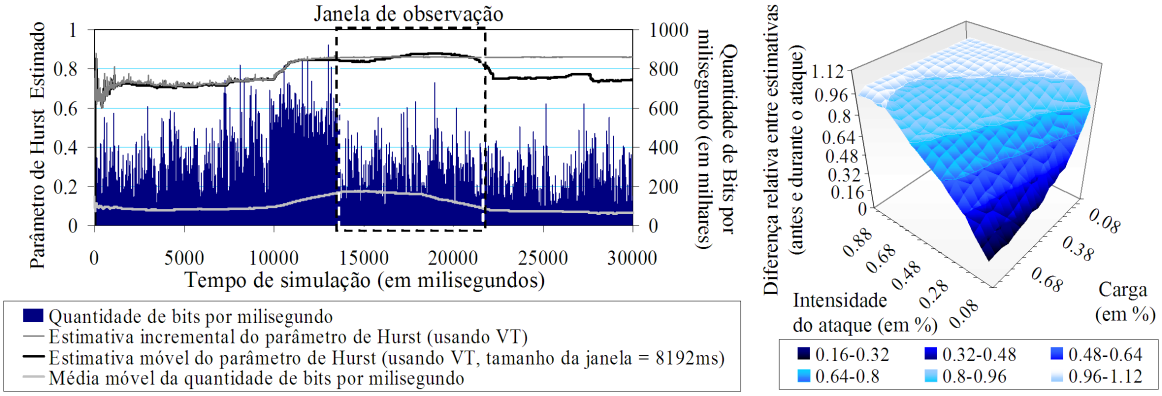

Figura 2: Representação gráfica de alguns dos resultados relativos às simulações com ataques de duração inferior ao tamanho da janela de observação (o tamanho da janela de observação era de 8,192s, a duração do ataque era de 4s, a carga era de 10% e a intensidade do ataque de 10%). Do lado esquerdo pode ver-se o histograma da evolução do parâmetro de Hurst (calculado através do estimador baseado no VT); enquanto que no lado direito é incluído o gráfico da diferença máxima entre estimativas do parâmetro de Hurst obtidas antes e durante o ataque, para diferentes combinações de carga e intensidade do ataque.

útil é de 10%. O parâmetro de Hurst do gerador de tráfego legítimo foi inicializado a 0.75, e um ataque com intensidade de 10% e duração de 4s foi injectado aos 10s de simulação. Para além da *quantidade de bits por milisegundo* e da respectiva média móvel (calculada para uma janela de observação de 8192ms), são também apresentadas no gráfico as curvas de evolução do parâmetro de Hurst, calculado usando o VT móvel e incremental. O tamanho da janela de observação está também representado (à escala) na figura.

Como se pode ver, depois de um período inicial de instabilidade, os valores do parâmetro de Hurst tendem para o valor esperado de 0.75. Assim que o ataque começa, os mesmos valores aumentam para 0.86 (aproximadamente) e variam em torno desse valor durante $4000 + 8192 \approx 12000$ms. Logo que o registo de tráfego contendo o ataque *abandona* a janela de observação, os valores do estimador móvel decrescem novamente para próximo de 0.75. O facto das estimativas do parâmetro de Hurst se manterem elevadas durante um período de tempo que supera o da duração do ataque está relacionado com o tamanho do mesmo. Como será explicado com mais detalhe em baixo, a entrada do ataque no estimador móvel corresponde a uma translação do processo analisado, que é inicialmente entendida como uma mudança no grau de auto-semelhança. Este *novo* estado em que o VT móvel se encontra é o resultado da presença de dois tipos de tráfego dentro da janela (legítimo, e legítimo+malicioso), que só é anulado depois do tráfego relativo ao ataque abandonar *por completo* a janela de observação. Note-se ainda que as estimativas devolvidas pelo VT incremental permanecem elevadas, mesmo depois do ataque terminar, já que o seu efeito demora a desaparecer da memória do estimador retrospectivo.

De maneira a obter uma ideia mais clara do comportamento do parâmetro de Hurst face a diferentes cenários de rede, foi desenhado um procedimento para testar (repetidas vezes) cerca de 324 combinações do par (C, I). De entre várias estatísticas, o procedimento devolvia a diferença máxima entre valores do parâmetro de Hurst local, antes e durante o ataque, o momento apontado como sendo o início do ataque e a duração do mesmo (o início do ataque era sinalizado por estimativas locais do parâmetro de Hurst superiores ao valor esperado em cerca de 0.01, por períodos de tempo superiores a 100ms; o fim do ataque correspondia ao *regresso* do parâmetro de Hurst ao valor esperado). Para facilitar a sua análise crítica, as diferenças máximas entre valores do parâmetro de Hurst foram normalizadas (divididas pelo supremo de todos os valores calculados) e representadas, como

uma função da carga de rede e da intensidade do ataque, no gráfico do lado esquerdo da figura 2. As referidas diferenças atingem máxima expressão para aproximadamente metade das combinações simuladas, tornando-se mais notáveis à medida que a intensidade do ataque aumenta.

5.2 Duração do Ataque Maior que o Tamanho da Janela de Observação

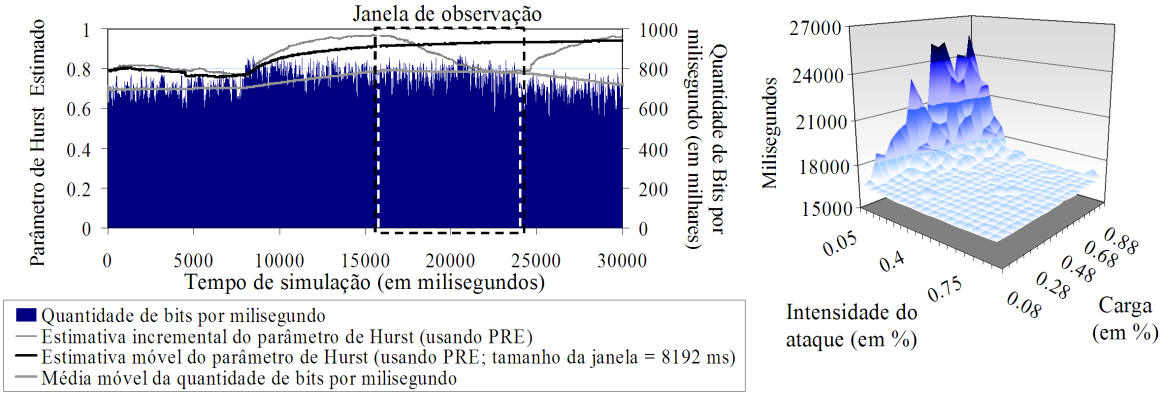

Figura 3: Representação gráfica de alguns dos resultados relativos às simulações com ataques de duração superior ao tamanho da janela de observação (o tamanho da janela de observação era de 8,192s, a duração do ataque era de 16s, a carga era de 70% e a intensidade do ataque de 10%). Do lado esquerdo pode ver-se o histograma da evolução do parâmetro de Hurst (calculado através do estimador baseado no PRE); enquanto que no lado direito figura a média dos momentos apontados como o início das anomalias.

O segundo tipo de cenário encenado diz respeito à situação onde a duração do ataque supera o tamanho da janela de observação. Uma possível ilustração deste cenário é incluída no lado esquerdo da figura 3. Neste caso, o gerador de tráfego foi instruido a simular uma carga de rede de 70% e um ataque com 10% de intensidade aos 8s. O parâmetro de Hurst do tráfego legítimo foi ajustado para 0.80 e os respectivos métodos de estimação eram baseados no PRE. O tamanho da janela de observação valia metade da duração da anomalia.

Como se pode verificar, e contrariamente ao que acontecia anteriormente, a estimativa móvel do parâmetro de Hurst regressa ao valor esperado ainda durante a análise do ataque. Isto acontece porque, assim que o registo de tráfego contendo o ataque passa a dominar o contexto do PRE móvel (note-se que isto também se aplica ao VT móvel), o método é incapaz de distinguir o processo em análise de uma translação do processo inicial (e legítimo). Logo que o ataque termina e começa a sair da janela de observação, o PRE detecta novamente a translação e as suas estimativas aumentam novamente até que o efeito daquele desaparece da janela de observação.

No lado direito da figura 3 foi incluida a representação da média dos momentos apontados como o início dos anomalias, em função da sua intensidade e da carga de rede. Qualquer ataque com expressão superior a 3% (em termos de largura de banda total) produz efeito suficiente para o detector antes descrito apontar com exactidão o momento em que processo muda. Para a maior parte dos casos, o início do ataque é apontado estar entre os 16 e os 17s.

5.3 A Destruição da Propriedade da Auto-Semelhança

De modo a investigar se a auto-semelhança é ou não perdida durante um ataque de rede intenso, foram implementados dois testes estatísticos diferentes. O teste de Kolmogorov Smirnov (*teste K-S*) foi usado para apurar se a distribuição de um registo de tráfego contendo um ataque é ou não *semelhante* à distribuição de várias agregações do processo em análise. O segundo teste avalia a qualidade da estimativa devolvida pelo VT (para mais detalhes, considere a leitura das referências [3; 6]), através do estudo da estatística conhecida como o *coeficiente de determinação*, normalmente simbolizada por R^2 [1].

A introdução de tráfego de um ataque de rede intenso corresponde a uma translação do processo auto-semelhante, e a uma consequente mudança das suas propriedades. A média móvel do processo aumenta, tal como a sua variância. Antes do início do ataque, e até durante o mesmo, a auto-semelhança é mantida a nível local, mas o mesmo pode não acontecer durante o período em que a janela de observação transita de tráfego legítimo para o registo contendo unidades de dados do ataque. Foi precisamente neste período de tempo que a análise foi efectuada.

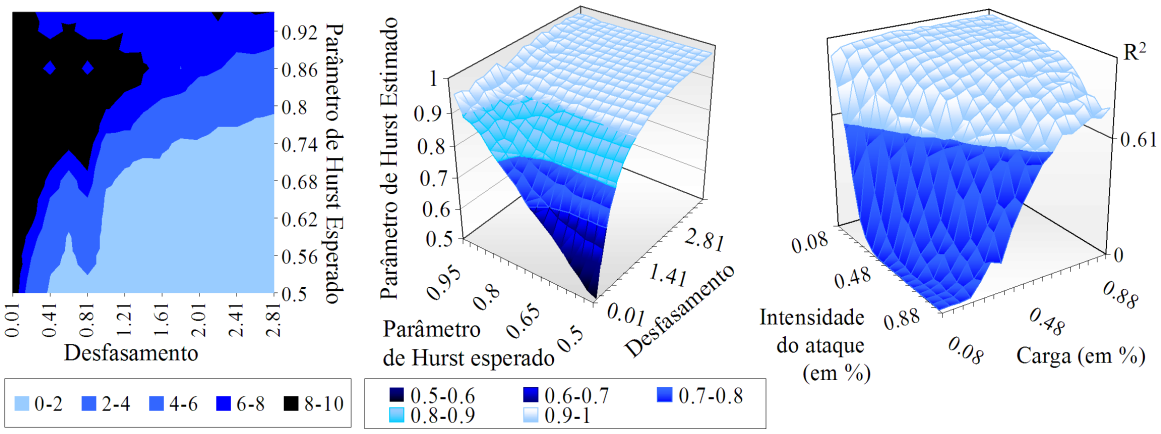

Figura 4: Compilação dos resultados dos testes à resiliência da auto-semelhança. Do lado esquerdo, representa-se o número médio de testes Kolmogorov Smirnov bem sucedidos (de um total de 10), em função do grau de auto-semelhança e do desfazamento aplicado ao sinal; ao centro mostra-se a superfície que define a diferença entre o parâmetro de Hurst do sinal auto-semelhante e o do transladado; e do lado direito representa-se a *qualidade* da regressão linear do VT, de acordo com a estatística R^2.

Foram simulados vários registos do período temporal em que o ínicio do ataque está algures no meio da janela de observação. Depois, o *processo da quantidade de bits por unidade de tempo* foi normalizado e agregado k vezes, vindo posteriormente a produzir-se a distribuição de probabilidade para todos esses processos. De modo a aplicar o *teste K-S*, foram tiradas as k maiores distâncias D_k, entre todas as distribuições dos processos agregados e a distribuição do processo inicial. Os vários D_k foram então comparados com valores críticos (para o grau de significância de 0.01) tabelados [12], sendo considerados como *bem sucedidos* no caso em que D_k era menor que o valor crítico. Simultaneamente, era pedido à classe que implementava o VT móvel que devolve-se o valor R^2 da pior regressão obtida ao longo da *sua* análise.

Os gráficos contidos na figura 4 resumem parte da investigação conduzida para um cenário em que a carga de rede era de 50% e a janela de observação era de 8192ms (os testes foram aplicados para $k = 10$, para escalas de agregação de $2^i, i = 1, ..., 10$). Os resultados representados à esquerda da figura mostram que a resiliência ao desfazamento provocado à sequência de valores em análise depende do grau de auto-semelhança da mesma. Apesar da dependência não aparentar ter uma fórmula explícita que a explique, facilmente

se depreende que à medida que o parâmetro de Hurst aumenta, maior é o desfazamento suportado pelo processo, antes da destruição da auto-semelhança. Repare-se que, neste caso, os autores consideraram que a perca da referida propriedade implicava o falhanço em pelo menos 2 dos 10 testes aplicados. Note também que para valores do parâmetro de Hurst entre 0.75 e 0.85, o processo analisado parece ser especialmente resistente às transformações a que foi sujeito, sendo capaz de suportar intensidades de aproximadamente 30% (igual ao desvio padrão do processo), antes de perder a auto-semelhança.

A última fase da maior parte dos estimadores do parâmetro de Hurst compreende a aproximação de determinado número de coordenadas via regressão linear. A adequação do modelo resultante dessa regressão, dada pelo valor de R^2, pode ser entendida como uma medida do *quão bem* a auto-semelhança se reflecte no processo em análise. R^2 varia entre 0 e 1, argumentando em favor da qualidade do método para valores próximos do limite superior. O gráfico colocado à direita da figura mostra que a introdução de ataques no tráfego auto-semelhante afecta a lei exponêncial em que o método VT se baseia. Contudo, se a perca da propriedade estudada fosse definida em função de R^2 (ou do chamado *teste F* [1] que se pode aplicar à transformação dada por $F = (k-2) \times R^2/(1-R^2)$), só após uma intensidade considerável é que se podia concluir acerca do falhanço da aproximação linear aos vários logaritmos das variâncias. A verdade é que o valor de R^2 (e consequentemente de F) se mantém elevado mesmo na presença de ataques com intensidade média, pelo que o teste mencionado não é capaz de descartar a possibilidade de existir uma relação exponêncial (fractal) entre o processo e suas agregações. Note que a linha de decisão da perca da auto-semelhança é a que divide a superfície nas duas secções com cores diferentes.

O gráfico do meio da figura 4 foi incluído com o objectivo de mostrar o comportamento das estimativas do parâmetro de Hurst, perante os cenários anteriormente descritos e testados. Como se pode observar, o sucesso ou falhanço dos *testes K-S*, ou a qualidade da regressão do VT, não parecem influenciar directamente os valores devolvidos pelos estimadores, que se aproximam imperetrivelmente de 1 (sem nunca o ultrapassar) à medida que o desfazamento aumenta.

5.4 Interpretação dos Resultados

Dos resultados incluídos anteriormente conclui-se que (i), a auto-semelhança não é necessariamente destruída pela presença de um ataque de rede intenso e que (ii), o parâmetro de Hurst aumenta *sempre* que um fluxo constante de tráfego é injectado na rede. Nesta secção propõe-se uma possível interpretação para estes factos, com base na teoria subjacente à auto-semelhança.

O processo das diferenças de primeira ordem de um processo auto-semelhante (definido em (2)) é parcialmente dominado por componentes constantes, cuja duração, amplitude e sinal, determinam as suas propriedades fractais. O parâmetro de Hurst aumenta de 0.5 para 1 à medida que a extensão e magnitude da parte constante aumenta. Durante os períodos de normal funcionamento da rede, as referidas componentes são o produto de vários fluxos de informação, gerados por nós remotos e direccionados até ao ponto de agregação, onde alimentam continuamente o *processo da quantidade de informação por unidade de tempo*, conferindo-lhe propriedades mais ou menos *persistentes*. Durante um ataque de rede intenso, os dois factores acima mencionados (duração e amplitude) são ambos afectados positivamente, e a *persistência* (a parte constante) do sinal é reforçada. Neste caso, e apesar de não serem conceitos equivalentes, a *constância* pode fortalecer a *auto-semelhança* ou até destruí-la, mas nunca diminuí-la.

É óbvio que a inserção de tráfego malicioso resulta sempre numa perca de estacionariedade, mas essa perca pode não resultar na destruição da auto-semelhança (a figura 3 ilustra um cenário que não resulta na perca da referida propriedade). É sabido, por exemplo de [3], que a estacionariedade dos *processos com dependências de longo alcance* é difícil de avaliar, já que a própria natureza dos processos fractais dita o deslocamento das pro-

priedades estatísticas a nível local. Estes deslocamentos podem, numa primeira análise, ser confundidos com falta de estacionariedade mas, na verdade, são apenas viés definidos pelas (auto) correlações. A introdução de modestos (em relação à carga de rede) fluxos de tráfego malicioso pode apenas resultar num deslocamento local e pequeno da largura de banda ocupada, que aumenta a auto-semelhança. Alheios à qualidade exacta do sinal de entrada, tudo o que os estimadores utilizados são capazes de observar é, basicamente, a transformação de um processo variável em um mais estável, para o qual a estimativa do parâmetro de Hurst *só* pode ser superior.

6 Conclusão

Este artigo resume a análise detalhada à evolução do grau de auto-semelhança durante intrusões com expressão significativa ao nível da largura de banda. Todos os resultados aqui contidos foram obtidos por simulação, mas corroborados por dois estimadores do parâmetro de Hurst diferentes. A possível perca da auto-semelhança, durante os referidos ataques, é testada recorrendo a duas abordagens estatísticas completamente diferentes, e todos os resultados são analisados do ponto de vista teórico, embora de modo breve.

A especificidade da análise delimita perfeitamente os dois cenários tomados em consideração nas simulações. Para o caso em que a duração do ataque é inferior ao tamanho da janela de observação dos estimadores, as estimativas do parâmetro de Hurst mantêm-se acima da média (ou daquilo que era esperado) enquanto o tráfego relativo ao ataque (ou parte desse tráfego) se encontra *dentro* da janela de observação. No caso oposto, as estimativas começam por subir assim que o tráfego malicioso começa a *chegar* no estimador, descendo até ao valor esperado assim que a janela de observação é completamente obsorta pela mistura de tráfego malicioso e legítimo. Assim que o ataque termina, regista-se de novo um aumento das estimativas do parâmetro de Hurst, que decresce logo que o tráfego relativo ao ataque *deixa* por completo a janela de observação.

Ficou demonstrado que a presença de um ataque de rede intenso não resulta *necessariamente* na destruição da propriedade da auto-semelhança. Na verdade, a destruição desta propriedade depende da expressividade da perca de estacionariedade, que por sua vez depende da intensidade do ataque, e da carga da rede. Por exemplo, a presença de um ataque com expressão relativamente modesta resulta apenas no aumento da auto-semelhança. Independentemente da perca ou preservação da estrutura fractal, os valores devolvidos pelos dois estimadores utilizados aumentam durante a presença do ataque, assinalando apenas um *aparente* aumento do grau de auto-semelhança do tráfego.

Aliados à baixa complexidade computacional dos estimadores utilizados, os resultados aqui contidos sugerem que a análise da auto-semelhança pode ser eficientemente utilizada para detectar anomalias, cuja natureza *pode* estar relacionada com ataques de rede. O método que elabora nesta análise pode ser posicionado imediatamente após os mais simples colectores de dados de tráfego, levantando alertas que podem despoletar novas investigações. Contudo, e também devido à especificidade das métricas em que se baseia, o seu juízo solitário não pode decidir a legitimidade ou ilegitimidade do tráfego.

Agradecimentos

Os autores gostariam de agradecer o apoio financeiro da *Fundação para a Ciência e Tecnologia, Portugal* (formalizado pelo contrato no. SFRH/BDE/15592/2006), da *Nokia Siemens Networks Portugal S.A.* e do projecto PTD-C/EIA/73072/2006 TRAMANET: *Traffic and TrustManagement in Peer-to-Peer Networks*. Estão igualmente gratos a João Gomes, por criticar construtivamente este trabalho.

Referências

[1] Michael Patrick Allen, *Understanding regression analysis*, Humanities, Social Sciences and Law, ch. The coefficient of determination in multiple regression, pp. 91–95, Springer US, Novembro 2007, Free Preview.

[2] W.H. Allen and G.A. Marin, *The LoSS Technique for Detecting New Denial of Service Attacks*, SoutheastCon, 2004, Florida Institute of Technology;, IEEE, Março 2004, pp. 302–309.

[3] Ton Dieker, *Simulation of fractional Brownian motion*, Master's thesis, University of Twente, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands, 2004.

[4] Fengmin Gong, *Deciphering Detection Techniques: Part III Denial of Service Detection*, White paper, McAfee Network Security Technologies Group, Janeiro 2003.

[5] Mohd Yazid Idris, Abdul Hanan Abdullah, and Mohd Aizaini Maarof, *Iterative Window Size Estimation on Self Similarity Measurement for Network Traffic Anomaly Detection*, Int. Journal of Computing and Information Sciences (IJCIS) **4** (2005), no. 4, 88–91.

[6] Pedro R. M. Inácio, Mário M. Freire, Manuela Pereira, and Paulo P. Monteiro, *Analysis of the Impact of Intensive Attacks on the Self-Similarity Degree of the Network Traffic*, The Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2008) (Cap Esterel, France), 2008, pp. 107–113.

[7] OD Jones and Y. Shen, *Estimating the Hurst index of a self-similar process via the crossing tree*, Signal Processing Letters, IEEE **11** (2004), no. 4, 416–419.

[8] W.E. Leland, M.S. Taqqu, W. Willinger, and D.V. Wilson, *On the self-similar nature of ethernet traffic (extended version)*, Networking, IEEE/ACM Transactions on **2** (1994), no. 1, 1–15.

[9] Ming Li, *Change trend of averaged Hurst parameter of traffic under DDOS flood attacks*, Computers & Security (2006), no. 3, 213–220.

[10] NLANR, *NLANR - National Laboratory for Applied Network Research - Internet measurement, Internet analysis*, 2005, Acedido a 29 de Março de 2008.

[11] I. Norros, *Studies on a Model for Connectionless Traffic, Based on Fractional Brownian Motion*, COST24TD(92)041, 1992.

[12] Paul Wessel, *Critical Values for the Two-sample Kolmogorov-Smirnov test (2-sided)*, acedido a 27 de Agosto de 2008.

[13] Vern Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, ACM Computer Communications Review (CCR) **31** (2001), no. 3.

[14] Mohd Fo`ad Rohani, Mohd Aizaini Maarof, Ali Selamat, and Houssain Kettani, *Uncovering Anomaly Traffic Based on Loss of Self-Similarity Behavior Using Second Order Statistical Model*, IJCSNS International Journal of Computer Science and Network Security **7** (2007), no. 9.

[15] Bennett Todd, *Distributed Denial of Service Attacks*, February 2000, Acedido a 30 de Março de 2008.

[16] Walter Willinger, Murad S. Taqqu, Robert Sherman, and Daniel V. Wilson, *Self-similarity through high-variability: statistical analysis of Ethernet LAN traffic at the source level*, IEEE/ACM Transactions on Networking **5** (1997), no. 1, 71–86.