Identificação da Componente de Tráfego de Ataque baseada em Discriminantes Estatísticos

Raimir Holanda Filho[1], J. E. Bessa Maia[2], Marcus F. F do Carmo[1]

[1]Mestrado em Informática Aplicada, Universidade de Fortaleza
Campus Unifor, Bl – J, Fortaleza, Brasil

[2]Departamento de Estatística e Computação, Universidade Estadual do Ceará
Campus do Itaperi, Fortaleza, Brasil

raimir@unifor.br, jmaia@uece.br, marcusfabio@edu.unifor.br

Abstract. The characterization of the network traffic composition is an important subject to network design. Capacity planning of links, processors, switches or buffers with acceptable level of services such as queue delay and packet loss, depends on the traffic composition and the demand that each component of this composition sets on over network elements. To study the influence of attacks into the network and servers performance, the first step consists of identify the amount of attack traffic present into the network workload. The approach presented here uses a small number of statistical discriminators and cluster analysis to identify the attack component present into the network traffic.

Resumo. A caracterização da composição do tráfego da rede é um tema fundamental na elaboração de um projeto de rede. Todos os dimensionamentos de capacidade sejam de links, processadores, comutadores ou *buffers*, com o objetivo de obter níveis aceitáveis de serviço, tais como, atrasos de fila e perda de pacotes, dependem da composição do tráfego e da demanda que cada componente dessa composição impõe sobre os elementos da rede. Para estudar o efeito de ataques sobre a performance da rede, a primeira etapa consiste na identificação do volume de tráfego de ataque presente na carga de trabalho da rede. A abordagem apresentada neste trabalho utiliza um reduzido número de discriminantes estatísticos e análise de agrupamento para identificar a componente de ataque presente no tráfego da rede.

1. Introdução

Planejar a capacidade dos elementos de uma rede de computadores, como *links*, processadores, comutadores ou *buffers*, requer que uma série de etapas seja realizada de forma sistemática. Uma etapa importante consiste na caracterização da carga de trabalho.

A caracterização da carga de trabalho é o processo de se descrever de forma precisa a carga de trabalho em termos de suas componentes. Cada componente da carga de trabalho é em seguida decomposto em componentes básicas. As componentes básicas são então caracterizadas pela intensidade da carga de trabalho e pelos parâmetros de demanda de serviços em cada recurso [Menascé e Almeida 2002].

Uma primeira etapa para o estudo da influência dos ataques na rede e no desempenho dos servidores é a detecção de que há um ataque em curso. Posteriormente há etapas como identificação da fonte ou natureza do ataque, quantificação, etc. Este

artigo explora a importância em se identificar a quantidade de tráfego de ataque presente em uma carga de trabalho de rede. Assim como em [Zuev e Moore 2005], a principal referência utilizada em nosso trabalho, não levamos em consideração os diferentes tipos de ataques e suas características diversas (DoS, Vírus, Worms, Spams, etc). Preocupamos-nos apenas em identificar a incidência ou não de um fluxo de ataque (seja ele qual for) no tráfego coletado.

Grandes esforços têm sido dedicados em pesquisas relacionadas a segurança em redes de computadores. Este fato decorre do aumento considerável com que as atividades de ordem pessoal, empresarial e governamental dependem das redes de computadores. Um ataque a uma rede de computadores pode implicar em diferentes níveis de ameaças, desde a perda de privacidade até enormes prejuízos de ordem financeira. Um ataque pode ser considerado, portanto, como a utilização de uma determinada rede com o propósito de comprometer a segurança das informações armazenadas ou transportadas nesta rede.

Existem várias abordagens na literatura para identificação de tráfego de ataques, dentre elas, detecção baseada em assinaturas [Kim e Karp 2004], detecção baseada em comportamento [Brutlag 2000], anomalias,[Barford et al. 2002], [Roughan et al. 2004], [Lakhina et al. 2004a], [Lakhina et al. 2004b], [Lakhina et al. 2005] e propriedades estatísticas [Zuev e Moore 2005].

Os métodos de identificação baseados em assinatura extraem os dados da rede e identificam os ataques usando seqüências de dados conhecidas e que estão presentes no conteúdo dos pacotes. Tais métodos além de ineficientes, pois não se adaptam a novos tipos de ataques, apresentam sérias restrições relacionadas à privacidade dos dados que estão trafegando pela rede e nem sempre assinaturas estão disponíveis para todos os tipos de ataques.

Uma segunda abordagem empregada utiliza uma massa de dados com ataques previamente identificados para treinar algoritmos de aprendizagem quanto ao comportamento dos ataques. Essa abordagem apresenta a vantagem de que o algoritmo pode ser novamente treinado para aprender sobre novos tipos de ataques. Entretanto, para que isso seja possível, nós devemos inserir instâncias desses novos ataques no arquivo de treinamento, e o método automaticamente reajustaria seu conjunto de regras para que a detecção possa ser realizada.

As duas abordagens apresentadas anteriormente possuem sérias limitações, pois ambas necessitam que os ataques sejam previamente conhecidos e, portanto, novos tipos de ataques não serão detectados. Para superar essas restrições, outras abordagens têm sido aplicadas.

O método de detecção de anomalias detecta comportamentos anormais nos dados, ou seja, detecta desvios do comportamento considerado normal. Esta abordagem apresenta a grande vantagem de ser possível além de detectar os ataques conhecidos, ser capaz de detectar novos tipos de ataques, pois esses novos ataques provocarão desvios no comportamento normal da rede. Normalmente, métodos de detecção de anomalias necessitam de um conjunto de dados considerado limpo, ou seja, sem a presença de ataques para que se conheça o comportamento normal da rede.

Esse trabalho baseia-se na utilização de métodos estatísticos multivariados para identificação do tráfego de ataque. A abordagem apresentada utiliza um reduzido

número de discriminantes estatísticos e análise de agrupamento para identificação de tráfego de ataque com resultados superiores aos encontrados até então na literatura relacionada. Análise de agrupamentos por ser uma técnica não supervisionada, permite que novos ataques sejam detectados. O método apresentado foi validado utilizando *traces* reais.

Na seção 2 deste artigo são apresentados os principais trabalhos publicados recentemente relacionados a identificação de tráfego de ataque. Na seção 3, descrevemos os dados utilizados para validar nossa proposta de identificação de tráfego de ataque. São utilizados dados reais, onde os fluxos de ataques foram previamente identificados. Uma descrição da metodologia para identificação de tráfego de ataque é apresentada na seção 4, onde descrevemos em detalhes a forma como a análise de agrupamento foi aplicada ao problema de identificação de tráfego de ataque. No decorrer da seção 5 são apresentados e discutidos os resultados encontrados e finalmente na seção 6 as principais conclusões e direções de pesquisas futuras.

2. Trabalhos Relacionados

Identificação de tráfego de ataque tem recebido considerável atenção nos últimos anos constituindo-se em uma importante área de pesquisa. Entretanto, muitos dos trabalhos publicados em identificação de tráfego de ataque têm se restringido a tipos específicos de ataques tais como *DoS attacks* [Hussain et al. 2003], *port scan* [Jung et al. 2004], *worms* [Kim e Karp 2004] e [Schechter et al. 2004].

Em [Jung et al. 2002], os autores apresentam uma metodologia para identificar *flash crowds* e ataques de negação de serviço (DoS – *Denial of Service*). Foram estudadas as propriedades de ambos os tipos de eventos com uma especial atenção para as características que distinguem os dois.

Uma abordagem comumente utilizada para detectar tais ataques tem sido tratar anomalias como desvios de volume de tráfego [Barford et al. 2002], [Brutlag 2000], [Lakhina et al. 2005], [Roughan et al. 2004]. Em [Lakhina et al. 2004a], são tratadas anomalias em redes de *backbone* analisando a quantidade de bytes através de um enlace enquanto que em [Lakhina et al. 2004b] são analisados o volume de tráfego em fluxos de Origem-Destino (OD). A abordagem de detecção de anomalias baseada em volume tem tido sucesso em identificar grandes mudanças no perfil do tráfego tal como ataques conhecidos como *bandwidth flooding attacks*, entretanto, existem várias classes de anomalias que não causam alterações significativas no volume de tráfego. Outras abordagens têm sido utilizadas baseadas na exploração de correlação de padrões entre diferentes variáveis da MIB SNMP [Thottan e Ji. 2003], ou baseadas em heurísticas para identificar tipos específicos de anomalias em fluxos de pacotes IP [Kim et al. 2004].

Em [Portnoy et al. 2001] é apresentado um método de detecção automática de intrusões onde é possível detectar ataques ainda desconhecidos, entretanto, é aplicado a um escopo reduzido de tipos de ataques. Um método baseado em anomalias [Taylor and Alves-Foss 2000] tem mostrado alta eficiência na operação por implicar em um baixo custo para a rede. Usando *traces* reais, em [Taylor and Alves-Foss 2001] é apresentado uma análise de eventos anormais de tráfego.

Todos esses métodos apresentados acima utilizam métricas baseadas em volume de tráfego o que pode levar a inúmeros falsos positivos, como por exemplo, a

identificação de um tráfego *flash crowd* como sendo um ataque DoS (*Denial of Service*) [Jung et al. 2002]. Nós acreditamos, portanto, que todos eles têm um alcance limitado na identificação de tráfego de ataques uma vez que não possuem um conjunto suficiente de informações para definir comportamentos anormais.

Por outro lado, como observado em [Zuev e Moore 2005] e em nosso trabalho, métodos que são capazes de examinar individualmente propriedades estatísticas dos fluxos são bastante mais eficientes.

3. Descrição dos *Traces*

Qualquer trabalho relacionado com a identificação de ataques requer a utilização de dados. Com o objetivo de avaliar a metodologia proposta e os discriminantes selecionados, foi utilizado um conjunto de *traces* de tráfego pré-processados. O método de coleta dos dados é descrito em [Moore et al. 2003], tendo sido os dados aqui utilizados disponibilizados em [Moore et al. 2005]. Esses dados são reais e foram coletados de uma rede com aproximadamente 1.000 usuários conectados a Internet através de uma conexão *full-duplex* Gigabit Ethernet e referem-se a um período de 24 horas. Foi gerado um conjunto de 10 arquivos sendo cada um referente a um período de 1.680 segundos (28 minutos), e disponibilizados para a comunidade científica. Os *traces* foram utilizados em [Moore e Papagiannaki 2005], [Moore et al. 2005], [Zuev e Moore 2005] e [Auld et al. 2007]. Neste pré-processamento, para cada fluxo coletado foi identificada a aplicação na qual ele está associado. A tabela 1 mostra as aplicações encontradas nos *traces* e suas classes correspondentes.

Tabela 1. Classes e Aplicações

Classes	Aplicações Presentes nos *Traces*
BULK	ftp
DATABASE	postgres, sqlnet oracle, ingres
INTERACTIVE	ssh, klogin, rlogin, telnet
MAIL	imap, pop2/3, smtp
SERVICES	X11, dns, ident, ldap, ntp
WWW	www
P2P	KaZaA, BitTorrent, GnuTella
ATTACK	Internet worm and virus attacks
GAMES	Half-Life
MULTIMEDIA	Windows Media Player, Real Player

O uso de *traces* pré-classificados possibilita a utilização de um subconjunto de fluxos de tráfego para treinamento do algoritmo de classificação. Após concluída esta etapa pode-se utilizar um outro subconjunto de fluxos de tráfego para validar a eficácia do método proposto.

Neste artigo é utilizada uma abordagem baseada em fluxo. Os fluxos são identificados como uma seqüência de pacotes que apresentam o mesmo conjunto de valores contidos nos seguintes campos do cabeçalho TCP/IP: endereço IP de origem, endereço IP de destino, porta TCP de origem, porta TCP de destino e tipo de protocolo.

A quantidade de fluxos de ataque e não ataque em cada *trace* é descrita na tabela 2 a seguir.

Tabela 2. Fluxos por Trace

Fluxos	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	Total
Ataque	122	19	41	324	122	134	89	129	367	446	1793
Não Ataque	24741	23782	22891	21961	21526	19250	55746	55365	65881	64590	375733
Total	24863	23801	22932	22285	21648	19384	55835	55494	66248	65036	377526
% Ataque	0,49%	0,08%	0,18%	1,45%	0,56%	0,69%	0,16%	0,23%	0,55%	0,69%	5,09%

Além das categorias de aplicações, durante o pré-processamento foi gerado para cada fluxo um conjunto de estatísticas relacionadas ao fluxo que em [Moore et al. 2005] são chamados discriminantes. Um total de 249 discriminantes foi gerado incluindo estatísticas simples sobre o tamanho do pacote e o tempo entre pacotes, e informações derivadas do protocolo de transporte (TCP) tais como contadores de pacotes *Syn* e *Ack*.

As informações estatísticas geradas foram derivadas a partir das informações contidas nos cabeçalhos dos pacotes enquanto que na definição da classe da aplicação foi utilizada uma análise baseada em conteúdo. Portanto, nossas análises têm como ponto de partida estes dados pré-processados nos quais para cada fluxo foram gerados um conjunto de estatísticas e uma classe que define a aplicação.

4. Metodologia

A metodologia constitui-se em duas etapas: seleção dos discriminantes e formação dos agrupamentos de fluxos de ataques. A seleção dos discriminantes constitui uma das etapas mais importantes e difíceis no processo de identificação de componentes de tráfego.

4.1. Seleção dos Discriminantes

A tarefa de identificação de tráfego de ataque é de fato uma tarefa de classificação. A etapa de identificação dos discriminantes que serão utilizados na fase de classificação é provavelmente a de maior importância. A qualidade da classificação está diretamente relacionada com os discriminantes escolhidos para sua elaboração.

Quando se considera a utilização de variáveis discriminantes, é essencial que se tenha medido, nos elementos amostrais, variáveis que possam realmente distinguir as populações, caso contrário a qualidade da classificação estará comprometida. Um equívoco bastante comum consiste em se pensar que quanto maior o número de discriminantes, melhor será a solução alcançada. Um dos métodos de detecção de discriminante bastante disseminado é baseado em análise de variância [Anderson 1958], tendo sido aplicado a este trabalho. A partir do *trace* classificado, cada variável é examinada individualmente e independentemente e sua distribuição F é calculada. A distribuição F utiliza a razão de duas estimativas, dividindo a estimativa da variância "entre" S_E^2 , pela estimativa da variância "dentro" S_D^2, assim definida:

$$\text{Distribuição F} = \frac{S_E^2}{S_D^2} \qquad (1)$$

onde,

$$S_E^2 = n\frac{\sum(\bar{x}_j - \bar{\bar{x}})^2}{(k-1)} \quad (2)$$

e

$$S_D^2 = \frac{1}{k(n-1)}\left[\sum(x_i - \bar{x}_1)^2 + \ldots + \sum(x_i - \bar{x}_k)^2\right] \quad (3)$$

sendo, *k* o número de amostras e *n* o número de observações em cada amostra.

Na distribuição F, existe uma distribuição diferente para cada combinação de tamanho da amostra *n* e número de amostras *k*. A distribuição é contínua em todo o intervalo de 0 a +∞. Além disso, grandes diferenças entre médias amostrais juntamente com pequenas variâncias amostrais podem resultar em valores de F extremamente grandes.

Após a definição dos valores da distribuição F para cada uma das 249 variáveis, as variáveis com valores da distribuição F mais significativos estão relacionadas às variáveis mais importantes para a discriminação dos grupos e, portanto, serão consideradas discriminantes.

4.2. Técnica de Análise de Agrupamento

A análise de agrupamento pertence a um conjunto de técnicas para análise estatística multivariada. Análise estatística multivarida é apropriada para qualquer conjunto de dados onde múltiplas medidas são realizadas com possíveis correlações entre essas medidas. Técnicas mutivariadas em geral, analisam a estrutura de correlação entre diversas variáveis, podendo revelar resultados mais completos do que se as variáveis fossem analisadas separadamente [Johnson 1998]. Análise de agrupamento, portanto, pode ser utilizada para encontrar grupos nos dados sob análise [Kaufman e Rousseeuw 1990]. A técnica de análise de agrupamento compreende um conjunto de diferentes algoritmos e métodos para agrupar objetos de tipos similares em respectivas categorias. O problema enfrentado por muitos pesquisadores em diferentes áreas consiste exatamente em como organizar os dados sob análise em estruturas que sejam suficientemente representativas. Em outras palavras, análise de agrupamento é uma ferramenta exploratória que busca particionar os componentes em diferentes grupos tal que membros de um mesmo grupo sejam os mais similares possíveis e membros de diferentes grupos sejam os mais diferentes possíveis [Jain 1991].

Estatisticamente, isso implica que a variância intra-grupo deve ser a menor possível e que a variância inter-grupo deve ser a maior possível. Cada agrupamento então descreve, em termos dos dados coletados, a classe a qual seus membros pertencem.

Análise de agrupamento é, portanto uma ferramenta de descoberta. Esta análise pode revelar associações nos dados sob análise, ainda que essas associações não sejam evidentes, porém são úteis uma vez que possam ser descobertas. Os resultados obtidos com a análise de agrupamento podem contribuir para a definição de um esquema de classificação mais formal.

Análise de agrupamento tem sido descrita na literatura através de várias técnicas. Entretanto, todas essas técnicas basicamente pertencem a duas classes: hierárquica e não hierárquica. Na abordagem não hierárquica, inicia-se com um conjunto arbitrário de agrupamentos e os membros dos agrupamentos são movidos até que a variância intra-grupo seja mínima. A abordagem hierárquica pode ser implementada de duas maneiras: divisiva ou aglomerativa. Utilizando a forma hierárquica aglomerativa, dados *n* componentes, o método inicia com *n* agrupamentos (cada agrupamento tendo um componente). Então agrupamentos são unidos sucessivamente até se obter um desejado número de agrupamentos. Na forma hierárquica divisiva, inicia-se com um único agrupamento (de *n* componentes) e então divide-se os agrupamentos sucessivamente até se obter um número desejado de agrupamentos. Diversos conceitos de distância têm sido utilizados para formar os agrupamentos. Os mais conhecidos são: distância euclidiana, distância ponderada, distância de Minkowski e o coeficiente de concordância de Jaccard [Mingoti 2005]. Neste trabalho utilizamos a distância euclidiana dada por:

$$dist(x,y) = \sqrt{\sum (x_i - y_i)^2} \quad (4)$$

onde x_i e y_i são as coordenadas dos pontos x e y.

Análise de agrupamento foi utilizada neste trabalho para dividir os fluxos de tráfego em dois grupos: ataque e não ataque, usando abordagem hierárquica divisiva e distância Euclidiana.

5. Resultados e Discussão

Neste trabalho, para a seleção dos discriminantes, aplicamos análise de variância. Este trabalho difere da referência [Zuev e Moore 2005] em pelo menos dois aspectos. Primeiro, estamos interessados em discriminar um único tipo de tráfego enquanto [Zuev e Moore 2005] tenta obter uma classificação mais ampla em dez categorias diferentes (tabela 1). Segundo, utilizamos um método mais simples na seleção dos discriminantes. Em [Zuev e Moore 2005], os autores usam o método Naïve Bayes para a seleção dos discriminantes. Nosso método consiste na seleção independente baseado na distribuição F. A partir do *trace* classificado, cada variável é examinada individualmente e independentemente e sua importância é analisada a partir dos valores da distribuição F. Por último, nós usamos um número reduzido de variáveis em comparação a [Zuev e Moore 2005].

A seleção dos discriminantes foi baseada nas variáveis que apresentaram grandes valores para a distribuição F. A tabela 3 apresenta as doze variáveis candidatas a discriminante baseado nos grandes valores da distribuição F.

Tabela 3. Variáveis candidatas a discriminantes

Número da Variável	Variável Candidata
1	Porta do Servidor
2	Número Mínimo do Total de Bytes em um Pacote IP *cliente para servidor*
3	Tamanho Máximo da Janela de Anúncio *cliente para servidor*
4	Média dos Bytes de Controle no Pacote *cliente para servidor*
5	Média do Tamanho do Segmento *servidor para cliente*
6	Tamanho Máximo da Janela de Anúncio *servidor para cliente*
7	Mediana dos Bytes de Dados IP *cliente para servidor*
8	Pacotes de Dados Atuais *cliente para servidor*
9	Tamanho Mínimo da Janela de Anúncio *servidor para cliente*
10	Variância dos Bytes de Dados *servidor para cliente*
11	Variância dos Bytes de Controle no Pacote *cliente para servidor*
12	Tamanho Máximo do Segmento *cliente para servidor*

Entre as doze variáveis listadas na tabela, algumas delas expressam informações redundantes. Como citado anteriormente na seção 4.1, as variáveis com valores da distribuição F mais significativos estão relacionadas às variáveis mais importantes para a discriminação dos grupos. Foram, portanto, selecionadas cinco variáveis que melhor explicavam o comportamento conhecido dos ataques. Estas variáveis são: Tamanho Máximo do Segmento *cliente para servidor* (D1), Tamanho Mínimo da Janela de Anúncio *servidor para cliente* (D2), Número Mínimo do Total de Bytes em um Pacote IP *cliente para servidor* (D3), Média dos Bytes de Controle no Pacote *cliente para servidor* (D4), Variância dos Bytes de Controle no Pacote *cliente para servidor* (D5).

Utilizando os cinco discriminantes descritos acima, agrupamentos de fluxos foram gerados utilizando técnicas hierárquicas e distância Euclidiana. A qualidade da separação dos fluxos em agrupamentos de ataque e não ataque está diretamente relacionada com os resultados do trabalho proposto. Para tanto, foram utilizados os seguintes parâmetros: *exatidão média*, *exatidão média de ataque* e *confiança.*

Os termos *exatidão média*, *exatidão média de ataque* e *confiança* são definidos a seguir:

$$\textit{Exatidão Média} = \frac{\text{nº de fluxos corretamente classificados nos } \textit{clusters}}{\text{total de fluxos do } \textit{trace}} \quad (5)$$

$$\textit{Exatidão Média de Ataque} = \frac{\text{nº de fluxos de ataques corretamente classificados nos } \textit{clusters}}{\text{total de fluxos de ataques no } \textit{trace}} \quad (6)$$

$$\textit{Confiança} = \frac{\text{nº de fluxos corretamente classificados nos } \textit{clusters} \text{ de ataque}}{\text{total de fluxos nos } \textit{clusters} \text{ de ataque}} \quad (7)$$

As tabelas 4, 5 e 6 mostram respectivamente a confiança, a exatidão média de identificação e a exatidão média na identificação de ataques usando as variáveis discriminantes D1, D2, D3, D4 e D5. O campo D1-5 representa as cinco variáveis

analisadas em conjunto. Foram utilizados os dez *traces* descritos na seção 3 aplicando-se os cinco discriminantes escolhidos.

As figuras 1, 2 e 3 foram construídas a partir dos dados dessas tabelas e ilustram o poder de separação dos cinco discriminantes selecionados e a variabilidade média entre os *traces* obtidos, usando como medida, respectivamente, a confiança média de identificação, a exatidão média de identificação e a exatidão média de identificação de ataques. Essa variabilidade é mostrada pelos valores máximos e mínimos de cada discriminante.

Tabela 4. Confiança por *trace* e por discriminante

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
D1	94,79	100,00	50,00	99,63	85,93	94,21	100,00	87,06	98,99	98,21
D2	100,00	64,29	93,75	100,00	99,17	96,95	100,00	100,00	96,49	90,07
D3	100,00	0,00	0,00	100,00	0,00	0,00	0,00	80,38	95,55	60,43
D4	88,80	100,00	58,33	100,00	92,04	95,28	83,33	80,25	95,28	98,99
D5	92,08	100,00	70,00	100,00	84,62	93,18	87,04	82,12	95,53	98,73
D1-5	85,51	80,00	76,19	100,00	97,50	96,85	100,00	80,89	95,30	100,00

Tabela 5. Exatidão média de identificação por *trace* e por discriminante

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
D1	96,40	98,20	95,90	94,20	97,50	97,30	91,90	93,40	92,30	87,70
D2	98,30	98,50	97,30	99,90	99,70	98,90	96,80	99,20	95,10	91,70
D3	88,30	98,10	95,90	100,00	86,00	81,70	91,10	96,70	98,10	70,80
D4	97,50	98,50	96,10	99,80	97,30	98,10	94,70	96,60	97,80	94,30
D5	96,30	98,20	96,30	99,80	96,80	98,00	95,10	96,80	97,90	93,70
D1-5	97,60	98,40	97,00	100,00	99,20	98,50	94,40	96,80	98,00	72,00

Tabela 6. Exatidão média na identificação de ataques por trace e por discriminante

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
D1	74,59	5,26	4,88	82,41	95,08	85,07	8,99	57,36	79,84	73,77
D2	86,07	47,37	36,59	99,69	98,36	94,78	64,04	93,80	89,92	91,48
D3	4,10	0,00	0,00	100,00	0,00	0,00	0,00	98,45	99,46	100,00
D4	90,98	21,05	17,07	99,38	85,25	90,30	50,56	97,67	98,91	88,12
D5	76,23	5,26	17,07	99,38	90,16	91,79	52,81	96,12	98,91	87,00
D1-5	96,72	21,05	39,02	100,00	95,90	91,79	37,08	98,45	99,46	37,22

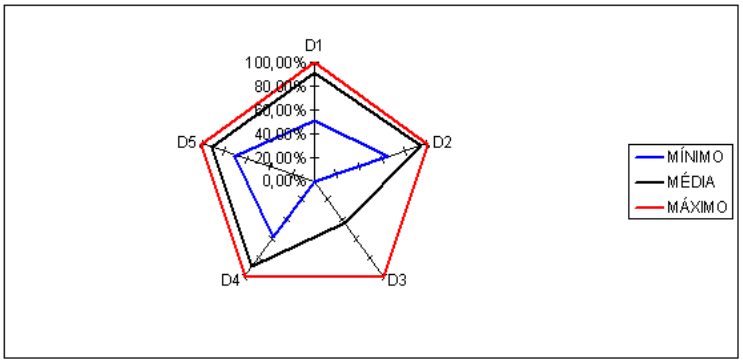

Figura 1. Gráfico de Kiviat para a confiança média na identificação

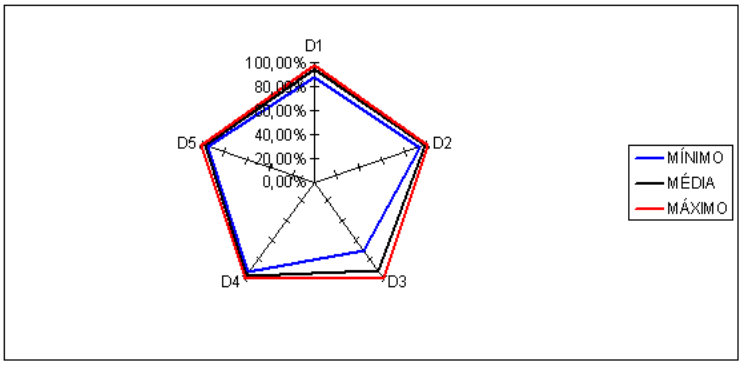

Figura 2. Gráfico de Kiviat para a exatidão média na identificação

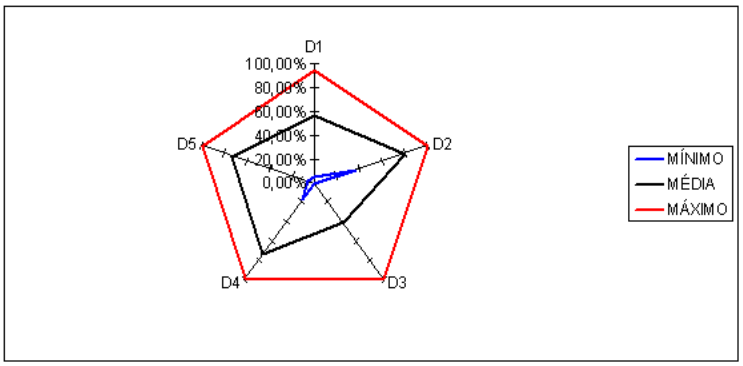

Figura 3. Gráfico de Kiviat para a exatidão média na identificação de ataques

Uma forma diferente e visualmente mais intuitiva de analisar os dados é através do gráfico de Kiviat mostrado nas figuras 1, 2 e 3. Num gráfico de Kiviat eixos radiais eqüidistantes representam as dimensões consideradas para análise. Neste, cada eixo representa um discriminante. Em cada eixo são marcados os valores mínimos, médios e máximos, e estes pontos são ligados. A figura assim constituída dá uma idéia visual do poder de separação de cada discriminante. Nessas figuras, a linha cheia central representa os valores médios e as linhas interna e externa representam os valores mínimos e máximos, respectivamente.

A tabela 7 a seguir apresenta os resultados para exatidão média e confiança, em comparação com os mesmos resultados obtidos em [Zuev e Moore 2005]. Nesta tabela aparecem as seguintes abreviações: NB para *Naïve Bayes*, FCBF para *Fast Correlation-based Filter* e Kernel para *Kernel Density Estimation*. A última linha, *Cluster*(5) mostra os resultados deste trabalho.

Tabela 7. Exatidão média e confiança dos métodos

Método	Exatidão Média (%)	Confiança (%)
NB	65,26	1,10
NB + Kernel	93,50	8,52
FCBF + NB	94,29	10,38
FCBF + NB + Kernel	96,29	13,46
Cluster (5)	95,19	91,22

Em [Zuev e Moore 2005] é aplicada a técnica Naïve Bayes aos dados coletados e descritos na seção 3 para categorizar o tráfego Internet em dez classes distintas de aplicações como apresentado na tabela 1. Em nosso trabalho aplicamos aos mesmos dados utilizados em [Zuev e Moore 2005] a distribuição F para selecionar as variáveis que melhor identificam um tráfego de ataque e, a partir daí, utilizamos a técnica de análise de agrupamento para separar em grupos os fluxos de ataque e não ataque.

Ressalte-se que entre os cinco discriminantes selecionados pelo método deste trabalho, três deles não coincidem com aqueles utilizados em [Zuev e Moore 2005]. Este fato aliado ao objetivo de selecionar um só tipo de aplicação explica os resultados alcançados notadamente melhores.

Como pode ser observado na tabela 7, o melhor resultado obtido em [Zuev e Moore 2005] foi de 13,46% de confiança para identificação de tráfego de ataque e 96,29% de exatidão média de identificação. Por outro lado, a seleção de discriminantes e a técnica de agrupamento aplicados neste trabalho resultaram em uma confiança de 91,22% para identificação de tráfego de ataque e uma exatidão média de identificação de 95,19%. Ou seja, em conclusão, pode-se ver que apesar da exatidão média de identificação ter aproximadamente o mesmo valor, a confiança na identificação de tráfego de ataque praticamente multiplicou por seis, atingindo um percentual viável de aplicação prática.

6. Conclusões

A caracterização do tráfego de uma rede é um ponto importante a ser abordado no projeto de rede. Para estudar a influência dos ataques em uma rede e o desempenho dos servidores, a primeira etapa consiste em identificar a quantidade de tráfego de ataque presente na carga de trabalho da rede. A abordagem apresentada usa um reduzido número de discriminantes estatísticos e análise de agrupamento para identificar a componente de ataque presente no tráfego da rede.

Identificação de tráfego de ataque é uma tarefa para a qual a taxa de sucessos atual está entre as mais baixas.

Este trabalho apresentou uma metodologia para identificação de tráfego de ataques, baseada na seleção de variáveis discriminantes e posterior identificação dos fluxos. Os resultados encontrados mostram que a metodologia utilizada é superior à principal referência utilizada no desenvolvimento de nosso trabalho. O melhor resultado

obtido em [Zuev e Moore 2005] foi 13,46% de confiança para identificação de ataques e 96,29% de exatidão média de identificação. Em comparação, os resultados deste trabalho alcançam 91,22% de confiança para identificação de ataques e 95,19% de exatidão média de identificação.

Esta é uma pesquisa em andamento. Como continuidade, estamos planejando aplicar a metodologia apresentada neste trabalho a *traces* próprios, coletados em dois ISPs. Também está em andamento a sua aplicação para a identificação de outras classes de tráfego, especificamente, tráfego P2P.

Paralelamente a identificação dos componentes de tráfego, estamos trabalhando na caracterização da carga de trabalho gerada por cada uma dessas componentes.

Referências

Anderson, T. W. (1958). An Introduction to Multivariate Statistical Analysis. Ed. John Wiley Sons, NY.

Auld T. et al. (2007). Bayesian Neural Networks for Internet Traffic Classification. IEEE Transactions on Neural Networks.

Barford, P., Kline, J., Plonka, D., and Ron, A. (2002). A signal analysis of network traffic anomalies. In Internet Measurement Workshop.

Brutlag, J. (2000). Aberrant behavior detection in timeseries for network monitoring. In USENIX LISA.

Hussain, A., Heidemann, J., and Papadopoulos, C. (2003). A Framework for Classifying Denial of Service Attacks. In ACM SIGCOMM, Karlsruhe.

Jain, R. (1991). The Art of Computer Systems Performance Analysis. In John Wiley Sons, Inc.

Johnson, D. (1998). Applied Multivariate Methods for Data Analysis. In Brooks/Cole Publishing Co.

Jung, J., Krishnamurthy, B. and Rabinovich, M. (2002). Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites. In Proceedings of ACM WWW.

Jung, J., Paxson, V., Berger, A., and Balakrishnan, H. (2004). Fast Portscan Detection Using Sequential Hypothesis Testing. In IEEE Symposium on Security and Privacy.

Kaufman, L. and Rousseeuw, P. (1990). Finding Groups in Data: An Introduction to Cluster Analysis. In Wiley and Sons, Inc.

Kim, H. A. and Karp B. (2004). Autograph: Toward Automated, Distributed Worm Signature Detection. In Usenix Security Symposium, San Diego.

Kim, M. S., Kang, H. J., Hung, S. C., Chung, S. H., and Hong, J. W. (2004). A Flow-based Method for Abnormal Network Traffic Detection. In IEEE/IFIP Network Operations and Management Symposium, Seoul.

Lakhina, A., Crovella, M., and Diot, C. (2004a). Characterization of Network-Wide Anomalies in Traffic Flows. Technical Report BUCS-2004-020, Boston University.

Lakhina, A., Crovella, M., and Diot, C. (2004b). Diagnosing Network-Wide Traffic Anomalies. In ACM SIGCOMM, Portland.

Lakhina, A., Crovella, M., and Diot, C. (2005). Mining anomalies using traffic feature distributions. In Proceedings of ACM SIGCOMM.

Menascé, D. and Almeida, V. (2002). Capacity Planning for Web Services. In Prentice Hall, New Jersey.

Mingoti, S. A. (2005). Análise de Dados através de Métodos de Estatística Multivariada: Uma Abordagem Aplicada. Ed.UFMG, Belo Horizonte, Brasil.

MOORE A. et al. (2003). Architecture of a Network Monitor. In Passive & Active Measurement Workshop (PAM).

Moore, A., Zuev, D., and Crogan, M. (2005). Discriminators for use in flow-based classification. RR-05.13 Department of Computer Science, University of London.

Moore, A. and Papagiannaki, K. (2005). Toward the Accurate Identification of Network Applications, In Proceedings of the Sixth Passive and Active Measurement Workshop (PAM), volume 3431, Springer-Verlag LNCS.

Portnoy, L., Eskin, E., and Stolfo, S. (2001). Intrusion detection with unlabeled data using clustering. In ACM Workshop on Data Mining Applied to Security (DMSA).

Roughan, M., Grif_n, T., Mao, Z. M., Greenberg, A., and Freeman, B. (2004). Combining Routing and Traffic Data for Detection of IP Forwarding Anomalies. In ACM SIGCOMM NeTs Workshop, Portland.

Schechter, S., Jung, J., and Berger, A. (2004). Fast Detection of Scanning Worm Infections. In Seventh International Symposium on Recent Advances in Intrusion Detection (RAID), Sophia Antipolis, France.

Taylor, C. and Alves-Foss, J. (2000). Low Cost Network Intrusion Detection.

Taylor, C. and Alves-Foss, J. (2001). NATE: Network Analysis of Anomalous Traffic Events. In Proceedings New Security Paradigms Workshop.

Thottan, M. and Ji., C. (2003). Anomaly Detection in IP Networks. In IEEE Trans. Signal Processing (Special issue of Signal Processing in Networking), pages 2191.2204.

Zuev, D. and Moore, A. (2005). Internet Traffic Classification using Bayesian Analysis Techniques. ACM SIGMETRICS, Alberta, Canada.