MÉTRICAS PARA A DETECÇÃO DE ATAQUES DDOS

Nícolas Rocha e Silva e Ronaldo Moreira Salles*
Instituto Militar de Engenharia, Seção de Sistemas e Computação – Praça General Tibúrcio, 80, 22290-270, Praia Vermelha, Rio de Janeiro, RJ, Brasil.
**nicolasime@gmail.com*

RESUMO

Enfrentar ataques DDoS constitui um problema de difícil solução, uma vez que o atacante emprega um grande número de máquinas em suas ações. A disponibilidade de ferramentas destinadas para esse fim aumentou, tornando mais frequente a sua ocorrência. Detectar a presença de um ataque constitui a primeira etapa para combatê-lo. Este trabalho apresenta alguns métodos de detecção de ataques DDoS, baseados na identificação de anomalias. O emprego de métricas mais sensíveis pode permitir a detecção antecipada de ataques DDoS, onde há um baixo percentual de pacotes maliciosos. Também é apresentada uma sugestão para a implementação de um sistema colaborativo de detecção, que pode garantir maior eficiência nos resultados.

Palavras-chave: DDoS, detecção, entropia, estimadores, divergência.

ABSTRACT

Facing DDoS attacks is a challenging task since a potential attacker may use a large number of hosts in his actions. Today it is not difficult to find several different tools available for this purpose, making the occurrence of such attacks becoming very frequent. Detecting the presence of an attack is the first step to combat it. This paper presents some methods to detect DDoS attacks based on identification of anomalies. Employing sensitive metrics may allow the early detection of DDoS attacks in network points where the rate of malicious packets is still growing. We also propose the construction of a collaborative detection system that may guarantee higher accuracy in the results.

Keywords: DDoS, detection, entropy, predictor, divergence.

INTRODUÇÃO

A Internet, desde a sua criação, tem se expandido a cada ano, tanto em número de usuários como em tecnologias envolvidas. De acordo com a *Internet Systems Consortium, Inc.* (ISC), em julho de 2011, foram computados 849.869.781 *host's* permanentemente conectado a essa rede (Figura 1). Trata-se de um poderoso meio de comunicação que permite o compartilhamento de informações através da transferência de dados. Através desse meio, vários serviços, oferecidos por entidades governamentais ou privadas, podem ser acessados por usuários de qualquer parte do planeta através de um dispositivo conectado à rede.

Por outro lado, o tráfego de dados maliciosos, capazes de causar os mais diversos tipos de danos, também está presente nesse meio, e que podem advir de ataques planejados. Por isso, cuidados com o sigilo, a autenticidade, a integridade e a disponibilidade tornaram-se ainda mais imprescindíveis, e constituem preocupações constantes tanto para empresas como para governos.

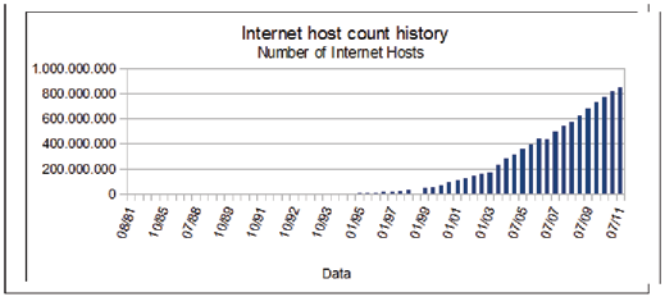

Figura 1. *Número de host's interconectados através da Internet. Fonte: (ISC, 2011)*

A Internet atual é vulnerável a ataques de negação de serviço distribuídos (DDoS). Ataques desse tipo têm como objetivo fazer com que uma rede ou serviço oferecido por ela fique inacessível a usuários legítimos, o que geralmente é alcançado quando um atacante envia pacotes a uma taxa maior do que a vítima pode processar (Castelúcio, 2009). Este é um dos diversos tipos de ataque que se aproveita das falhas de programação da pilha TCP/IP, que possibilita ao invasor explorar a enorme assimetria de recursos que existe entre a Internet e a vítima.

Cada vez mais os DDoS se tornam mais sofisticados e difíceis de detectar. Por isso mesmo trata-se de uma tarefa bastante desafiadora. Embora existam estudos desde o ano de 2000, ainda não há uma resposta definitiva para a solução desse problema, de forma que ainda há espaço para contribuições.

Uma das maneiras de combater esse tipo de ataque se dá através da observação das fases que antecedem um ataque. Controlar um número expressivo de máquinas requer medidas de comando e controle para se garantir a eficiência do DDoS. Esse tráfego também transita pela Internet, e pode contribuir para a descoberta antecipada da botnet que realiza o ataque.

Existem várias iniciativas de estudos, com diferentes abordagens, voltados para a detecção de botnet's maliciosas (Wang, 2009). Encontrar os componentes desta rede antes mesmo do ataque ocorrer constitui uma medida preventiva muito

vantajosa, já que pode evitar muitos danos a partir de ações tomadas contra os agentes previamente identificados. Entretanto, quando essas identificações não ocorrem, as redes ficam vulneráveis aos ataques, caso não haja outro mecanismo de defesa. Além disso, podem ocorrer ataques de inundação sem a formação de uma botnet, quando, por exemplo, usuários são convocados a participar voluntariamente de um ataque organizado (Jornalnh, 2012). Sendo Assim, torna-se necessário o estudo de mecanismos eficientes de detecção de DDoS.

TRABALHOS RELACIONADOS

Existem várias pesquisas cujo objetivo consiste na minimização de danos causados por um ataque DDoS ou na compreensão dos mecanismos envolvidos nesse processo (Figura 2). Boa parte dos estudos concentra seus esforços na detecção e classificação de anomalias, empregando as mais diversas técnicas, como em (Lakhina, 2005) e (Luo, 2013). Alguns desenvolvem métodos para a identificação dos focos de ataque, cujo objetivo é traçar a rota seguida pelos pacotes maliciosos, como em (Law, 2002), (Demir, 2010), (Shui, 2013) e (Baskar, 2013). Outros estudam o comportamento das *botnets* nas fases que antecedem ao ataque, a fim de identificar os vetores de ataque antes mesmo de ele ocorrer, como em (Cabrera, 2001), (Dittrich, 2008), (Ferrer, 2010), (Jin, 2012), (Sharifnya, 2013) e (Khattak, 2014).

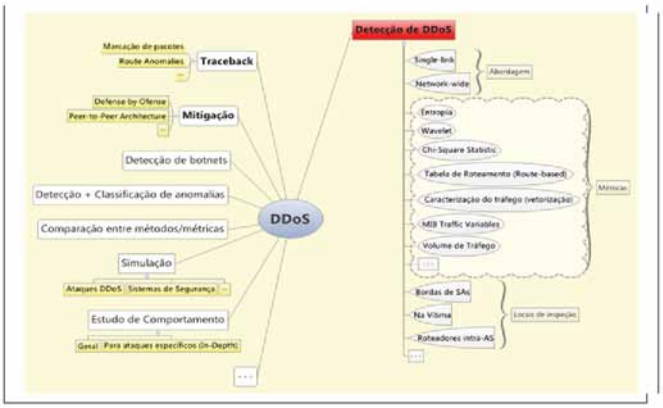

Figura 2. *Trabalhos relacionados a ataques DDoS*

De maneira geral, o combate contra 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 (Castelucio, 2009).

No que diz respeito à detecção, são propostos diferentes mecanismos baseados em wavelet (Kaur, 2010) (Kaur, 2013), entropia (Lakhina, 2005) (Lucena, 2008) (Xinlei, 2014), Bayes (Chwalinski, 2013) (Katkar, 2013), redes neurais (Chen, 2013), distribuição polinomial (Paul, 2013,) tabela de roteamento (Park, 2000), defense by ofense (Walfish, 2010), caracterização do tráfego (Feng, 2009), marcação de pacotes (Law, 2002) (Anitha, 2013), que podem adotar uma abordagem *single-*

-*link* (Lucena, 2008) (Demir, 2010) (Yuan, 2013) ou *network-wide* (Chen, 2006) (Fei, 2012) (Buvaneswari, 2013) (Nafir, 2014). Algumas arquiteturas independem de base histórica (Lin, 2005), enquanto que outras têm seus parâmetros adaptados de acordo com uma *baseline* para melhor se ajustar a fatores sazonais (Kline, 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 em COSSACK (Papadopoulos, 2003) e DefCOM (Mirkovic, 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, 2007).

A detecção antecipada pode ser alcançada através da distribuição de detectores em pontos afastados (Sardana, 2010), que não são objetivos do ataque, mas que constituem vias por onde passam os fluxos destinados à vítima. Obviamente, há um custo adicional para se manter tal arquitetura, mas que pode ser reduzido através de algumas medidas. Uma delas se faz por meio de uma abordagem colaborativa, onde o esforço conjunto de instituições pode proteger um número muito maior de redes e fortalecer o sistema como um todo, tornando-o mais viável e eficiente. Para reduzir o número de detectores necessários e ainda manter essa distribuição, basta realizar a inspeção de pacotes nos roteadores de borda de Sistemas Autônomos, já que constituem pontos de concentração de fluxo (Park, 2000) (Lin, 2005).

Nestes roteadores a concentração de volume de tráfego é bem elevada, tornando a inspeção dos pacotes bastante custosa. Por isso é comum utilizar métodos que minimizem a carga de processamento na coleta e tratamento de dados. Normalmente, isto é feito capturando-se apenas uma determinada percentagem dos pacotes que passam pela interface monitorada. Desta forma é possível realizar uma detecção baseada numa assinatura estatística do tráfego de rede associado a determinado tipo de anomalia (Estevez-Tapiador, 2004). Outra abordagem bem adequada para redes de *backbone*, dado o grande volume de pacotes que costuma atravessar seus roteadores, se dá através da inspeção dos fluxos de pacotes, sendo possível verificar se há ou não a presença de alguma anomalia correlata, sem a necessidade de inspecionar cada pacote IP trafegado na rede (Lucena, 2008) (Sanmorino, 2013).

No que diz respeito ao rastreamento da origem, são vários os sistemas propostos que adotam diferentes abordagens, tais como marcação de pacotes (Castelucio, 2009) (Law, 2002) (Anitha, 2013) e armazenamento de resumos baseados em filtros (Laufer, 2005) (Snoeren, 2002). A detecção dos ataques tem papel determinante para a eficiência desses sistemas, devido à dependência existente entre essas etapas. Por conta disso, alguns trabalhos propostos já sugerem uma solução conjunta, como em (Xiang, 2011) e (Chen, 2007).

No que diz respeito à mitigação e eliminação dos efeitos causados pelo ataque, em (Walfish, 2010), os autores propõem uma solução baseada numa ação dos

usuários legítimos provocada pela vítima, cujo intuito é diferenciá-los das máquinas pertencentes à *botnet* que esteja atacando. Em (Wang, 2009) a solução prevê o compartilhamento de informações que auxiliam na manutenção de filtros cujo objetivo consiste em bloquear tráfegos indesejados. Em ambos os casos, mecanismos de detecção também são necessários.

Apesar dos avanços na detecção do tráfego não desejado, especialmente sobre *backbones* de alta velocidade, muitas das abordagens apresentam um custo computacional elevado, requerem mudanças na infraestrutura ou mesmo apresentam resultados imprecisos. 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, 2008).

(Moura, 2009) propôs em sua dissertação de mestrado uma abordagem *single-link* para a detecção de anomalias em enlaces de uma rede WAN a partir da observação da entropia de fluxos de pacotes IP que passam por uma dada interface, combinado ao uso de um estimador de comportamento para estas séries temporais, no caso a estimativa de Holt-Winters (Brutlag, 2000). Tal abordagem parece ser adequada também para tráfegos entre WAN's, devido às características dessa métrica e do estimador empregado. Entretanto, foram empregados neste trabalho, para os estimadores estudados, parâmetros padrão, baseados nos valores adotados em (Brutlag, 2000), e que, supostamente, se adequariam a qualquer tráfego e tipo de anomalia. Adotar a mesma abordagem entre SA, talvez não seja a mais eficiente. Parâmetros mais ajustados ao tráfego podem ser mais adequados, mesmo com um maior índice de falsos positivos.

(Chen, 2007), por outro lado, propôs um novo esquema distribuído de detecção com agregação de informações através da comunicação entre vários domínios de rede e alcançou bons resultados, no que diz respeito ao número de falsos alertas e prevenção da inundação causada. Neste esquema a detecção é realizada em três camadas. Na camada mais baixa, todos os roteadores executam um algoritmo capaz de detectar flutuações suspeitas de tráfego, enviando um alerta a um servidor. Na segunda camada, fica a cargo deste servidor construir uma sub-árvore que mapeia dentro do SA o caminho do suposto ataque. Na camada mais alta, os servidores dos diferentes SA, que participam deste Sistema Colaborativo e formam uma rede sobreposta, comunicam-se entre si, mapeando todo o percurso do ataque.

No ataque conhecido como *3.4 DDoS Attack*, que ocorreu no dia 04/03/2011, dezenas de websites da Coréia do Sul, incluindo websites de agências financeiras, de bancos, de shoppings, de fóruns, de portais, e, principalmente, governamentais, tornaram-se alvos de um ataque bem expressivo. Trata-se de um ataque de dimensões semelhantes ao do *7.7 DDoS Attack,* que também mobilizou uma *botnet* com milhares de máquinas. Devido a uma ação colaborativa fornecida pelo sistema *AhnLab Smart Defense* (ASD), boa parte dos usuários tiveram garantida a continuidade do serviço apesar do ataque massivo (Ahnlab, 2011).

Tais sistemas tem se mostrado promissores no combate ao DDoS e, por conta disso, parece bastante plausível que a ação colaborativa de sistemas *single-link* se adeque a um cenário de detecção inter-SA, cujo o intuito é detectar ataques DDoS

o mais longe da vítima possível, prevenindo antecipadamente a inundação. Contudo, a seleção da métrica que se adeque a esse cenário pode ser determinante para a eficiência do sistema como um todo. Métricas mais sensíveis, como a entropia de Shannon e Divergência, aplicadas nas distribuições estatísticas dos endereços IP ou dos tamanhos dos pacotes, têm sido consideradas eficazes na detecção de tráfego anormal (Xiang, 2011). Entretanto, os elevados índices de falsos positivos e a dificuldade encontrada na configuração dos parâmetros que determinam as margens de segurança são problemas que precisam ser contornados para viabilizar o seu emprego.

Acredita-se que o compartilhamento de alertas e a correlação de dados podem colaborar fortemente para o descarte dos falsos positivos e permitir o uso de técnicas mais sensíveis para a redução do nível de falsos negativos.

NEGAÇÃO DISTRIBUÍDA DE SERVIÇO

De acordo com a cartilha de Segurança para Internet, disponibilizada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), DDoS (*Distributed Denial of Service*) consiste num ataque de negação de serviço distribuído, onde um conjunto de computadores é utilizado para tornar indisponíveis um ou mais serviços ou computadores conectados à Internet (CERT. BR, 2011).

Na maioria das vezes, o intuito desses ataques não é realizar uma invasão, mas impedir que usuários legítimos utilizem um determinado serviço de um computador ou rede. Para tanto, o atacante promove na vítima um aumento do consumo de recursos, tais como memória, poder de processamento, espaço em disco e, principalmente, largura de banda. Estes efeitos são provocados quando a vítima recebe uma quantidade de pacotes ou solicitações maior do que o serviço pode suportar (Feitosa, 2008).

Um ataque DDoS baseia-se no emprego de centenas ou mesmo milhares de máquinas, normalmente comprometidas, que juntas são usadas numa ação coordenada. A quantidade de elementos empregados serve para potencializar o ataque, mas são requeridas algumas etapas para que o ataque ocorra de forma organizada e eficiente. De forma geral, são 3 as fases: (i) “intrusão em massa”, na qual ferramentas automáticas são usadas para comprometer máquinas e obter acesso privilegiado (acesso de *root*); (ii) instalação de software DDoS nas máquinas invadidas com o intuito de montar uma rede de ataque; (iii) lançamento de pacotes contra uma ou mais vítimas, consolidando efetivamente o ataque (Solha, 2011).

A estrutura geral adotada nesse tipo de ataque é composta pelos seguintes elementos:

- **Atacante**: Máquina que coordena o ataque e controla os mestres;
- **Mestre**: Máquina que recebe ordens do atacante e as repassa para os escravos;
- **Client:** Aplicação residente em cada mestre usada para receber as ordens do atacante e repassá-las aos escravos, enviando as instruções para os respectivos *daemons*;
- **Escravo**: Máquina que recebe ordens dos mestres e gera o tráfego contra um ou

mais alvos, conforme definido pelo atacante;

Daemon: Aplicação residente em cada escravo usada para receber as ordens do mestre e executá-las, efetivando assim o ataque;

- **Vítima**: Máquina que sofre o ataque.

Essa forma de atuação contribui não apenas para a constituição de tráfegos bastante significativos, mas também para o anonimato do atacante no momento do ataque. A maneira como os elementos são organizados pode ser visualizado na Figura 3.

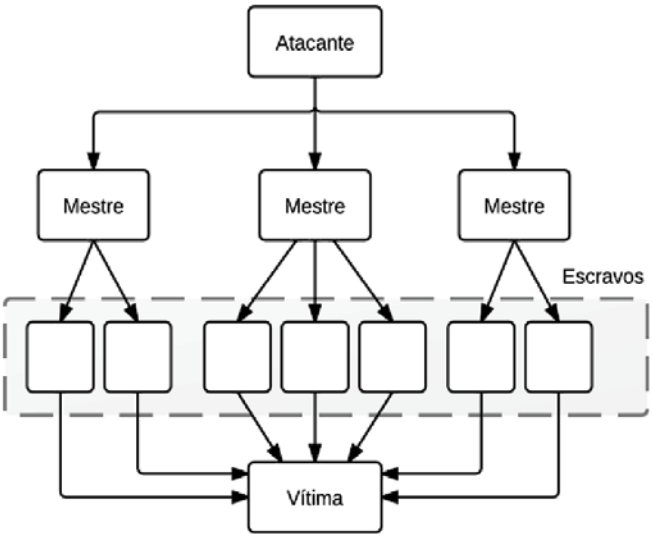

Figura 3. *Estrutura de um ataque DDoS*

Recentemente, grupos de hackers têm convocando internautas interessados em participar de ataques de negação de serviço contra diversas instituições, muitas vezes como forma de protesto ou retaliação (Labovitz, 2010). Normalmente, os ataques são previamente combinados através de calendários organizados, e os programas utilizados para esse fim são disponibilizados na internet para download por esses grupos (Jornalnh, 2012). Neste caso, o ataque de inundação não segue a estrutura descrita na Figura 3, uma vez que os ataques são iniciados voluntariamente, não havendo a necessidade de máquinas que assumem o papel de atacante ou de mestres. Vale salientar que milhares de usuários que realizaram o download desse programa tiveram suas máquinas infectadas (Symantec, 2012).

Existe uma grande variedade de ataques DDoS, e que podem ser classificados de acordo com o grau de automação, vulnerabilidade explorada, mecanismos de propagação, etc. Foi proposto em (Specht, 2004) uma taxonomia que agrupa estes ataques em duas classes principais: ataques de esgotamento da largura de banda e ataques de esgotamento de recursos (Figura 4). No primeiro caso, a inundação da rede da vítima atrapalha o acesso ao serviço, enquanto que no segundo, o consumo de recursos impede a vítima de processar requisições de usuários legítimos.

Figura 4. *Taxonomia de um ataque DDoS*

Os ataques de esgotamento da largura de banda caracterizam-se pelo envio de grande quantia de tráfego IP (*Flood Attacks*), tais como *UDP Flooding* e *ICMP Flooding*, ou pela amplificação de ataque, quando os zumbis enviam pacotes para um endereço de *broadcast IP* e toda a sub-rede associada a esse endereço manda mensagens de resposta à vítima (Figura 5).

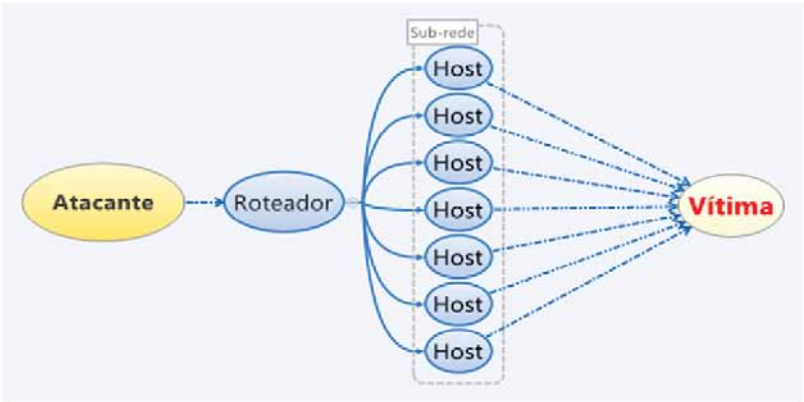

Figura 5. *Amplificação de ataque*

No caso nos ataques de esgotamento de recurso, podem ser exploradas algumas fragilidades da pilha de protocolos TCP/IP, e por conta disso, utilizar esta modalidade contra qualquer computador conectado à Internet. O uso adulterado dos protocolos TCP SYN e PUSH+ACK constituem exemplos deste modalidade de ataque. O envio de pacotes mal formados constitui outra maneira de consumir recursos da vítima. Neste caso, os pacotes IP apresentam algum tipo de incoerência em seu cabeçalho, como, por exemplo, todos os bits do campo *QoS* com o valor 1, ou mesmo o endereço de origem igual ao endereço de destino. Em todos esses casos, e em outros não citados, o aumento número de processos ativos causado pela atividade dos zumbis podem consumir todo o poder de processamento da vítima ou mesmo derrubar o sistema. Um dos fatores que contribuem para a dificuldade na identificação dos fluxos maliciosos, advém da natureza das requisições, que geralmente possuem conteúdo aparentemente legítimo e são originados a partir de conexões TCP válidas.

MÉTODOS DE DETECÇÃO

De maneira geral, combater 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 (Castelucio, 2009). O presente trabalho tem seu enfoque na etapa de identificação do ataque.

Atualmente, os métodos de detecção de ataques DDoS podem ser agrupadas em duas classes principais, cujas métricas se baseiam ou na assinatura de ataques ou na presença de anomalias no tráfego (Xiang, 2011). Na primeira classe, deve-se conhecer um conjunto de assinaturas, tais como padrões ou conjuntos de caracteres, presentes em pacotes maliciosos. Neste caso, além de ser necessário conhecer a assinatura do ataque, o custo computacional para identificar os ataques é bem elevado, e o seu emprego em tráfegos backbone torna-se inviável, a não ser que sejam empregados métodos estatísticos para reduzir o número de pacotes inspecionados. Na outra classe, alterações no comportamento da rede servem como indicação da presença de tráfego malicioso, sendo desnecessário conhecer assinaturas para a identificação de ataques.

Nas métricas baseadas em anomalias, o comportamento do tráfego de rede em condições normais serve de base para a determinação de limites que são ultrapassados na presença de ataques. Nesse caso, a principal vantagem reside na capacidade de detectar ataques desconhecidos. Podem ser baseados em limiares fixos (*threshold*) ou limites que são atualizados em tempo de execução a partir de estatísticas geradas durante o período em que ataques não são detectados.

Os alertas com limiares fixos são adequadas para medidas como, por exemplo, consumo de memória ou processamento, mas são limitados quando há algum tipo de variação, mesmo que esperada (sazonalidade) (Moura, 2009). Neste caso, o número de falsos positivos pode crescer de forma indesejável. Por outro lado, em ataques mais elaborados, limites atualizados em tempo de execução podem ser treinados pelos atacantes, de forma que o sistema vai, gradualmente, interpretando como normal o comportamento anômalo da rede. Além disso, equilibrar as taxas de falsos positivos com as de falsos negativos pode não ser uma tarefa simples (Xiang, 2011).

Entretanto, várias métricas baseadas na teoria da informação tem sido propostas para tentar compensar essas limitações. A entropia de Shannon, por exemplo, fornece o grau de concentração de uma dada distribuição de valores, enquanto que a divergência mede a diferença entre duas distribuições de probabilidade. Essas técnicas tem sido consideradas efetivas na detecção de ataques DDoS, particularmente quando se avalia as distribuições de endereçamento IP e de tamanhos de pacotes.

Entropia de Shannon

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:

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

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 tem a mesma probabilidade de ocorrência.

Em trabalhos anteriores percebeu-se que os valores de Entropia podem representar a dispersão de valores presentes numa dada distribuição, e apresentam boa sensibilidade na identificação de ataques *DDoS*, quando a entropia dos endereços de origem e destino observados num determinado intervalo sofrem alterações expressivas em seus valores. A concentração de pacotes com o mesmo destino tende a aumentar repentinamente, ou seja, o valor de entropia associado ao endereço IP de destino diminui de forma inesperada. Quanto à entropia dos endereços de origem, o valor tende a aumentar, uma vez que aumenta a dispersão. Este último valor está diretamente ligado ao número de atacantes ativos e a taxa de pacotes que cada um envia à vítima. Vale salientar que técnicas de *spoofing* podem ou não ser empregadas nos endereços de origem, da maneira que o atacante achar mais conveniente para tentar mascarar a quantidade real de atacantes, bem como a sua localização, e a identificação da anomalia.

Divergência

Medidas de Divergência são amplamente empregadas em problemas estatísticos cujo foco reside na identificação de mudanças em séries temporais (Basseville, 1993). Existem vários tipos de funções que podem ser empregadas para medir a diferença entre dois conjuntos (Li, 1995), tais como distância de Hellinger (Sengar, 2008), divergência de Kullback-Leibler (Basseville, 1993), divergência Chi-Square (Feinstein, 2003), etc.

Diferente do que ocorre no cálculo da entropia, que retrata a dispersão dos valores em uma dada distribuição probabilística, a divergência permite a comparação entre duas distribuições consecutivas, permitindo a identificação de mudanças abruptas. Quando ocorre um ataque DDoS, espera-se que o número de pacotes destinados a um determinado endereço cresça repentinamente, alterando significativamente sua distribuição de probabilidade. No corrente trabalho, serão abordadas duas modalidades: Chi-Square e divergência de Hellinger.

Chi-Square

A Distância ou Divergência de Chi-Square, ou de X^2, constitui uma medida que retrata a diferença entre duas distribuições de probabilidade, e pode ser definida da seguinte forma.

Sejam duas distribuições discretas de probabilidade, P = (p0, p1, … , pk-1) e Q = (q0, q1, … , qk-1), onde $p_i \geq 0$, $q_i \geq 0$ e $\sum p_i = \sum q_i = 1$. Então, a divergência/distância de X^2 entre a distribuição atual P e anterior Q é dada pela expressão:

$$X^2(P||Q)=\sum_{i=0}^{k-1}(p_i-q_i)^2/q_i \quad (2)$$

Onde X^2 pode assumir valores entre 0 e infinito, de forma que X^2 ($P||Q$) = 0, quando $P = Q$. A medida em que as distribuições se tornam mais discrepantes, X^2 ($P||Q$) aumenta, e quando $P \neq Q$, X^2 ($P||Q$) ≈ ∞.

Vale salientar que esta medida de divergência é assimétrica, de forma que o pico formado devido à mudança no tráfego só ocorre no início do ataque, quando os valores calculados aumentam abruptamente. Para contornar o problema de divisão por zero na expressão (2), que ocorre quando $q_i = 0$, este número pode ser substituído por um valor ε tão pequeno quanto se queira.

Distância de Hellinger

Distância de Hellinger (DH) também constitui uma forma de medir a divergência entre duas distribuições de probabilidade, independentemente da configuração de parâmetros (Sengar, 2008). Pode ser definida da seguinte maneira:

Sejam duas distribuições discretas de probabilidade, $P = (p_0, p_1, \ldots, p_{k-1})$ e $Q = (q_0, q_1, \ldots, q_{k-1})$, onde $p_i \geq 0$, $q_i \geq 0$ e $\sum p_i = \sum q_i = 1$. Então, a DH entre a distribuição atual P e anterior Q é dada pela fórmula:

$$DH(P,Q)=\frac{1}{2}\sum_{i=0}^{k-1}\left(\sqrt{p_i}-\sqrt{q_i}\right)^2 \quad (3)$$

Onde DH pode assumir valores entre 0 e 1, de forma que DH(P,Q) = 0, quando P = Q, e DH(P,Q) = 1, quando P e Q apresentam uma distância máxima. Esperam-se maiores valores de divergência no início e no final de um ataque, com a formação de picos que se destacam.

Limites de Segurança

Para identificar anomalias em séries temporais de medidas de divergência, causadas pelos ataques, podem ser empregados limites de segurança calculados a partir das seguintes expressões:

$$lim_i=\mu_i+2\sigma_i \quad (4)$$

$$\mu_i=\alpha\mu_{i-1}+(1-\alpha)DIV_i \quad (5)$$

$$\sigma_i^2=\alpha\sigma_{i-1}^2+(1-\alpha)(DIV_i-\mu_i)^2 \quad (6)$$

Onde μ_i e σ_i representam, respectivamente, a média e o desvio padrão dos valores de divergência, atualizados através das expressões (5) e (6), cuja suavização das séries é ajustada por α. DIV_i constitui o valor de divergência calculado no instante i.

Estimadores

O emprego de métricas como as descritas nas subseções acima fornece informações relevantes sobre o tráfego de dados inspecionados e, quando utilizadas adequadamente, permitem a detecção de ataques DDoS. Para isso, a distribuição

probabilística das variáveis selecionadas deve sofrer uma alteração significativa ao ocorrer uma anomalia desta natureza. Além disso, existe a necessidade de determinar os limites que separam o tráfego com ataque daquele considerado normal.

Durante a verificação de um tráfego livre de ataques DDoS, o valor da entropia referente aos endereços de destino, por exemplo, apresenta um valor diferente a cada intervalo de tempo. A partir da gravação desses valores calculados é possível montar uma série temporal de valores de entropia referente ao tráfego observado. 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, serão abordados dois estimadores bastante empregados, Exponential Weighted Moving Average (EWMA) e Holt-Winters (HW).

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:

$$x_{t+1} = \alpha X_t + (1 - \alpha)x_t \qquad (7)$$

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.

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, 2004). Na Tabela 1 são apresentadas as equações empregadas nesses dois modelos.

Tabela 1. *Equações dos Modelos de Holt-Winters*

Componente	HW Aditivo	HW Multiplicativo
Residual	$a_t = \alpha(X_t - c_{t-m}) + (1 - \alpha)(a_{t-1} + b_{t-1})$	$a_t = \alpha(X_t \div c_{t-m}) + (1 - \alpha)(a_{t-1} + b_{t-1})$
Tendência	$b_t = \beta(a_t - a_{t-1}) + (1 - \beta)b_{t-1}$	$b_t = \beta(a_t - a_{t-1}) + (1 - \beta)b_{t-1}$
Sazonalidade	$c_t = \gamma(X_t - a_t) + (1 - \gamma)c_{t-m}$	$c_t = \gamma(X_t \div a_t) + (1 - \gamma)c_{t-m}$
Estimativa	$x_{t+1} = a_t + b_t + c_{t+1-m}$	$x_{t+1} = (a_t + b_t)c_{t+1-m}$

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.

Limites de Segurança

Para as margens de confiança, pode ser utilizada a seguinte expressão de suavização exponencial simples para o erro de estimativa:

$$e_t = \gamma| X_t - x_t| + (1 - \gamma)e_{t-m} \quad (8)$$

Onde e_t representa o erro de estimativa no instante t. A componente atualiza-se a cada erro calculado, levando-se em conta os erros calculados no 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 (Mirkovic, 1998). Dessa forma, os limites superior e inferior podem ser calculados a partir das seguintes expressões:

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

$$lim_{Inf} = xt - \delta.e_{t-m} \quad (10)$$

Quando o valor real ultrapassa os limites, fica caracterizada a ocorrência de uma anomalia, que pode indicar a ocorrência de um falso positivo, caso não haja um ataque, ou a detecção do DDoS, caso haja.

CARACTERÍSTICAS DOS TRÁFEGOS INTER-SA

Um Sistema Autônomo (SA) é um grupo conectado de redes IP, executados por um ou mais operadores de rede, que tem uma mesma política de roteamento claramente definida (Hawkinson, 1996).

Sabe-se que todos os computadores se conectam à internet fazem parte de algum SA. Dessa forma, o tráfego de pacotes destinados a máquinas de outro SA deve passar por seus roteadores de borda, que concentram esses fluxos em enlaces inter-SA. Além disso, os SA podem permitir a passagem de tráfego de outros SA através de suas conexões. Por conta disso, o tráfego nestes enlaces tende a apresentar volumes altos, já que abrangem os fluxos de várias conexões, e a variedade de endereços de origem e destino pode ser bastante ampla, particularmente quando o SA permite a passagem de tráfegos de outros SA.

PADRÃO NETFLOW

Tráfegos inter-SA comportam volume de tráfego agregado bastante elevado. Por conta disso, torna-se computacionalmente inviável inspecionar todos os paco-

tes trafegados na rede. Entretanto, com o auxílio de protocolos, muitos roteadores permitem a exportação de informações relevantes do tráfego, viabilizando o seu monitoramento.

A *Cisco Systems* (Cisco, 2011) desenvolveu um protocolo proprietário aberto para a utilização em roteadores Cisco, embora também seja usado em equipamentos de outros fabricantes, conhecido como NetFlow. Os serviços oferecidos por este padrão permitem que administradores de rede tenham acesso a informações referentes aos fluxos IP que passam por suas redes. Os dados exportados podem ser utilizados para vários propósitos, tais como gerenciamento e planejamento de redes, mineração de dados, combate a ataques DDoS, etc. Os roteadores compatíveis com esse padrão gravam o tráfego que passa pelas interfaces e enviam para um ou mais servidores, também conhecidos como "coletores *NetFlow*", informações detalhadas desses fluxos de dados, utilizando pacotes UDP ou SCTP (*Stream Control Transmission Protocol*).

De acordo com (Cisco, 2011), um fluxo IP é uma sequência unidirecional de pacotes que compartilham os mesmos valores para: IP de origem, IP de destino, porta de origem, porta de destino e protocolo. Além disso, caso o intervalo entre os pacotes exceda um dado valor, geralmente 15 segundos na maioria dos roteadores, considera-se que um novo fluxo foi iniciado. Um fluxo IP também pode ser encerrado através de pacotes RST e FIN, para conexões TCP, ou quando o tempo de vida máximo do fluxo é alcançado, geralmente 30 minutos na maioria dos casos.

CONSTRUÇÃO DE UM SISTEMA COLABORATIVO DE DETECÇÃO

Nesta seção, será apresentada a sugestão de um sistema colaborativo que pode aproveitar as peculiaridades das métricas abordadas no corrente trabalho.

Neste sistema, o compartilhamento de dados entre diferentes Sistemas Autônomos e a correlação de alertas pode reduzir os índices de falso positivos e permite uma detecção mais eficaz. Além disso, com o emprego de limites mais sensíveis, a detecção pode ocorrer antecipadamente, em pontos mais afastados da vítima.

No sistema aqui sugerido, a detecção do ataque DDoS ocorre em três etapas. Na primeira, os roteadores de borda enviam para um ou mais servidores pacotes do tipo *NetFlow* referentes aos fluxos que passam pelo Sistema Autônomo. A partir desses dados, podem ser montadas séries temporais que representam o histórico do tráfego avaliado. Nesta etapa, a cada atualização desta série, verifica-se a ocorrência de anomalias nas interfaces, de acordo com as métricas empregadas. Sob condições normais, espera-se que os valores calculados a partir desse extrato respeitem as margens de segurança, que também são atualizadas dinamicamente. Os pacotes *NetFlow*, gerados periodicamente, fornecem dados que são suficientes para a criação e atualização dessas séries temporais e limites.

Para se garantir o mínimo possível de ataques não detectados, critérios suficientemente rigorosos devem ser implementados, uma vez que a taxa de pacotes maliciosos pode ser relativamente baixa em Sistemas Autônomos que estejam mais afastados da vítima. Entretanto, a incidência excessiva de falsos positivos tornaria a técnica inviável. A seleção de métricas e parâmetros mais adequados ao tráfego monitorado pode atender a essas exigências, tornando os limites mais confiáveis.

Verificar a presença de anomalias nos roteadores de borda dos Sistemas Autônomos facilita, de certa forma, o monitoramento dos tráfegos, pois esses pontos são concentradores de fluxos. Entretanto, avaliações individualizadas das violações de limites ocorridos nos roteadores não garantem bons resultados, devido ao alto índice de falsos positivos ocasionados pelo emprego de limites mais sensíveis.

Na segunda etapa, as suspeitas identificadas na etapa anterior são avaliadas como um todo. Nesse momento, busca-se por afunilamentos de fluxo malicioso, caracterizado pela alteração no padrão de tráfego destacada na Figura 6 (c), quando duas ou mais entradas e uma saída apresentam alertas. Essa configuração e aquela destacada na Figura 6 (a) constituem indícios da passagem de ataques DDoS pelo SA avaliado.

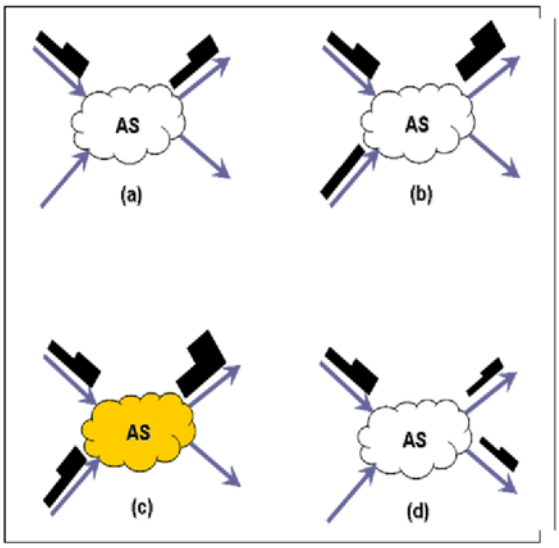

Figura 6. *Padrões de Tráfego em roteadores de borda de Sistemas Autônomos*

Os endereços mais frequentes num mesmo intervalo podem ser facilmente extraídos a partir da leitura de pacotes *NetFlow*. Através dessa análise, pode-se identificar o endereço da vítima, já que o número de pacotes direcionados a esta máquina tende a aumentar. Espera-se que essa identificação seja mais evidente na saída do SA, devido ao acúmulo do tráfego malicioso.

Uma vez identificada a vítima, um alerta pode ser montado e compartilhado com com outros SA. O padrão IDMEF trata da transmissão e do armazenamento de alertas e é bastante flexível (Debar, 2007), podendo ser adaptado para que atenda às necessidades desse sistema.

Na terceira etapa, o SA envia esse alerta para um ou mais SA participantes do sistema colaborativo. Pode-se utilizar o protocolo BGP para viabilizar essa comunicação, uma vez que este protocolo permite a troca de mensagens entre SA, mesmo quando eles não são vizinhos. Desta maneira, forma-se uma uma rede sobreposta, como pode ser observado na Figura 7.

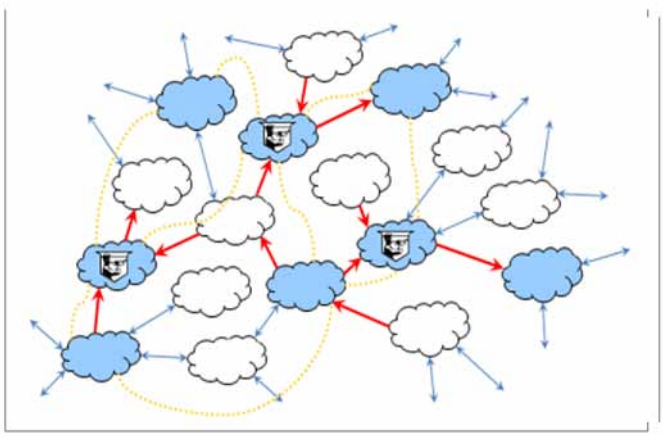

Figura 7. *SA participantes do Sistema Colaborativo de Detecção*

Após o recebimento dos alertas, os mesmos podem ser armazenados numa tabela, para fins de correlação. Espera-se que sejam gerados vários alertas, mas a confirmação da presença do ataque só se dará quando, num dado intervalo de tempo, um mesmo endereço estiver presente em alertas de vários SA. Desta forma, os falso positivos gerados na primeira e na segunda etapa podem ser descartados, aumentando a eficácia do sistema. À medida em que os ataques se aproximam da vítima, o volume de tráfego malicioso aumenta e, consequentemente, torna-se mais evidente a confirmação e identificação do ataque, como pode ser visto na Figura 8.

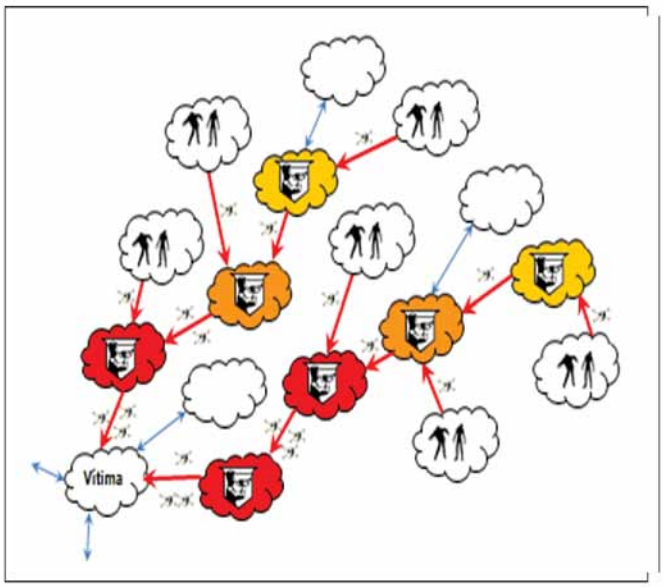

Figura 8. *Compartilhamento de alertas confirmando a existência de ataque*

Esta sugestão apenas representa uma maneira de realizar a detecção de um ataque DDoS de forma antecipada seguindo um esquema colaborativo, e que ainda precisa ser melhor estudada para verificar sua viabilidade.

CONSIDERAÇÕES FINAIS

Embora existam estudos desde o ano de 2000, ainda não há uma resposta definitiva contra ataques DDoS, de forma que ainda há espaço para contribuições. Soluções baseadas na correlação de dados e agregação do tráfego em fluxos, parecem ser a tendência para soluções futuras.

Neste artigo, foram apresentados algumas das pesquisas relacionadas à detecção de ataques DDoS, com enfoque nos métodos baseados na detecção de anomalias. Foram apresentadas, também, algumas das métricas que podem ser empregadas na identificação de ataques.

O emprego de métricas mais sensíveis representa uma maneira de realizar a detecção de um ataque DDoS de forma antecipada, pois possibilita a identificação de alterações mais suaves do comportamento do tráfego. A utilização de um esquema colaborativo, como o sugerido neste artigo, pode reduzir os índices de falso positivos e permitir uma detecção mais eficaz, tornando a solução mais viável.

REFERÊNCIAS BIBLIOGRÁFICAS

- *AHNLAB, INC.; Analytical report on 3.4 DDoS attack; White paper, April 2011; URL: http://www.ahnlab.com, acessado em 10 de julho de 2011.*
- *ANITHA, E.; Malliga, S.;* **A packet marking approach to protect cloud environment against DDoS attacks;** *Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.367,370, 21-22 Feb.* ***2013****.*
- *BASKAR, M.; Gnanasekaran, T.; Saravanan, S.;* **Adaptive IP traceback mechanism for detecting low rate DDoS attacks;** *Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on , vol., no., pp.373,377, 25-26 March* **2013***.*
- *BASSEVILLE, M.; Nikiforov, I.;* **Detection of Abrupt Changes: Theory and Applications;** *Em Englewood Cliffs, NJ: Prentice Hall, Inc.,* **1993***.*
- *BRUTLAG, J. D.;* **Aberrant Behavior Detection in Time Series for Network Monitoring***; Proceedings of the 14th Systems Administration Conference (LISA 2000),* **2000***.*
- *BUVANESWARI, M.; Subha, T.;* **IHoneycol: A distributed collaborative approach for mitigation of DDoS attack;** *Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.340,345, 21-22 Feb.* **2013***.*
- *CABRERA, J. B. D.; Lewis, L.; Qin, X.; Lee, W.; Prasanth, R. K.; Ravichandran, B.; Mehra, R. K.;* **Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables - A Feasibility Study;** *7th IFIP/IEEE International Symposium on Integrated Network Management, Seattle, WA-May 14-18,* **2001***.*
- *CASTELÚCIO, A. O.; Salles, R. M.; Ziviani, A.;* **An AS-Level Overlay Network for IP Traceback***; IEEE Network, Vol. 23, pp. 36-41,* **2009***.*
- *CERT.BR.;* **Cartilha de segurança para Internet***; URL:* http://cartilha.cert.br*, acessado em 10 de novembro de* **2011***.*
- *CHEN, Y.; Hwang, K.;* **Collaborative Change Detection of DDoS Attacks on Community and ISP Networks;** *IEEE Networks, pp. 401 - 410,* ***2006****.*
- *CHEN, Y.; Hwang, K.; Ku, W. S.;* **Collaborative Detection of DDoS Attacks over Multiple Network Domains***; IEEE Transactions on Parallel and Distributed Systems, Vol. 18, Issue 12, pp.*

1649 - 1662, **2007**.

- *CHEN, Yonghong; Ma, Xinlei; Wu, Xinya;* **DDoS Detection Algorithm Based on Preprocessing Network Traffic Predicted Method and Chaos Theory***; Communications Letters, IEEE , vol.17, no.5, pp.1052,1054, May* **2013**.
- *CHWALINSKI, P.; Belavkin, R.; Cheng, X.;* **Detection of Application Layer DDoS Attacks with Clustering and Bayes Factors;** *Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on , vol., no., pp.156,161, 13-16 Oct.* ***2013***.
- *Cisco Systems, INC.; NetFlow Version 9 Flow-Record Format; white paper URL: http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html, acessado em 2 de junho de 2011.*
- *DEBAR, H.; Curry, D.; Feinstein, B.;* **The Intrusion Detection Message Exchange Format (IDMEF);** *RFC 4765, March* **2007***, URL http://www.ietf.org/rfc/rfc4765.txt.*
- *DEMIR O.; Khan B.;* **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* **2010**.
- *DITTRICH D.; Dietrich S.;* **P2P as botnet command and control: a deeper insight***; IEEE Network, 3rd International Conference on Malicious and Unwanted Software pp. 41-48,* **2008**.
- *ESTEVEZ-Tapiador, J. M.; Garcia-Teodoro, P.; Diaz-Verdejo, J. E.;* **Anomaly Detection Methods in Wired Networks: a Survey and Taxonomy***; Computer Communications, Vol. 27, 1569-1584,* **2004**.
- *FEI Wang; Xiaofeng Wang; Jinshu Su; Bin Xiao;* **VicSifter: A Collaborative DDoS Detection System with Lightweight Victim Identification;** *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on , vol., no., pp.215,222, 25-27 June* **2012**.
- *FEINSTEIN, L.; Schnackenberg, D.; Balupari, R.; Kindred, D.;* **Statistical approaches to DDoS attack detection and response;** *Em: DARPA Information Survivability Conference and Exposition, 2003. Proceedings, Vol. 1 , pp. 303 – 314, April* **2003**.
- *FEITOSA, E. L.; Souto, E. J. P.; Sadok, D.;* **Tráfego Internet não Desejado: Conceitos, Caracterização e Soluções;** *Livro-texto dos Minicursos do VIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, páginas 91-137,* **2008**.
- *FENG, J.; Liu, Y.;* **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),* **2009**.
- *FERRER, Z.; Ferrer, M. C.; In-depth Analysis of Hydraq; URL:* http://www.ca.com/files/securityadvisornews/in-depth_analysis_of_hydraq_final_231538.pdf*, acessado em novembro de* **2010**.
- *HAWKINSON, J.;* **Guidelines for creation, selection, and registration of an Autonomous System (AS);** *RFC* **1930***, March 1996, URL:* http://tools.ietf.org/html/rfc1930.
- *ISC;* **internet host count history;** *URL:* https://www.isc.org/solutions/survey/history*, acessado em 7 de novembro de* **2011**.
- *JIN Zhigang; Wang Ying; Wei Bo;* **P2P Botnets detection based on user behavior sociality and traffic entropy function***; Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, vol., no., pp.1953,1955, 21-23 April* **2012**.
- *Jornalnh;* **Anonymous convoca ataque ao Facebook no dia 28 de Janeiro 2012***, URL:* http://www.jornalnh.com.br/tecnologia/369601*, acessado em 22 de maio de* **2012**.
- *KALEKAR, P. S.; Rekhi, K.;* **Time series Forecasting using Holt-Winters Exponential Smoothing;** *School of Information Technology, December 6,* **2004**.

- *KATKAR, V. D.; Kulkarni, S. V.;* **Experiments on detection of Denial of Service attacks using Naive Bayesian classifier;** *Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on , vol., no., pp.725,730, 12-14 Dec. 2013.*
- *KAUR G.; Saxena V.; GUPTA J. P.;* **Anomaly Detection in Network Traffic and Role of Wavelets***; IEEE, 2nd International Conference on Computer Engineering and Technology (ICCET),* **2010***.*
- *KAUR, G.; Varma, S.; Jain, A.;* **A novel statistical technique for detection of DDoS attacks in KDD dataset;** *Contemporary Computing (IC3), 2013 Sixth International Conference on , vol., no., pp.393,398, 8-10 Aug.* **2013***.*
- *KHATTAK, S.; Ramay, N. R.; Khan, K. R.; Syed, A. A.; Khayam, S. A.;* **A Taxonomy of Botnet Behavior, Detection, and Defense;** *Communications Surveys & Tutorials, IEEE , vol.16, no.2, pp.898,924, Second Quarter* **2014***.*
- *KLINE, J.; Nam, S.; Barford, P.; Plonka, D.; Ron, A.;* **Traffic Anomaly Detection at Fine Time Scales with Bayes Nets***; The Third International Conference on Internet Monitoring and Protection, 2008. ICIMP'08, PP. 37-46,* **2008***.*
- *LABOVITZ, C.;* **The Internet Goes to War***; Em ARBOR SERT, URL:* http://ddos.arbornetworks.com/2010/12/the-internet-goes-to-war/*, acessado em 22 de maio de* **2012***.*
- *LAKHINA, A.; Crovella, M.; Diot, C.;* **Mining Anomalies Using Traffic Feature Distributions***; Proceedings of the* **ACM SIGCOMM'05***, Philadelphia, Pennsylvania, USA,* **2005***.*
- *LAUFER, R. P.; Velloso, P. B.; Cunha, D. de O.; Moraes, I. M.; Bicudo, M. D. D.; Duarte, O. C. M. B.;* **A new IP traceback system against denial-of-service attacks***; Em 12th International Conference on Telecommunications - ICT'2005, Capetown, South Africa, May* **2005***.*
- *LAW, K. T.; Lui, J. C. S.; Yau, D. K. Y.;* **An Effective Methodology to Traceback DDoS Attackers;** *X IEEE Int'l Symp, MASCOTS'02,* **2002***.*
- *LI, T.;* **Robust Divergence Measures for Time Series Discrimination***; Tech. Rept. 237, Department of Statistics, Texas A&M Univ., College Station,* **1995***.*
- *LIN, B. P.; Uddin, M. S.;* **Synmon Architecture for Source-based SYN-flooding Defense on Network Processor***; IEEE, 2005 Asia-Pacific Conference on Communications, Perth, Western Australia,* **2005***.*
- *LUO, Y. B.; Wang, B. S.; Sun, Y. P.; Zhang, B. F.; Chen, X. M.;* **FL-LPVG: An approach for anomaly detection based on flow-level limited penetrable visibility graph;** *Information and Network Security (ICINS 2013), 2013 International Conference on , vol., no., pp.1,7, 22-24 Nov.* **2013**
- **LUCENA***, S. C.; A. S.;* **Detecção de Anomalias Baseada em Análise de Entropia no Tráfego da RNP***; XIII WGRS, pp. 163-176, 2008.*
- *MIRKOVIC, J.; Reiher, P.;* **D-WARD: A Source-End Defense against Flooding DoS Attacks***; IEEE Trans. Dependable and Secure Computing, pp. 216-232,* **2005***.*
- *MOURA, A. S.;* **Detecção de Anomalias em Redes WAN usando Estimativa de Holt-Winters Aplicada a Medidas de Entropia***; Dissertação de Mestrado – UFRJ-***2009***.*
- *NAFIR, Abdenacer; Mazouzi, Smaine; Chikhi, Salim;* **Collective intrusion detection in wide area networks;** *Innovations in Intelligent Systems and Applications (INISTA) Proceedings, 2014 IEEE International Symposium on , vol., no., pp.46,51, 23-25 June* **2014***.*
- *PAUL, V.; Prasadh, K.; Sankaranarayanan;* **Application: DDoS Attacks Resistance Scheme Using Polynomial Distribution Model;** *Advances in Computing and Communications (ICACC), 2013 Third International Conference on , vol., no., pp.304,307, 29-31 Aug.* **2013***.*
- *PAPADOPOULOS, C.; Lindell, R.; Mehringer, J.; Hussain, A.; Govindan, R.;* **COSSACK: Coordinated Suppression of Simultaneous Attacks***; Proc.Third DARPA Information Survivability Conf. and Exposition (DISCEX-III'03), pp.2-13,* **2003***.*

- *PARK K.; Lee H.;* **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,* ***2000****.*
- ***PASCHALIDIS****, I. C.; Smaragdakis, G.;* **Spatio-Temporal Network Anomaly Detection by Assessing Deviations of Empirical Measures***; IEEE/ACM Transactions on Networking, vol.17, no.3,* ***2009****.*
- *PHAAL, P.; Panchen, S.; Mckee, N.; InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks; RFC 3176 (Informational), setembro* ***2001****. URL http://www.ietf.org/rfc/rfc3176.txt.*
- *SANMORINO, A; Yazid, S.;* **DDoS Attack detection method and mitigation using pattern of the flow;** *Information and Communication Technology (ICoICT), 2013 International Conference of , vol., no., pp.12,16, 20-22 March* ***2013****.*
- SARDANA*, A.; Joshi, R. C.;* **Dual-Level Attack Detection and Characterization for Networks under DDoS***; International Conference on Availability, Reliability, and Security, ARES '10 , pp. 9 - 16,* ***2010****.*
- *SARRAUTE, C.; Miranda, F.; Orlicki, J. I.;* **Simulation of Computer Network Attacks;** *Symposium on Computing Technology, Argentine,* ***2007****.*
- *SENGAR, H.; Wang H.; Wijesekera, D.; Jajodia, S.;* **Detecting VoIP Floods Using the Hellinger Distance;** *Em IEEE Transactions on Parallel and Distributed Systems, Journal Vol. 19, Issue 6, pp. 794 - 805, June* ***2008****.*
- *SHARIFNYA, R.; Abadi, M.;* **A novel reputation system to detect DGA-based botnets;** *Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on , vol., no., pp.417,423, Oct. 31 2013-Nov. 1* ***2013****.*
- *SHANNON, C. E.;* **A mathematical theory of communication;** *Bell System Technical Journal, 27:379-423 and 623-656,* ***1948****.*
- *SHUI, Yu; Wanlei, Zhou; Song, Guo; Minyi, Guo;* **A dynamical Deterministic Packet Marking scheme for DDoS traceback;** *Global Communications Conference (GLOBECOM), 2013 IEEE , vol., no., pp.729,734, 9-13 Dec.* ***2013****.*
- *SNOEREN, A. C.; Partridge, C.; Sanchez, L. A.; Jones, Tchakountio, C. E. F.; Schwartz, B.; Kent, S. T.; Strayer, W. T.;* **Single-packet IP traceback;** *IEEE/ACM Trans. Netw., 10(6):721–734, December* ***2002****.*
- *SOLHA, L.; Teixeira , R.; Piccolini, J.;* **Tudo que você precisa saber sobre os ataques DDoS***; URL:* http://www.rnp.br/newsgen/0003/ddos.html*, acessado em 10 de maio de* ***2011****.*
- *SPECHT, S.; Lee. R.;* **Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures;** *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September* ***2004****.*
- *SYMANTEC.* **Anonymous Supporters Tricked into Installing Zeus Trojan***; Março 2012, URL:* http://www.symantec.com/connect/blogs/anonymous-supporters-tricked-installing-zeus-trojan*, acessado em 22 de maio de* ***2012****.*
- *WALFISH, M.; Vutukuru, M.; Balakrishnan, H.; Karger, D. R.; Shenker, S.;* **DDoS defense by offense;** *ACM Transactions on Computer Systems (TOCS), Journal Vol. 28, Issue 1,* ***2010****.*
- *WANG, L.; Wu, Q.; Liu, Y.;* **Design and Validation of PATRICIA for the Mitigation of Network Flooding Attacks***; IEEE CSE'09, Vanoucer, BC, Canada,* ***2009****.*
- *XIANG, Y.; Li, K.; Zhou, W.;* **Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics;** *IEEE Transactions on Information Forensics and Security, Vol. 6, No. 2, June*

2011.

- *XINLEI, Ma; Yonghong, Chen;* **DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy;** *Communications Letters, IEEE , vol.18, no.1, pp.114,117, January* **2014**.
- *YUAN, Tao; Shui, Yu;* **DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics;** *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on , vol., no., pp.233,240, 16-18 July* **2013**.