Um Modelo de Composição de Detectores de Intrusão Heterogêneos Baseado em Conjuntos Difusos

Inez Freire Raguenet, Carlos Maziero

Programa de Pós-Graduação em Informática Aplicada
Pontifícia Universidade Católica do Paraná (PPGIA – PUCPR)

inez.raguenet@pucpr.br, maziero@ppgia.pucpr.br

Resumo. *A capacidade de detecção de um IDS depende de diversos fatores, incluindo sua arquitetura interna e os algoritmos utilizados. Assim, detectores distintos poderão apresentar comportamentos distintos quando submetidos ao mesmo fluxo de eventos. A teoria de diversidade de projetos vem sendo usada com sucesso na área de tolerância a faltas e também pode trazer benefícios na área de detecção de intrusão. O objetivo deste artigo é propor uma modelagem matemática baseada na teoria de conjuntos difusos para a composição de detectores de intrusão heterogêneos que analisam o mesmo fluxo de eventos. Com esse modelo, busca-se combinar os resultados individuais de cada detector em um resultado global de melhor qualidade.*

Abstract: *The performance of an intrusion detector depends on several factors, like its internal architecture and the algorithms employed. Thus, distinct detectors can behave distinctly when submitted to the same event flow. The project diversity theory has been successfully used in the fault tolerance domain, and can bring benefits to the intrusion detection area. The objective of this paper is to propose a mathematical model, based on the fuzzy set theory, for the composition of heterogeneous intrusion detectors analyzing the same event flow. This model intends to combine the individual detectors' results into a global result with better quality.*

1. Introdução

Na maioria das instalações onde é necessário controlar e detectar o acesso indevido aos recursos de um sistema opta-se, por razões práticas, pela utilização de um único programa de detecção de intrusão (IDS). Em poucos casos se vê o uso de mais de um IDS; onde isto ocorre, normalmente se faz a replicação do mesmo detector em posições estratégicas de uma rede.

Entende-se que a opção de se replicar o uso do mesmo IDS se deve à dificuldade operacional de implantar programas diferentes e também à dificuldade de consolidar resultados gerados por IDSs diferentes. Por outro lado, o uso de réplicas do mesmo detector pode gerar resultados tendenciosos, pois o detector escolhido pode ter falhas que o levem a gerar alarmes falsos (os chamados "falsos positivos") ou ignorar ataques conhecidos (os chamados "falsos negativos").

Pode-se constatar, também, que o conceito de diversidade de projetos [Azivienis 1984], pelas diversas vantagens já demonstradas na área de tolerância a faltas e mesmo

de segurança [Littlewood 2004], também pode ser aplicado à área de detecção de intrusão. Percebe-se que a capacidade de detecção de um IDS depende de diversos fatores, incluindo sua arquitetura interna e os algoritmos utilizados [Maxion 2005]. Assim, detectores distintos poderão apresentar comportamentos distintos quando submetidos ao mesmo fluxo de eventos. Ao aplicar os conceitos de diversidade de projetos em detecção de intrusão, busca-se obter um sistema de detecção composto por detectores individuais que não apresentem as mesmas falhas de projeto ou de funcionamento, e cujos resultados se complementem.

A proposta do trabalho aqui descrito é a de apresentar um modelo matemático, fundamentado na Teoria dos Conjuntos, que possibilite a combinação dos resultados de um conjunto de detectores individuais heterogêneos, construindo assim um *detector de intrusão composto* (CIDS – *Compound Intrusion Detection System*) baseado no conceito de diversidade de projetos. Este modelo deve ser capaz de mapear e tratar os resultados dos detectores individuais, gerando um resultado consolidado de melhor qualidade que os detectores isolados.

Este artigo se divide da seguinte forma: a seção 2 apresenta o conceito de CIDS; na seção 3 são apresentados os objetos do estudo e algumas definições; na seção 4 são apresentados os modelos de combinação baseados na teoria dos conjuntos tradicional para dois ou mais detectores; na seção 5 o modelo é estendido para a teoria de conjuntos difusos e é introduzido o conceito de *grau de importância* de um ataque; a seção 6 apresenta resultados experimentais para validar o modelo proposto; finalmente, a seção 7 conclui o artigo e propõe algumas perspectivas de continuidade do trabalho.

2. Composição de Detectores de Intrusão

Tradicionalmente, a composição de detectores de intrusão tem sido feita visando cobrir um sistema distribuído amplo, cujo alcance estaria além da capacidade de detectores individuais. Essa abordagem, denominada *Distributed IDS*, consiste basicamente em espalhar detectores em vários pontos do sistema, cada um analisando os eventos gerados pelo(s) sistema(s) sob sua responsabilidade. Como o volume de alarmes gerado por essa abordagem pode ser imenso, foram propostas representações padronizadas dos alarmes gerados pelos sensores [Carey 2002], mecanismos para a configuração centralizada dos mesmos [Kreibich 2005] e técnicas de correlação dos alarmes oriundos dos vários sensores, visando fornecer visões consolidadas das intrusões [Dain 2001, Cuppens 2002, Julish 2003].

Outra possibilidade de composição de detectores é demonstrada por [Bachi 2003], que apresenta o *Collaborative Intrusion Detection System*, uma agregação de detectores em três níveis diferentes (rede, *kernel* e aplicação), munido de componentes adicionais que auxiliam na tarefa da consolidação dos resultados individuais. A composição de detectores complementares também é discutida em [Ko 2000].

Estudos recentes mostram que detectores diferentes possuem capacidades de detecção diferentes, muitas vezes complementares. Por exemplo, o artigo [Maxion 2005] mostra que algoritmos de detecção baseados em anomalias podem ter “pontos cegos” e propõe uma solução para IDSs compostos baseada na diversidade de algoritmos.

Mais recentemente, outras preocupações na avaliação dos IDSs surgiram voltadas para obtenção de resultados comparativos de desempenho e de custos de implementação. Em [Mell et al 2003], os autores se preocupam com a *precisão* dos IDSs, um conceito que envolve a quantidade de ataques que o IDS é capaz de detectar, a probabilidade de geração de alarmes falsos comparada com a probabilidade de detecção de ataques, a robustez do IDS contra ataques direcionados ao host onde ele é executado, a escalabilidade do IDS em relação ao tráfego, a habilidade de correlacionar eventos e, enfim, a habilidade de detectar novos ataques até então desconhecidos. Em [Ulvila et al 2003], os IDSs compostos são avaliados através da montagem de uma árvore de decisão dos *custos esperados*; neste estudo, são analisadas implementações de dois ou mais IDSs, em combinações paralelas e seqüenciais, tendo como preocupação final decidir a combinação que traz o menor custo e o melhor resultado.

Nas próximas seções será desenvolvido um modelo matemático que visa compor os resultados de *n* detectores de intrusão distintos analisando simultaneamente o mesmo fluxo de eventos. Deve ficar claro que cada detector é visto como uma caixa-preta, portanto sua arquitetura e seus algoritmos internos não são considerados na composição. A Figura 1 ilustra a visão "caixa preta" considerada neste trabalho. Nesse modelo genérico, os eventos de entrada podem ser o fluxo de pacotes em um segmento de rede, a seqüência de chamadas de sistema geradas por uma aplicação, os arquivos de *log* de um sistema operacional, etc. Por sua vez, a *base de conhecimento* contém regras descrevendo os ataques conhecidos (para detectores baseados em assinatura) ou os parâmetros que definem o estado normal do sistema (para detectores baseados em anomalia). O detector em si aplica as regras da base de conhecimento sobre os eventos de entrada e gera alarmes na saída conforme a necessidade.

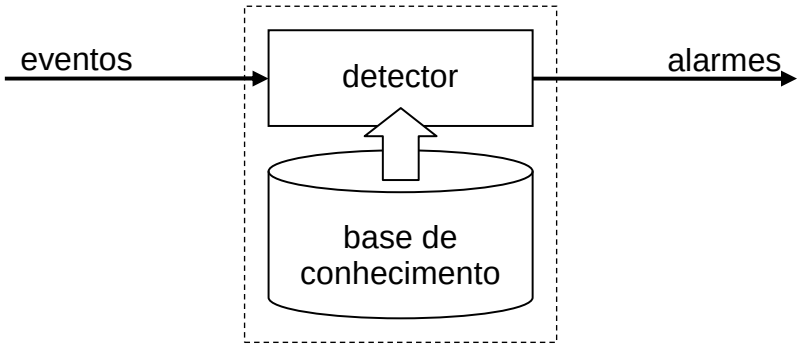

Figura 1 – Modelo genérico de detector de intrusão

3. Definições

Nesta seção serão definidos alguns termos-chave usados no decorrer do texto. Dentre estes termos estão, por exemplo, as definições de *eventos* e *ataques*. Como o modelo proposto é baseado nas teorias de conjuntos tradicionais e difusos, também serão definidos formalmente os conjuntos usados na modelagem.

- **Evento** – qualquer ação que ocorra entre dois hosts ou entre um host e um operador, que pressuponha uma interação entre ambos e que possa ser registrada por um detector.

- **Ataques** - eventos identificados e classificados por um detector como um acesso que represente uma seqüência de ações com o objetivo de se aproveitar de alguma vulnerabilidade do sistema.
- **Eventos Normais –** eventos não classificados como ataques pelo detector.
- **Conjunto Universo (U)** – conjunto que compreende todos os eventos possíveis de serem encontrados em qualquer sistema. A princípio, todo tipo de acesso ou operação em um sistema informatizado faz parte do conjunto U.
- **Conjunto de Eventos Normais (N)** – conjunto que compreende os eventos esperados, pressupostos, aceitos e para os quais um sistema está preparado para responder.
- **Conjunto de Eventos Direcionados ao Sistema (T) –** compreende todos os eventos direcionados a um sistema, dentre eles os acessos normais (esperados pelo sistema), os anômalos (classificados como ataques pelos detectores) e os não detectados pelos detectores.
- **Conjunto de Eventos Detectados por um Detector (D) –** compreende todos os eventos detectados por um detector ativado em um sistema.
- **Sistema de Detectores Compostos (IDS-Composto, CIDS) –** sistema onde existe mais de um detector operando na detecção de intrusão. O resultado final de um CIDS resultará da composição dos resultados obtidos por cada um dos detectores individualmente.

4. Modelagem da Composição

A abordagem matemática seguida neste artigo baseia-se, a princípio, na Teoria dos Conjuntos Tradicional. A intenção desta modelagem é a de tornar possível apontar qualitativamente cada subconjunto de objetos envolvidos no funcionamento de um IDS. Os conjuntos definidos na seção anterior foram selecionados dentre as possibilidades de conjuntos inerentes ao funcionamento de um IDS; seus relacionamentos serão representados nos diagramas a seguir. Uma única abordagem semelhante foi proposta em [Leckie 2002], mas essa se restringe a retratar somente um detector, enquanto a modelagem aqui proposta aqui admite extensão para *n* detectores.

A primeira modelagem, ilustrada na Figura 2, mostra um sistema munido de somente um detector. Neste diagrama, todos os conjuntos definidos na seção anterior serão identificados pelas letras: U – o conjunto de todos os eventos possíveis no sistema; N – o conjunto de eventos normais, ou seja, aqueles esperados pelo sistema; T – o conjunto de eventos direcionados ao sistema; D_1 – o conjunto de eventos detectados pelo detector IDS_1 . Também são identificados alguns subconjuntos de interesse.

No diagrama da Figura 2, é possível identificar:

- em (1), o subconjunto de D_1 que contém os eventos normais observados pelo detector IDS_1 ($D_1 \cap N$);
- em (2), o subconjunto de D_1 que contém os ataques detectados pelo detector IDS_1 ($D_1 – N$);

- em (3), o subconjunto de T que contém os eventos direcionados ao sistema que não foram percebidos pelo detector IDS_1 (T – D1); neste conjunto estão incluídos os falsos negativos (T – D1)-N.

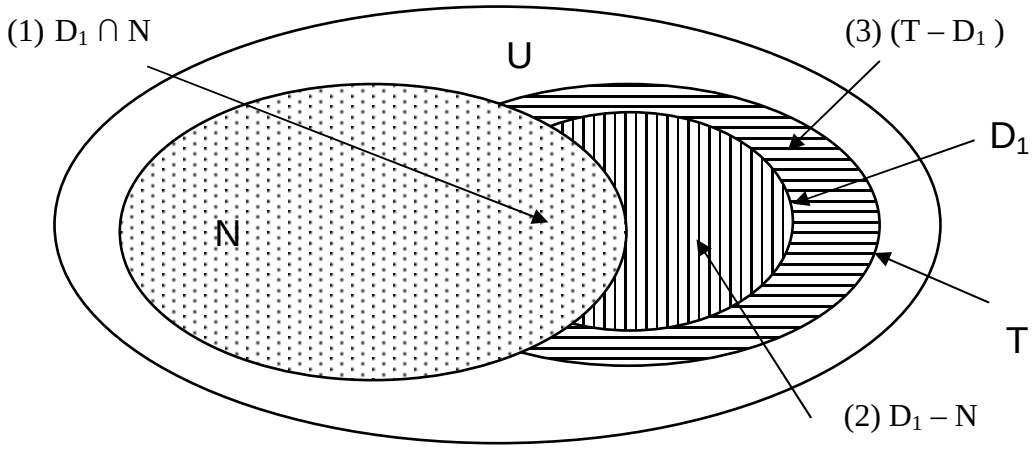

Figura 2 – Diagrama de Venn para Modelagem com um Detector

Com o intuito de facilitar as representações gráficas, o modelo será estendido para somente 2 detectores, IDS_1 e IDS_2, como está ilustrado na Figura 3. Neste diagrama, o conjunto de eventos detectados pelo detector IDS_1 será identificado pelo conjunto D_1, enquanto que o conjunto de eventos detectados pelo detector IDS_2 será identificado pelo conjunto D_2.

O conjunto final da detecção do CIDS pode ser obtido de duas maneiras: na primeira, mais restritiva, são considerados os ataques comuns, detectados por ambos IDSs; na segunda, mais abrangente, são considerados todos os ataques detectados por cada um dos IDSs.

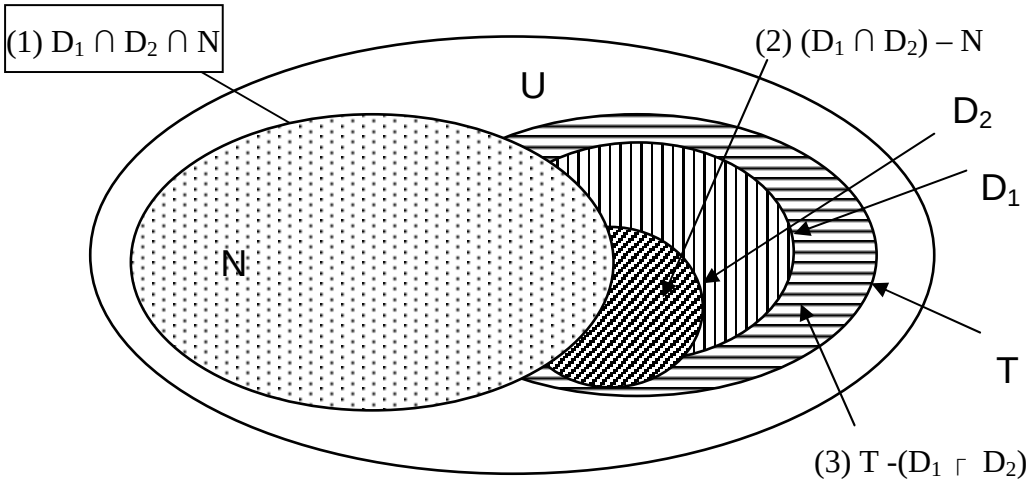

Figura 3 - Modelagem com Dois Detectores

Na interpretação mais restritiva, o conjunto de resultados do CIDS será dado pela interseção dos conjuntos de resultados dos IDSs individuais :

- em (1), os eventos normais observados por ambos ($D_1 \cap D_2 \cap N$);
- em (2), os ataques detectados por ambos (($D_1 \cap D_2$) – N);
- em (3), os ataques não detectados por nenhum dos IDSs (T - (D1 $\cup$ D2))

Esta abordagem é mais restritiva pois considera como ataques somente os eventos detectados por ambos IDSs. Por um lado, visa diminuir os falsos positivos; por outro lado, corre o risco de descartar eventos importantes que porventura tenham sido detectados por um IDS com maior capacidade de detecção de alguns ataques em particular.

A extensão para *n* detectores pode ser modelada da mesma forma: os eventos normais detectados pelo CIDS serão representado por $(\bigcap_{i=1}^{n} D_i) \cap N$ e os ataques detectados pelo CIDS serão representado por $(\bigcap_{i=1}^{n} D_i)$ - N.

Ao optar pela interseção de todos os conjuntos de detecção, o conjunto de resultados do CIDS $(\bigcap_{i=1}^{n} D_i)$ pode ser "menor" do que alguns dos conjuntos de resultados individuais (D_1, D_2, ..., D_n), já que os ataques que não tenham sido detectados por todos os IDSs serão desconsiderados. Para compensar este fato, já que entende-se que os ataques detectados individualmente não devem ser totalmente ignorados, será apresentada, na próxima seção, uma metodologia que permitirá atribuir um *grau de importância* a cada um dos eventos classificados como ataque por cada um dos componentes do CIDS. Desta maneira, todos os ataques detectados, mesmo aqueles que não estejam presentes em todos os conjuntos de detecção, terão um certo nível de importância na composição do resultado final.

Na segunda interpretação, o conjunto de resultados do CIDS será dado pela união dos conjuntos de resultados dos IDSs individuais. No caso do diagrama que representa os dois detectores, o conjunto final de eventos considerados como ataques será (($D_1 \cup D_2$) – N); para um modelo com *n* detectores, o conjunto final será dado pela união de todos os conjuntos de ataques detectados $(\bigcup_{i=1}^{n} D_i - N)$. Esta abordagem é mais abrangente pois considera os pontos fortes de todos os IDSs da composição, entretanto pode gerar um número maior de falsos positivos.

5. Atribuição do Grau de Importância

Como mencionado na seção anterior, a primeira interpretação do modelo para CIDS proposto neste artigo pode descaracterizar ataques importantes pelo fato destes ataques não terem sido percebidos por todos os detectores do CIDS; já a segunda interpretação considera uma quantidade maior de eventos, mas aumenta o grau de incerteza do sistema. Portanto, o modelo será adaptado para comportar um pouco de cada uma das considerações acima: da primeira, será aproveitada a maior precisão, da segunda, será aproveitada a maior abrangência. Para tanto, serão acrescentados ao modelo alguns conceitos da Teoria de Conjuntos Difusos, uma generalização da Teoria

dos Conjuntos. Com a "fuzzificação do modelo", ou seja, a transposição do modelo da teoria tradicional para a teoria difusa, as classificações individuais dos detectores serão reconsideradas sob o ponto de vista do entendimento coletivo (do conjunto de detectores) e os todos os ataques detectados terão algum tipo de validade no resultado final.

Para evitar o descarte de eventos classificados como ataques por somente alguns dos detectores, será introduzido o conceito de *grau de importância* do evento, uma medida que servirá para graduar a importância de um ataque de acordo com o número de IDSs que o detectam; eventos detectados por um número maior de IDSs terão um grau de importância maior no conjunto de detecção do CIDS, e vice-versa.

Para atribuir-se um valor numérico ao grau de importância de um ataque, será definida uma função denominada *função de presença*, $f_k(\boldsymbol{e})$. Esta função serve para identificar se um evento ***e*** está ou não presente no conjunto D_k de ataques detectados pelo detector IDS_k pertencente a um CIDS com *n* detectores. O somatório *S* de todos os valores da função de presença do evento ***e*** no CIDS será utilizado na composição final do grau de importância deste ataque. Sejam:

(i) D_k o conjunto de ataques detectados pelo detector IDS_k ,

(ii) ***e*** um evento classificado como ataque por algum dos *n* detectores que compõem o CIDS,

então a *função de presença* $f_k(\boldsymbol{e})$ pode ser definida como

$$f_k(e) = \begin{cases} 1, \text{se } e \in Dk, \\ 0 \text{ se } e \notin Dk \end{cases} \qquad (1)$$

Para produzir-se o conceito final de *importância do ataque* o modelo original será "fuzzificado", ou seja, adaptado à Teoria de Conjuntos difusos. Em resumo, na teoria de conjuntos difusos um elemento pode pertencer totalmente ou parcialmente a um conjunto difuso. Para definir "o quanto" um elemento pertence a um conjunto, deve ser estabelecida uma *função de grau de pertinência*. Esta função atribuirá, ao elemento ***e***, um valor numérico (um número real), entre 0 e 1, 0 indicando total ausência e 1 indicando total presença do elemento no conjunto difuso. Outra característica da Teoria de Conjuntos Difusos é a de que qualquer conjunto difuso pode ser totalmente definido pela sua função de grau de pertinência. Para então fazer a *fuzzificação* do modelo, devem ser definidos um conjunto difuso e uma função de grau de pertinência inerentes ao modelo original.

O conjunto difuso escolhido será chamado de "Importância" (I) e a função de grau de pertinência para um certo evento ***e*** (a função $\mu I(\boldsymbol{e})$) medirá o quanto o evento ***e*** é importante. Em outras palavras, $\mu I(\boldsymbol{e})$ medirá o grau de importância do evento ***e*** no contexto do CIDS. Para criar-se a função de grau de pertinência $\mu I(\boldsymbol{e})$, algumas condições foram estabelecidas:

(i) os parâmetros de construção da função serão: 1) a quantidade de IDSs que compõem o CIDS e 2) o conjunto dos valores possíveis para o grau de importância de um evento (os números reais entre 0 e 1);

(ii) deverá ser uma função exponencial crescente pois se deseja que o crescimento seja rápido nos primeiros termos e que seja possível estabilizar seu crescimento nos termos finais (tenha uma "tendência" para o valor máximo 1);

(iii) $\mu I(\boldsymbol{e})$ deverá valor mínimo zero, ou seja, deverá ser zero se o evento ***e*** não for detectado por nenhum dos IDSs do CIDS;

(iv) os valores produzidos pela função não devem ser absolutos, ou seja, o grau de importância de um evento ***e*** detectado pelo CIDS deve ser diretamente proporcional ao número de IDSs que o detectam e inversamente proporcional ao número total de IDSs que compõem o CIDS.

Em (2) é apresentada a forma genérica de uma função que obedece a (i), (ii) e (iii) estabelecidos acima e que será adaptada à *fuzzificação* do modelo:

$$f(x) = 1 - \left(\frac{1}{1+x} \right) \qquad (2)$$

Na adaptação, *x* será substituído pelo somatório das funções de presença $f_k(\boldsymbol{e})$ e as proporções direta e inversas citadas acima em (iv) serão aplicadas, produzindo-se a função de grau de pertinência $\mu I(\boldsymbol{e})$ apresentada em (3). Sendo $S = \sum_{k=1}^{n} f_k(e)$, então

$$\mu\, I(\boldsymbol{e}) = \left(1 - \left(\frac{1}{1+S} \right) \right) * \frac{S}{n} \qquad (3)$$

Na prática, esta *fuzzificação* do modelo foi feita visando possibilitar a criação de alguns pontos de decisão no CIDS:

(i) em um CIDS com *n* detectores, qual o número mínimo de detectores do CIDS que precisam acusar um ataque para que este ataque seja considerado "relevante" ?;

(ii) qual o número mínimo de detectores que devem compor um CIDS para que seja possível validar o resultado de um número fixo de detectores ?

Antes de responder as perguntas acima, é necessário quantificar a importância de cada ataque detectado, o que pode ser feito através da definição de uma *escala de importância*. Propõe-se estabelecer, de forma empírica, uma tabela de graus de importância de um ataque (Tabela 1).

Tabela 1 – Graus de Importância

$\mu\, I(\boldsymbol{e})$	**Grau de Importância**
de 0 a 0,25	baixa importância
de 0,26 a 0,44	merece atenção
de 0,45 a 0,84	relevante
de 0,85 a 1,0	muito relevante

A título de ilustração, com base na equação definida em (3) e nos valores da Tabela 1, elaborou-se a tabela dos graus de importância para eventos detectados em CIDS com até 6 detectores (Tabela 2).

Tabela 2 – Análise do Grau de Importância – CIDS com até 6 detectores

Número de IDS que detectaram o ataque	Número de IDS que compõem o CIDS					
	1	2	3	4	5	6
1	0,50	0,25	0,17	0,13	0,10	0,08
2	----	0,67	0,44	0,33	0,27	0,22
3	----	----	0,75	0,56	0,45	0,38
4	----	----	----	0,80	0,64	0,53
5	----	----	----	----	0,83	0,69
6	----	----	----	----	----	0,86

A análise das colunas da Tabela 2 mostra qual o número mínimo de IDSs que precisam detectar um ataque para que o CIDS seja alertado também: por exemplo, um CIDS composto por 3 detectores já levanta um alerta que "merece atenção" se os ataques forem percebidos por 2 dos seus detectores; se o CIDS for composto por 6 detectores, este mesmo alerta será levantado se 3 dos detectores perceberem o ataque.

A análise das linhas da Tabela 2 mostra a importância que é atribuída a um ataque de acordo com o número de alertas obtido no CIDS; por exemplo, ataques detectados por 3 detectores de um CIDS podem ser "relevantes" (se o CIDS tiver 4 IDSs) ou do tipo que "merecem atenção" (se o CIDS tiver 6 IDSs).

O gráfico da Figura 4, que mostra a variação do o grau de importância de um evento quando detectado por todos os detectores do CIDS, foi traçado para mostrar que a função de grau de pertinência comporta-se exponencialmente como esperado.

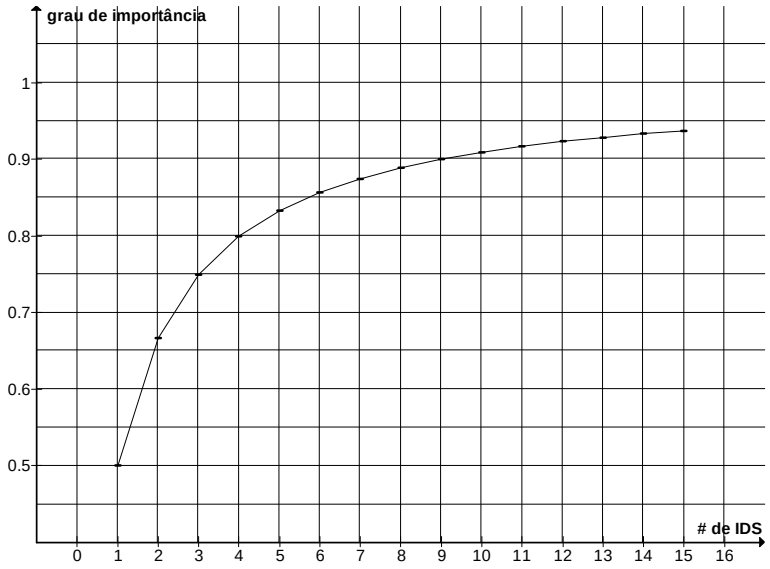

Figura 4 – Gráfico da variação do Grau de Importância de um ataque detectado por todos os detectores de um CIDS

A análise dos cálculos feitos até então permite tirar algumas conclusões preliminares:

(i) ataques detectados a partir de, aproximadamente, *n*/2 detectores em um CIDS com *n* detectores já devem merecer atenção;

(ii) CIDS compostos de 4 ou mais detectores já mostram resultados relevantes mesmo quando o ataque não é detectado por todos os IDSs;

(iii) somente a partir de 13 detectores é possível considerar um ataque "muito relevante" sem a necessidade de todos os detectores terem percebido o ataque;

6. Validação do Modelo Proposto

Dois experimentos foram montados para aplicar o modelo desenvolvido com vistas à sua validação. No primeiro, o CIDS contou com 5 detectores de intrusão distribuídos em 3 computadores, H1, H2 e H3, conectados a uma mesma rede local (Ethernet, 10 Mbps) através de um *hub*, analisando o mesmo tráfego de rede por cerca de 30 horas. No segundo experimento, o CIDS contou com os 2 detectores do computador H2 e executou o mesmo procedimento de análise durante 13 dias. A arquitetura de rede usada nos experimentos está apresentada na Figura 5. Em ambos os experimentos os detectores analisaram tráfego real originado na Internet e direcionado a dois servidores, um servidor IIS 5.0 (servidor web, habilitado no host H1, hospedando 4 domínios) e um servidor *Mail Enable* (de correio eletrônico, atendendo 4 domínios e 15 caixas-postais), este último instalado em um host no qual não foi ativado nenhum sensor.

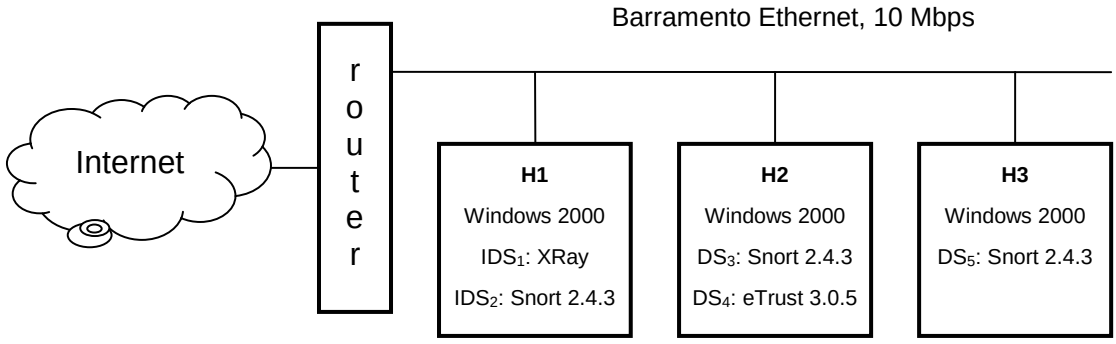

Figura 5 – O ambiente de rede usado nos experimentos

A configuração dos computadores é a seguinte:

- **H1**: Intel Pentium IV 2.0 GHz, 1 GB RAM, Windows 2000 Server, GroundZero XRay (detector IDS_1), Snort 2.4.3 build 26 (detector IDS_2), servidor Web IIS 5.0.
- **H2**: AMD Athlon 1,7 GHz, 512MB RAM, Windows 2000 Server, CA eTrust 3.0.5.55 (detector IDS_3) e Snort 2.4.3 build 26 (detector IDS_4) , nenhum outro serviço foi instalado.
- **H3**: Intel Pentium III 750 MHz, 384 MB RAM, Windows 2000 Server, Snort 2.4.3 build 26 (detector IDS_5), nenhum outro serviço foi instalado.

Experimento 1

Este experimento foi executado ao longo de dois dias; sua finalidade foi a de calcular o grau de importância de cada ataque identificado pelo CIDS. Ao todo foram detectados 35 ataques, identificados aqui pelo conjunto {A1, ... , A35}, assim classificados (Tabela 3):

Tabela 3- Distribuição dos Ataques Detectados no Experimento 1

	nome do ataque	IDS1	IDS2	IDS3	IDS4	IDS5
A1	code/command injection	x				
A2		x				
A3		x				
A4	exploit	x				
A5		x				
A6		x				
A7		x				
A8	http-inspect		x			
A9			x			
A10			x		x	
A11			x		x	x
A12			x		x	x
A13					x	x
A14					x	x
A15	WEB-CGI		x			
A16			x			
A17			x			
A18	Attack-Responses		x			
A19						x
A20					x	x
A21	Virus Outbound		x		x	
A22	WEB-MISC				x	x
A23						x
A24					x	x
A25						x
A26					x	x
A27					x	x
A28					x	x
A29					x	
A30					x	
A31	Port-Scan				x	x
A32	WEB-PHP				x	x
A33					x	x
A34	QUESO Scan			x		
A35				x		

Os graus de importância dos ataques detectados pelo CIDS estão na Tabela 4.

Tabela 4 – Graus de Importância dos Ataques do Experimento 1

20 eventos	0,10	baixa importância
13 eventos	0,27	merece atenção
2 eventos (A11 e A12)	0,45	relevante

Uma observação importante neste experimento é a de que a maior parte dos ataques registrados pelo CIDS foram direcionados ao host H1, no qual os detectores locais IDS_1 e IDS_2 não identificaram nenhum ataque em comum. Também se observou que o Snort, neste host, identificou o menor número de ataques dentre os Snorts em atividade (10 contra 17 do IDS_4 e 16 do IDS_5). Para esta última questão, a hipótese levantada aqui e que deverá ser analisada mais detalhadamente em estudos posteriores, é a de que, como alguns ataques visam alocar a total capacidade de processamento do computador atacado, o ataque em si inibe o funcionamento do detector, pelo menos temporariamente .

Experimento 2

Este experimento foi executado durante 13 dias, porém o CIDS só contou com o IDS_2 e IDS_3. Seu objetivo foi, inicialmente, a comprovação da modelagem proposta usando a Teoria dos Conjuntos. Ao final do experimento, foi possível comprovar a validade do diagrama da Figura 3; concluiu-se, também, que usar a somente os resultados incluídos na intersecção dos conjuntos de detecção restringe bastante o universo de resultados (neste experimento, o número de ataques detectados pelo IDS_3 é quase 10 vezes maior do que o número de ataque detectados por IDS_2). Os resultados do experimento foram os seguintes:

(i) D_2 = total de ataques detectados pelo IDS_2 (29 ataques de baixa importância)

(ii) D_3 = total de ataques detectados pelo IDS_3 (297 ataques de baixa importância)

(iii) $(D_2 \cup D_3) - N)$ = total de ataques detectados pelo CIDS – abordagem mais abrangente (396 ataques relevantes)

(iv) $((D_2 \cap D_3) - N)$ = total de ataques detectados pelo CIDS na abordagem mais restritiva (70 ataques relevantes)

Algumas observações dos resultados de ambos os experimentos:

(i) A metodologia usada para confrontar os resultados dos detectores e garantir que detectores diferentes detectaram um mesmo ataque foi a comparação do horário, endereço IP de origem e destino de cada ataque registrado por cada um dos detectores. Os relógios de todos os servidores foram sincronizados com uma fonte de horário externa, através do protocolo SNTP; todos os detectores receberam a última atualização disponível e detectores iguais foram configurados de forma idêntica.

(ii) Durante os experimentos, observou-se que detectores idênticos instalados em computadores com configuração de hardware e/ou software distintas reagem de forma distinta, ou seja, não detectam necessariamente os mesmos ataques. Isso provavelmente deve-se às características próprias do hardware e software de rede (sistema operacional) em cada máquina, fazendo com que, na prática, os detectores não recebam exatamente os mesmos eventos de entrada.

(iii) Caso fosse adotada a abordagem mais restritiva no Experimento 1, *nenhum* ataque seria considerado globalmente pelo CIDS, já que não houve consenso entre os 5 detectores;

(iv) O detector GroundZero XRay, apesar de ter algumas características de IDS de rede, é fundamentalmente um IDS de host (HIDS), enquanto o Snort é um IDS de rede (NIDS). No Experimento 1, nenhum dos ataques identificados pelo XRay (IDS_1) foi identificado pelos demais detectores; tal situação talvez possa ter sido gerada pela falta de ajuste "fino" das regras do Snort.

(v) No Experimento 1, dar-se-ia mais atenção aos dois ataques que obtiveram grau de importância 0,45. Um destes "ataques", porém, era um acesso legítimo ao serviço de *webmail* disponível na rede.

7. Conclusões e Trabalhos Futuros

A composição de detectores pode trazer um volume muito grande de resultados individuais. Este artigo propõe uma modelagem dos resultados possíveis de um CIDS tratando a composição de resultados de duas maneiras: na primeira, mais restritiva, são considerados os eventos comuns, detectados por todos os IDSs; na segunda, mais abrangente, são considerados todos os eventos detectados por cada um dos IDSs. Para quantificar a importância de um ataque detectado no CIDS, é proposta uma metodologia de cálculo do "grau de importância" de um evento. Os experimentos demonstraram que a diversidade de projetos é um fator importante na construção de CIDS pois traz resultados diversos, mesmo ao utilizar o mesmo IDS em hosts que difiram de alguma forma; mostraram também que a utilização de HIDS e NIDS na composição de resultados não é trivial e requer ajustes mais cuidadosos na montagem do CIDS.

Como trabalho futuro, pretende-se aprofundar a teoria matemática em uso para aplicá-la ao modelo com o intuito de ajustá-lo e talvez até possibilitar a eliminação de alguns eventos do CIDS, especialmente aqueles que se configuram como falsos positivos e falsos negativos. Pretende-se, também, tornar mais preciso o valor do grau de importância *global* (atribuído pelo CIDS) de um ataque; para tal, pretende-se possibilitar a atribuição de graus de importância individuais (pela interpretação individual de cada ataque detectado por cada um dos IDSs); esta precisão talvez possa ser alcançada, por exemplo, alterando, no cálculo da função de presença definida em (1), o valor fixo de $fk(e) = 1$ para $fk(e) = \alpha$ ($0 \leq \alpha \leq 1$), onde α seria um grau de importância atribuído pelo IDS individual ao evento.

Novos testes também deverão contemplar conjuntos controlados de ataques para que seja possível comparar os resultados do CIDS com os resultados dos IDSs individuais e finalmente atestar a validade da solução proposta.

Referências

Avizienis, A. and Kelly J. P. J. *Fault Tolerance by Design Diversity: Concepts and Experiments,*" IEEE Computer, pp. 67-80, August, 1984.

Axelsson, Stefan, *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection*. 6th ACM conference on Computer and Communications Security, 1999.

Bachi, S., Mei, Y., Foo B., Wu Y., *Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS*, Proceedings fo the 19th Annual Computer Security Applications Conference, 2003.

Carey N., Clark A., Mohay G. *IDS Interoperability and Correlation Using IDMEF and Commodity Systems*. Proceedings of the 4th International Conference on Information and Communications Security**,** December 2002.

Cuppens F., Miège A. *Alert Correlation in a Cooperative Intrusion Detection Framework*. IEEE Symposium on Security and Privacy, 2002.

Dain O., Cunningham R. *Fusing heterogeneous alert streams into scenarios*. 8th ACM Conference on Computer and Communications Security, 2001.

Julisch K. *Clustering intrusion detection alarms to support root cause analysis*. ACM Transactions on Information and System Security, November 2003.

Ko K., Fraser T., Badger L., Kilpatrick D. *Detecting and Countering System Intrusions Using Software Wrappers*. 9th USENIX Security Symposium, USA, 2000.

Kreibich C., Sommer R. *Policy-Controlled Event Management for Distributed Intrusion Detection*. 4th Intl Workshop on Distributed Event-Based Systems, June 2005.

Leckie, Tysen, *Bayesian Metrics for SEADS*, September 3, 2002, http://www.cs.fsu.edu/~yasinsac/group/slides/leckie3.pdf

Littlewood B. and Strigini L. *Redundancy and Diversity in Security*. 9th European Symposium on Research in Computer Security, France, 2004.

Maxion, R., Tan, K., *The Effects of Algorithmic Diversity on Anomaly Detector Performance*, Intl Conference on Dependable Systems & Networks, 01 – July – 2005.

Nguyen, Hung T. and Walker, Elbert A. *A First Course in Fuzzy Logic*, Chapman & Hall/CRC, 2000.

Mell, P., Hu, V., Lippmann, R., Haines, J., Zissman, M. *An Overview of Issues in Testing Intrusion Detection Systems*. National Institute of Standards and Technologie (NIST) Interagency Report 7007, June 2003.

Shaw, Ian S., Simões, Marcelo Godoy, *Controle e Modelagem Fuzzy*, Editora Edgard Blücher Ltda., 1999

Ulvila, Jacob W. and Gaffney, Jr., John E., *Evaluation of Intrusion Detection Systems*, Journal of Research of the National Institute of Standards and Technology, Volume 108, Number 6, November - December 2003.