Correlacionamento Distribuído de Alertas em Sistemas de Detecção de Intrusão

Thiago E Bezerra de Mello, Roberto A Hexsel

[1]Departamento de Informática, UFPR
Centro Politécnico - Curitiba, PR

thiago,roberto@inf.ufpr.br

Abstract. *As networks become faster intrusion detection systems must be able to cope with large amounts of data related to possible invasions, and generate alarms advising of potential network attacks. These alarms must be summarized prior to being analyzed by a human being. We present a parallel (distributed) alert correlation system that performs alarm correlation in two phases, local pre-processing and distributed post-processing. By splitting up the correlation system amongst several computers, each one might be smaller (and therefore cheaper) than would be necessary in a centralized system. We describe experiments performed to validate our design.*

Resumo. *Com o aumento da taxa de transmissão de dados em redes, os sistemas de detecção de intrusão processam muitas informações e podem gerar grandes volumes de evidências de tentativas de ataques, tornado-se necessário um sistema que produza, de forma resumida, evidências para análise por um humano. Nesse artigo descrevemos um sistema de correlacionamento distribuído de alertas, baseado em duas fases de correlacionamento, com pré-processamento local e pós-processamento distribuído. O sistema visa correlacionar alertas de forma paralela em uma rede de alta velocidade, através de sub-sistemas de correlacionamento que executam em computadores de menor custo do que aqueles que executam em sistemas centralizados. São descritos experimentos efetuados para a validação de conceito.*

Palavras Chave Detecção de Intrusão Distribuída, Correlacionamento de Alertas em Redes de Alta Velocidade, Correlacionamento Paralelo de Alertas.

1. Introdução

É cada vez maior a incidência de ataques explorando vulnerabilidades em sistemas computacionais, e todo sistema computacional conectado a uma rede é um alvo em potencial. Os *sistemas de detecção de intrusão* (SDI) são ferramentas automatizadas que auxiliam na detecção de tentativas de intrusão [CW01, Lai00]. Um SDI pode analisar o tráfego de uma rede, ou dados locais de uma máquina na qual é executado, à procura de tentativas de ataques com naturezas diversas. Um SDI que analisa tráfego de rede é chamado *Sistema de Detecção de Intrusão para Rede* (SDIR), e um SDI que analisa dados ou arquivos de registro locais em uma máquina é chamado de *Sistema de Detecção de Intrusão para Máquina* (SDIM). Um *Sistema Híbrido de Detecção de Intrusão* (SHDI) combina as

informações obtidas por um conjunto de SDIRs e SDIMs para melhorar a confiabilidade e diminuir o tempo necessário para a detecção de ataques.

Um SDIR examina o tráfego em um segmento, ou em toda uma rede. O tráfego é analisado através de uma interface de rede em modo promíscuo à procura de qualquer tipo de evidência de tentativa de ataque. Ao suspeitar de uma tentativa de ataque, o SDIR pode gerar um alerta com dados sobre o tipo do ataque, endereços IP da possível fonte e do alvo da tentativa, além da data e hora da tentativa. Uma fração dos alertas contém falso-positivos porque a suspeita é baseada em evidências de ataques que podem ser infundadas. O *Snort* é um SDIR projetado para efetuar análise de tráfego em tempo real e manter um registro de pacotes em redes IP. O Snort efetua análise de protocolos transportados nos pacotes IP para descobrir padrões de conteúdo, permitindo a detecção de vários tipos de ataques [Roe99, RG01].

Em uma rede de alta velocidade, um SDIR centralizado convencional pode ser incapaz de efetuar uma análise precisa dos dados que passam por ele porque a carga de processamento no SDIR é proporcional à intensidade do tráfego analisado. Note que o SDIR analisa o tráfego passivamente, e portanto não interfere com aquele, mas a confiabilidade da detecção pode ser comprometida em condições de tráfego intenso, se a capacidade de processamento for insuficiente para examinar o tráfego e computar as condições necessárias para gerar um alarme. Por conta disso, em redes de alta velocidade a detecção de intrusão pode ser realizada de forma paralela, através do particionamento de tráfego para que cada um de vários *sensores SDIR* analise apenas a fração do tráfego que é destinada à ele. Esta abordagem também é conhecida como “detecção de intrusão distribuída”.

Quanto maior a velocidade de transmissão da rede, potencialmente maior o número de tentativas de ataques, e portanto mais alertas são gerados. O número de alertas gerados pelo sistema de detecção de intrusão em uma rede (ou máquina) pode ser tão elevado que seja impossível aos administradores humanos tratar as informações e atuar em função de eventuais ameaças. Quanto maior o número de alertas, menor passa a ser a importância atribuída a cada um deles pelo administrador por conta da impossibilidade de verificação de cada alerta individualmente.

Para reduzir a quantidade de informação que deve ser tratada emprega-se o *correlacionamento de alertas* (ou de *eventos*), que permite ao administrador a extração eficiente de informações das tentativas de ataques. O correlacionamento de eventos é utilizado também na área de tolerância a falhas, gerenciamento de segurança e detecção de intrusão. Na detecção de intrusão a correlação é realizada através de alertas emitidos por SDIRs [DW01].

Um *SDIR baseado em correlacionamento distribuído de alertas* (SDI-CDA) consiste de um conjunto de pares *sensor-correlacionador*, uma base de dados e uma estação de gerência de rede. Cada par sensor-correlacionador avalia uma fração do tráfego da rede e todos os pares cooperam para a geração de alertas ao administrador da rede. No que se segue, o termo ‘sensor’ representa um par “sensor-correlacionador”.

Em uma rede de alta velocidade, um SDIR centralizado deve executar numa máquina com capacidade de processamento tal que lhe permita analisar todo o tráfego na rede. Tipicamente, a capacidade de processamento necessária para analisar tráfego da ordem de gigabytes por segundo só é disponível em máquinas de custo elevado. Por

outro lado, os sensores de um SDI-CDA podem executar em máquinas de menor custo, e o número de sensores pode ser escolhido em função da intensidade de tráfego e da precisão que se deseja na detecção de ataques. Assim, com um SDI-CDA pode-se obter tanta precisão na detecção de ataques quanto se deseja a um custo menor do que com um SDI centralizado.

Este artigo descreve um sistema distribuído de correlacionamento de alertas com sensores baseados no Snort. O SDI-CDA desenvolvido pelos autores permite ao administrador da rede definir, com grande flexibilidade, quais eventos, ou combinações de eventos, devem provocar a emissão de uma notificação ao operador. Por conta do talento e criatividade dos atacantes, são constantes as novidades em termos de tipos e táticas de ataque. A flexibilidade na configuração do SDI-CDA permite fácil adaptação aos novos padrões de ataque. Além disso, o sistema foi concebido para observar tráfego em redes de alta velocidade e portanto seu projeto enfatiza o desempenho na detecção de ataques, tanto por conta da intensidade de tráfego quanto do custo dos computadores em que o SDI-CDA executa.

O SDI-CDA é capaz de detectar ataques pela observação de tráfego na rede, e foi concebido e projetado para operar em redes de alta velocidade e com boa escalabilidade. O SDI-CDA poderia ser usado como um componente de um SHDI complexo como EMERALD [PN97, VS01], DOMINO [YBJ04], ou AASGARD [CWSR01]. Outra abordagem na detecção de ataques, especialmente ataques de negação de serviço (NdS), é a análise indireta do comportamento dos componentes de uma rede através de suas *Management Information Base*s (MIBs) [CQL$^+$01, Gib02, RMW02]. Componentes como roteadores e comutadores podem ser consultados periodicamente e alterações nos valores das variáveis de estado podem indicar que a rede esteja sob um ataque de negação de serviço. A observação das MIBs não implica na instalação de equipamentos dedicados à observação do tráfego, o que reduz o custo do sistema de detecção. O SDI-CDA descrito neste artigo é mais complexo porque envolve um número maior de componentes dedicados, porém permite a detecção de outras formas de ataque, além da NdS.

O texto está organizado da seguinte maneira. A Seção 2. discute o correlacionamento de alertas, e a Seção 3. descreve a arquitetura do SDI-CDA, e a Seção 4. descreve os experimentos efetuados para caracterizar o comportamento do SDI-CDA. Nossas considerações finais encontram-se na Seção 5..

2. Correlacionamento de Alertas

O administrador da rede deve ser capaz de analisar os alertas e deles extrair informações sobre a ameaça à segurança da rede. Para tanto, um sistema de correlacionamento de alertas agrega os dados contidos em vários alertas de forma a reduzir a quantidade de informações que deve ser avaliada pelo administrador.

O correlacionamento de eventos pode envolver uma ou mais dentre quatro técnicas: (i) compressão, (ii) priorização, (iii) generalização, e (iv) correlacionamento baseado em tempo [Vaa02] [HRTT03]. A técnica de *compressão de alertas* descarta várias ocorrências de um mesmo alerta. Na técnica de *correlacionamento por priorização* atribui-se prioridade aos alertas considerados mais importantes, e que portanto devem ser examinados com mais presteza. Na técnica de *correlacionamento por generalização* buscam-se alertas com uma ou mais características similares, agrupando-os em um só alerta. A

técnica de *correlacionamento baseado em tempo* procura associar eventos com uma tentativa de ataque que pode ocorrer em um dado intervalo ou período. Através de uma um mais destas técnicas é possível também descobrir alertas que sejam falsos-positivos. Existem outras formas de correlacionamento, tais como o sistema de correlacionamento de alertas baseado em probabilidades, descrito em [VS01].

Da mesma forma que para um SDIR centralizado que observa uma rede de alta velocidade, um sistema de correlacionamento de alertas necessita de grande capacidade computacional para relacionar um número elevado de alertas em tempo-real [CD01, DW01, CM02, MMDD02]. Os alertas gerados pelos sensores podem ser divididos entre sub-sistemas de correlacionamento, aumentando assim a capacidade agregada de correlacionar números elevados de alertas através de processamento paralelo. A eficiência do paralelismo depende de dois processos de correlacionamento, o *correlacionamento local* e o *correlacionamento distribuído* de alertas entre os sub-sistemas de correlacionamento. A correlação local de alertas é utilizada em ambientes comerciais tais como o sistema *RealSecure SiteProtector Fusion Module* da ISS [ISS99]. A *correlação distribuída de alertas* [dM04] é uma extensão do correlacionamento 'normal' de alertas e é descrita em detalhe na próxima seção.

3. Arquitetura do Sistema de Correlacionamento Distribuído

O sistema de correlacionamento distribuído SDI-CDA consiste de três componentes, que são (i) o espalhador de tráfego, (ii) os sensores e (iii) os correlacionadores de alertas, ou *Nariz*es. Estes componentes são descritos adiante. A Figura 1 mostra um SDI-CDA com um espalhador que divide o tráfego para três pares sensor-correlacionador. Cada sensor analisa sua parcela de tráfego e caso suspeite de tentativa de ataque, emite um alerta para o correlacionador a que está ligado. O correlacionador então compara o alerta recebido com alertas previamente armazenados em sua base local de alertas. Os três correlacionadores usam um canal de comunicação exclusivo, para efetuar o correlacionamento distribuído, e quando necessário, enviam alertas ao administrador da rede, e os armazenam numa base global de alertas.

Os *Nariz*es se comunicam através de um protocolo simples codificado com soquetes. O canal de comunicação exclusivo pode ser implementado com uma rede local disjunta da rede observada, ou as mensagens entre os *Nariz*es podem trafegar pela rede observada. Neste segundo caso, a segurança da comunicação entre os correlacionadores pode ser comprometida.

Espalhador Para que sensores de custo razoável sejam capazes de analisar o tráfego em redes de alta velocidade, o fluxo é dividido em "porções", e cada porção é analisada por um sensor ou por um conjunto de sensores. A divisão do tráfego é implementada no espalhador, por meio de distribuição circular de tráfego (*round robin*). O SDI-CDA utiliza o espalhador de tráfego descrito em [KVVK02]. No caso de tráfego TCP, cada porção de tráfego corresponde a uma sessão TCP, sendo portanto a distribuição baseada em conexões [ISS00]. No caso de tráfego UDP ou ICMP, a distribuição se dá pacote a pacote.

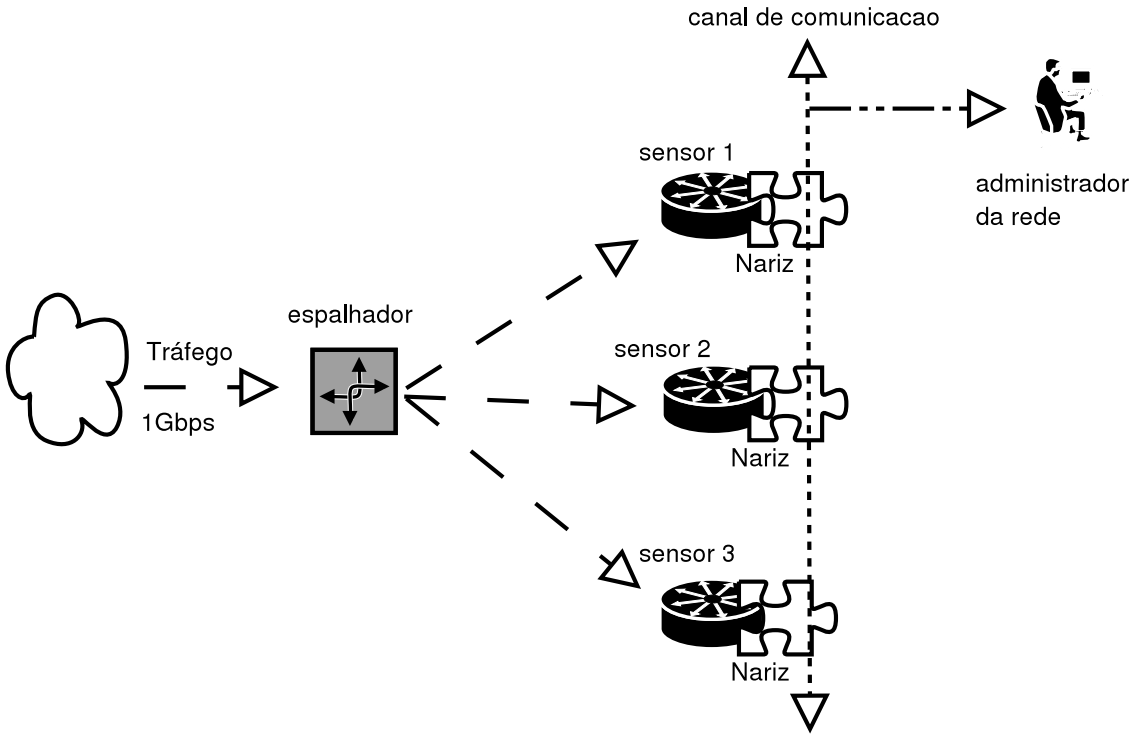

Figura 1. Arquitetura do sistema SDI-CDA

Sensores Os sensores utilizam o SDIR de domínio público Snort [Roe99, RG01]. O Snort pode emitir alertas de tentativas de ataques em tempo-real e em diversos formatos. Seu mecanismo de detecção utiliza uma arquitetura modular, possibilitando a incorporação de extensões, de pré-processadores de detecção, e de novas regras de detecção [SHM02]. As regras utilizadas pelo Snort permitem gerar alertas de tentativas de ataques, ou copiar os pacotes suspeitos para um arquivo de *log*, por exemplo. O SDI-CDA utiliza sensores autônomos para a detecção de intrusão, e cada sensor reporta seus alertas ao correlacionador a que está ligado.

Correlacionadores O sistema de correlacionamento de alertas no SDI-CDA é composto por três componentes: (i) correlacionamento de alertas local que é executado sobre os alertas gerados pelo sensor SDIR associado ao correlacionador, (ii) correlacionamento de alertas distribuído pela troca de mensagens entre os correlacionadores, e (iii) base central de alertas que é gerida pelo administrador da rede. O sistema possui regras simples de correlação de alertas emitidos por sensores, e os alertas não correlacionados são inseridos na base local como alertas novos. Os correlacionadores obtém os alertas dos sensores, correlacionam cada alerta localmente, e se comunicam para executar o correlacionamento distribuído. A troca de mensagens obedece um protocolo simples implementado sobre soquetes, e as mensagens são difundidas para todos os correlacionadores que compõem o SDI-CDA.

Base de Alertas Para armazenar os alertas é utilizado o banco de dados de domínio público *SQLite* [SQL]. A biblioteca *SQLite* disponibiliza um conjunto de clas-

ses para o gerenciamento e acesso aos dados na base, e é executada no mesmo espaço de endereçamento da aplicação, dispensando a comunicação entre processos ou comunicação através da rede. A base de alertas é mantida na memória principal para aumentar a velocidade do correlacionamento de alertas[1]. Quando o tamanho da base local se aproxima da capacidade da memória física, os registros que não são atualizados há mais tempo (lru) são descarregados para uma base centralizada, junto da estação de gerência da rede.

3.1. Mecanismo de Correlacionamento

O correlacionamento de alertas depende do 'casamento' das informações contidas em um alerta com informações de alertas anteriores já registrados na base de dados. Um alerta é composto de um certo número de *variáveis de correlacionamento*, e sobre estas variáveis são aplicadas as *regras de correlacionamento*, que casam as informações contidas no alerta com aquelas da base de alertas. As variáveis e as regras são descritas a seguir.

Variáveis de Correlacionamento O correlacionamento dos alarmes é efetuado pela aplicação de regras de correlacionamento sobre *variáveis de correlacionamento*, que são extraídas dos registros de eventos gerados pelos sensores. Um alerta emitido pelo Snort é mostrado abaixo. Este alerta foi gerado com a opção de alerta resumido (opção `-A fast`); as quebras de linha facilitam a formatação.

```
10/11-11:14:26.252905
[**] [1:0:0] WEB-MISC cross site scripting attempt [**]
[Priority: 0] {TCP} 192.168.0.129:47503 -> 192.168.0.95:80
```

Os campos utilizados para correlacionar os alertas emitidos pelos sensores são: (1) endereço IP origem, (2) endereço IP destino, (3) porta destino, (4) classe do ataque, (5) hora do ataque e (6) data. Os campos hora e data do ataque não são usados nesta versão do SDI-CDA. No caso do alerta mostrado acima, os valores das variáveis seriam preenchidos da seguinte forma:

1. endereço IP origem: 192.168.2.129;
2. endereço IP destino: 192.168.0.95;
3. porta destino: 80;
4. classe do ataque: WEB-MISC;
5. hora do ataque: 11:14:26;
6. data: 10/11.

Além dessas, outras três variáveis são utilizadas, duas obtidas a partir dos endereços das redes origem e destino. A terceira variável é o *limiar* do alerta, que é utilizada no correlacionamento distribuído e expressa o grau de coincidência entre alertas. O limiar é uma variável do tipo inteiro (≥ 0) que é incrementada a cada novo alerta que satisfaça a uma regra de correlacionamento com um alerta previamente armazenado.

[1]Por exemplo, para inserir e correlacionar 9 mil alertas diferentes foram utilizados 12 Mbytes de RAM, e a operação demorou 15 segundos num Pentium III (500MHz). O tempo necessário para efetuar o mesmo processamento em memória secundária (disco rígido) foi de 5 minutos.

Regras de Correlacionamento O correlacionamento de alertas é usado para reduzir a quantidade de informação que deve ser processada pelo administrador da rede. Neste sentido, o correlacionamento funciona como um filtro que elimina informação redundante e consolida as informações relevantes. As regras de correlacionamento de alertas consistem de operações binárias para relacionar alertas com características semelhantes. As regras empregadas no SDI-CDA, definidas pelas Equações 1 e 2 abaixo, são baseadas no modelo descrito em [HRTT03].

São dois os tipos de regras, (i) as regras de endereço, e (ii) a regra de classe de ataque. As *regras de endereço* (*RE*s) contém cinco cláusulas, *REipD*, *REipO*, *REpD*, *RErD* e *RErO*, baseadas nas variáveis `ipDestino`, `ipOrigem`, `portaDestino`, `redeDestino` e `redeOrigem`, respectivamente. As *RE*s são avaliadas como verdadeiras se o conteúdo de uma das variáveis de um alerta previamente armazenado for igual ao conteúdo da mesma variável em um alerta novo. Note que tanto o endereço da máquina quanto o endereço da rede são necessários para que se possa distingüir "ataques *contra* máquinas distintas na mesma rede" de "ataques *originados de* máquinas distintas na mesma rede".

A *regra de classe de ataque RCA* depende da variável *classe do ataque*, e é avaliada como verdadeira quando o conteúdo da variável *classe* de um alerta previamente armazenado é igual ao conteúdo desta mesma variável em um novo alerta. A cada avaliação verdadeira de uma das *RE*s ou da *RCA*, o valor da variável *limiar* é incrementado. Caso um alerta satisfaça a todas as cláusulas, o *limiar* desse alerta será incrementado seis vezes – $5 \times$*RE*s $+$ *RCA*.

Os resultados da avaliação das regras *RE* e *RCA* são agregados na regra *REC*, que avalia como verdadeira quando um alerta de uma certa classe já existe na base ($\cdots \wedge RCA$) e algum dos endereços fonte ou destino do novo alerta é o mesmo que no alerta pré-existente. A regra *REC* é utilizada na união de alertas (discutida adiante) e é formalizada na Equação 1.

$$REC = ((REipD \vee REipO \vee REpD \vee RErD \vee RErO) \wedge RCA) \quad (1)$$

Para eliminar alertas duplicados, o sistema de correlacionamento avalia a chamada Regra de Duplicata (*RD*). A avaliação da regra *RD* é verdadeira, se todas as avaliações das *RE*s e *RCA* forem verdadeiras, como mostra a Equação 2. As regras *RD* e *REC* são utilizadas nos correlacionamentos local e distribuído.

$$RD = (REipD \wedge REipO \wedge REpD \wedge RErD \wedge RErO \wedge RCA) \quad (2)$$

3.2. Correlacionamento local

No correlacionamento local as regras *RD* e *REC* são avaliadas sempre que um novo alerta é obtido do sensor. Caso a avaliação daquelas resulte em falso, o novo alerta é inserido na base local de alertas. Se a avaliação da regra *RD* for verdadeira, então a variável *limiar* do alerta na base que satisfez a regra *RD* é incrementada e o novo alerta é descartado por ser uma duplicata. Se a avaliação da regra *REC* for verdadeira, então a variável *limiar*

do alerta também é incrementada, mas ao invés de descartar o novo alerta é realizada a união do novo alerta com o alerta pré-existente, concatenando-se os valores das variáveis que diferem. A hora e a data são atualizadas para aquelas do alerta mais recente. O correlacionamento local é baseado naquele descrito em [HRTT03].

3.3. Correlacionamento Distribuído

A função do correlacionamento distribuído é distribuir informações sobre possíveis ataques aos correlacionadores vizinhos, e possivelmente enviar um alerta para o administrador da rede. O modelo de correlacionamento distribuído concebido para o SDI-CDA estende o modelo de Haines *et al* [HRTT03] com a atribuição de pesos distintos para alarmes tratados localmente e para mensagens recebidas de outros sensores do SDI-CDA. Além dos diferentes pesos, dois valores de gatilho são usados para disparar ações de comunicação entre sensores, ou de emissão de alerta para o administrador da rede.

Quando um alerta é inicialmente inserido na base de um correlacionador, seu *limiar* é zero. Na medida em que novos alertas sejam correlacionados, o *limiar* é incrementado e pode atingir um dos dois valores de gatilho *conversa* ou *pânico*. Quando o limiar atinge o valor de *conversa*, o correlacionador envia mensagens aos seus vizinhos informando-os do alarme em questão. Um limiar maior que o de *pânico* causa o envio de uma mensagem ao administrador da rede.

Limiares e Gatilhos Quando é realizado o correlacionamento distribuído, disparado pelo recebimento de um alerta de um correlacionador vizinho, o incremento do *limiar* pode ser maior, para se diferenciar os alertas correlacionados remotamente dos correlacionados localmente. Alertas recebidos de correlacionadores vizinhos denotam os inúmeros correlacionamentos já efetuados pelos vizinhos, e por isso podem ter maior importância ou gravidade.

O valor do *limiar* de um alerta ao longo do tempo e depende do número de cláusulas *RCA* e *RE*s avaliadas como verdadeiras. Quando correlacionado localmente, o incremento em *limiar* é a somatória da cláusulas *RCA* e *RE* verdadeiras multiplicado pelo valor do *degrau local*. Quando o alerta é recebido de um vizinho, o incremento em *limiar* é a somatória das cláusulas *RCA* e *RE*s verdadeiras multiplicado pelo valor do *degrau remoto*. O valor do degrau remoto pode ser superior ao do degrau local para aumentar a gravidade de um alerta correlacionado remotamente. A Equação 3 formaliza o cálculo do *limiar*.

$$
\begin{aligned}
limiar(t+1) &= limiar(t) \\
&+ (RCA_{\text{loc}} + RE_{\text{loc}}) \times \mathsf{degrau}_{\text{local}} && \text{se alarme local} \\
&+ (RCA_{\text{rem}} + RE_{\text{rem}}) \times \mathsf{degrau}_{\text{remoto}} && \text{se alarme remoto}
\end{aligned}
\tag{3}
$$

A Figura 2 mostra um diagrama de tempos com o comportamento do *limiar* de um alerta. Quando o *limiar* de um alerta é incrementado, o sistema de correlacionamento verifica se o valor do *limiar* desse alerta alcançou um dos dois gatilhos, *conversa* ou *pânico*. A inclinação da reta na Figura 2 é proporcional ao tamanho do incremento a cada novo correlacionamento (degrau local). O ponto *A* da figura mostra que o *limiar* alcançou o gatilho *conversa*, quando são emitidos alertas aos Narizes vizinhos. O salto no

valor do *limiar* mostrado no ponto *B* representa o acréscimo causado pelo recebimento do mesmo alerta de outro correlacionador. Esse salto é proporcional ao valor do degrau para o correlacionamento distribuído. Uma mensagem é enviada ao administrador no ponto *C*, quando é atingido o limiar de *pânico*. O valor do *limiar* é decrementado fazendo com que este fique abaixo do gatilho *conversa*, evitando assim o envio de mensagens repetidas ao administrador. Se o decremento pós-*pânico* for pequeno, o *limiar* resultante ficará acima de *conversa* e o Nariz não emitirá novas mensagens aos vizinhos.

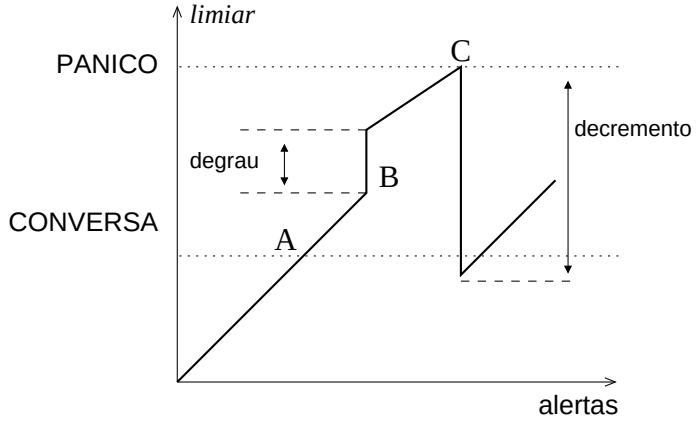

Figura 2. Relação entre *limiar*, degraus e gatilhos

O decremento mostrado na Figura 2 (fora de escala) é aquele definido na Equação 4 e foi escolhido com base nos experimentos realizados na fase inicial de desenvolvimento do SDI-CDA. Além desta, foram avaliadas quatro outras fórmulas para o decremento.

$$\textit{limiar}_{(t+1)} = \textit{limiar}_{(t)}/3 \quad (4)$$

$$\textit{limiar}_{(t+1)} = \textit{pânico}/10 \quad (5)$$

$$\textit{limiar}_{(t+1)} = \textit{conversa}/10 \quad (6)$$

$$\textit{limiar}_{(t+1)} = (\textit{pânico} - \textit{conversa}) - degrau \quad (7)$$

$$\textit{limiar}_{(t+1)} = 0 \quad (8)$$

A Equação 4 produz números relativamente baixos de mensagens ao administrador. Dependendo dos valores de *conversa* e *pânico* utilizados, as Equações 5 e 6 terão comportamento similar se $\textit{pânico}/\textit{conversa} < 10$. O decremento da Equação 7 coloca o *limiar* logo abaixo de *conversa*, causando freqüentes trocas de mensagens entre os Narizes. A Equação 8 produz o menor número de mensagens ao administrador por causa da atribuição de zero ao *limiar*. Note que a diferença entre os valores de *conversa* e *pânico* é inversamente proporcional ao número de mensagens enviadas ao administrador.

Os valores de gatilho podem ser determinados pelo usuário através de um arquivo de configuração chamado `limiar.conf`, cuja estrutura é mostrada na Figura 3. Na coluna *Classe do Ataque* é definida a classe do ataque, na coluna *conversa* é definido o valor de *limiar* para o envio de mensagens entre os Narizes, e na coluna *pânico* é definido um valor de *limiar* que dispara o envio de mensagens ao administrador da rede. As colunas $\textit{degrau}_{\mathrm{loc}}$ e $\textit{degrau}_{\mathrm{rem}}$ definem os valores usados para incrementar o *limiar* quando da correlação local ou remota, conforme a Equação 3.

Classe	conversa	pânico	degr_{loc}	degr_{rem}	comentário
WEB-MISC	10	30	4	15	infreqüente e perigoso
DDOS	12	40	1	10	infreqüente e incômodo
PORTSCAN	40	90	1	2	freqüente e inócuo
VIRUS	1	1	0	0	redes Unix são imunes
PADRÃO	20	40	1	20	*default* para as demais

Figura 3. Estrutura do arquivo de configuração

A tabela na Figura 3 contém valores hipotéticos para indicar as possibilidades de configuração do SDI-CDA. Nesta configuração, um ataque da classe WEB-MISC é considerado tão perigoso que um ou dois alertas desta classe dispariam o envio de mensagens aos correlacionadores vizinhos, e uma mensagem recebida de um vizinho dispararia um alarme ao administrador. Por outro lado, um 'ataque' da classe VÍRUS seria considerado inócuo e descartado numa rede de máquinas com Unix/Linux.

Configuração do correlacionamento local e remoto O sistema de correlacionamento do SDI-CDA pode ser configurado com bastante flexibilidade, permitindo ajustes finos na filtragem da informação que será apresentada ao administrador. Em grande medida, a flexibilidade é necessária para acomodar requisitos que mudam ao longo do tempo, e que podem, freqüentemente, ser conflitantes. A seguir são discutidos três problemas de configuração que devem ser resolvidos pelo administrador quando o sistema é configurado.

Problema 1: Pode acontecer que uma seqüência de alertas similares seja distribuída entre os correlacionadores, mas em nenhum deles tenha sido atingido o valor do gatilho *conversa*, e portanto, o administrador da rede não é avisado da tentativa de ataque. Para evitar que isso ocorra, os valores dos gatilhos de *conversa* e de *pânico* devem ser estabelecidos na proporção inversa ao número de correlacionadores no SDI-CDA, para compensar o espalhamento de tráfego: $\textit{conversa}, \textit{pânico} \propto 1/(\#\text{correlacionadores})$.

Problema 2: Quanto maior for o degrau de incremento do *limiar*, mais rápido um alerta será emitido ao administrador da rede. O valor do degrau influi diretamente no número de mensagens transmitidas pelos correlacionadores, fazendo com que o gatilho de *pânico* seja atingido rapidamente, causando assim o envio freqüente de mensagens ao administrador. Neste caso deve-se escolher um degrau pequeno para o incremento do *limiar* por conta da correlação distribuída, e um valor elevado para o gatilho do *pânico*.

Problema 3: As soluções para os Problemas 1 e 2 são conflitantes. O administrador da rede deve definir valores para os gatilhos de *conversa* e *pânico* tais que um número relativamente pequeno de alertas dispare o correlacionamento distribuído. O valor do degrau remoto tem um efeito multiplicativo com relação ao correlacionamento local. Se o degrau remoto for N, cada mensagem recebida de outro Nariz equivale a N alertas correlacionados localmente. Se o degrau remoto for igual a *conversa*, cada mensagem recebida de outro Nariz equivale ao número de alertas correlacionados localmente que dispararia a emissão de mensagens aos demais Narizes, compondo e exacerbando o efeito multiplicativo do degrau.

Validade dos alarmes ao administrador Como mostram os três problemas de configuração, a diferença entre os valores de *pânico* e *conversa*, juntamente com os degraus local e remoto, determinam o número de mensagens enviadas ao administrador da rede bem como o intervalo entre duas notificações sobre uma mesma classe de evento. Quanto maior a diferença de *conversa* e *pânico* e menor o degrau, mais demora para que o sistema de correlacionamento envie mensagens ao administrador. A configuração destes valores pode afetar seriamente a confiabilidade do SDI-CDA, causando tanto falsos-negativos – por conta da demora ou de má configuração– quanto falsos-positivos. Estes últimos são incômodos mas não potencialmente catastróficos como um falso-negativo. O número de falsos-positivos pode ser controlado através dos parâmetros de configuração do SDI-CDA, com base nos experimentos descritos na Seção 4.. As informações disponíveis em `www.dshield.org` podem ser usadas para ajustar os valores de *conversa* e *pânico* em função da atividade reportada por outros SDIs na Internet.

Dois outros problemas com a detecção distribuída são (i) a descoberta em tempo hábil de novos tipos de ataques, e (ii) detecção de ataques com poucos pacotes. No caso da identificação de novos tipos de ataque pelo operador humano, sua descoberta pode demorar porque os registros de alertas ficam armazenados nas bases dos correlacionadores e estas são descarregadas para uma base central apenas quando o tamanho da base local se aproxima da capacidade de memória dos correlacionadores, o que pode implicar em descargas a intervalos mais ou menos longos. Assim, a base central contém uma visão dos ataques atrasada no tempo. Com relação a ataques baseados em número reduzido de pacotes, o espalhador de tráfego pode inviabilizar sua detecção e portanto os valores do degrau e dos limiares devem ser escolhidos especial cuidado. Ou, algum outro meio de detecção deverá ser empregado, concorrentemente ao SDI-CDA.

4. Experimentos

Para avaliar o projeto do SDI-CDA foram realizados experimentos para validação do conceito, especialmente quanto a (i) correlacionamento pela distribuição dos sensores e o processamento paralelo dos alertas, e (ii) avaliação dos efeitos dos valores dos gatilhos de *conversa*, *pânico* e degraus na filtragem dos alertas. Como as variáveis de correlacionamento de cada alerta são registradas na base e tratadas individualmente, para fins de validação de projeto os experimentos usam sempre um único tipo de alerta.

No primeiro experimento foram enviados 500 alertas iguais para um correlacionador. O desempenho de cada uma das fórmulas de decremento é mensurado pelo número de mensagens enviadas ao administrador. Nos testes o degrau local tem valor 3, o valor de *conversa* é fixado em 20, e os valores de *pânico* são 40, 60 e 80. A Figura 4 mostra o resultado de simulações com o uso das 5 fórmulas para o decremento (Equações 4, 5, 6, 7 e 8). O eixo x mostra os valores do limiar de *pânico*, e o eixo y mostra o número de mensagens enviadas ao administrador da rede.

O gráfico na Figura 4 confirma o comportamento especificado na Seção 3.3. e mostra que: (i) quanto menor o gatilho de *pânico*, maior o número de mensagens enviadas ao administrador; (ii) quanto maior a diferença entre os gatilhos de *conversa* e de *pânico*, menor o número de mensagens; (iii) após o envio de uma mensagem ($limiar > pânico$), a Equação 5 ($limiar_{(t+1)} \leftarrow pânico/10$) produz um decremento pequeno após o envio da mensagem (cfe. Fig. 2), enquanto que as demais equações produzem um bom efeito de

filtragem das repetições. A Equação 8 ($limiar_{(t+1)} \leftarrow 0$) é a mais drástica, re-inicializando o *limiar* a cada mensagem.

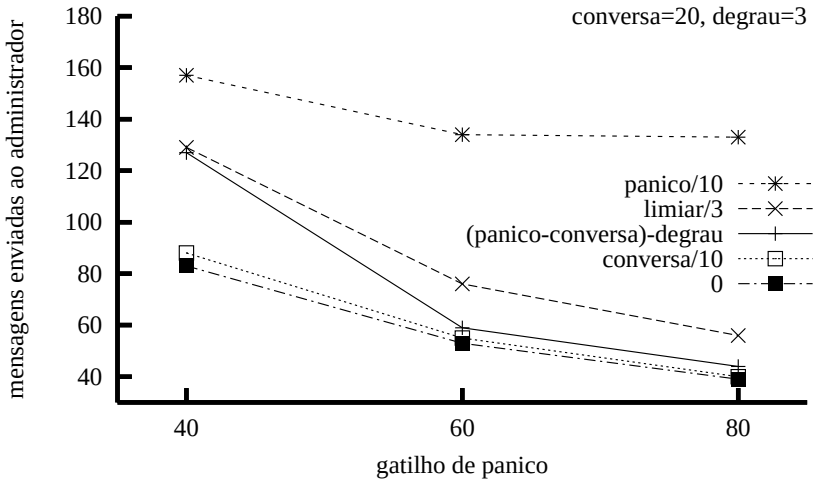

Figura 4. Efeito das 5 fórmulas para cálculo do decremento

Para evidenciar a relação entre os parâmetros de configuração (*conversa*, *pânico*, degrau) foram efetuados experimentos com 1, 2 e 3 correlacionadores, utilizando 100 alertas idênticos igualmente divididos entre os Narizes: 100 alertas para um Nariz, 50 para cada um de dois Narizes, e 34, 33 e 33 alertas para cada um de três Narizes. O valor do degrau é 1 e o decremento[2] é calculado por $limiar_{(t+1)} \leftarrow limiar/3$. O valor do gatilho *conversa* foi mantido em 40 e foram testados 6 valores diferentes de *pânico*: 50, 60, 70, 80, 90 e 100. A Figura 5 mostra o efeito de filtragem obtido com o correlacionamento. O número de alertas emitidos ao administrador (eixo y) mantém uma relação inversa ao número de correlacionadores.

A Figura 5 mostra que quanto maior a distância entre os gatilhos de *pânico* e *conversa*, mais acentuada é a filtragem das repetições. Para os mesmos valores nos gatilhos, o número de mensagens é inversamente proporcional ao número de correlacionadores. Note-se que o degrau remoto é pequeno ($= 1$), o que atenua fortemente o efeito do correlacionamento distribuído –cada alarme recebido dos vizinhos, que representa a correlação de pelo menos 40 variáveis, equivale ao correlacionamento local de somente uma variável.

[2]Note que $limiar/3 \geq pânico/3$ se os valores dos degraus forem elevados.

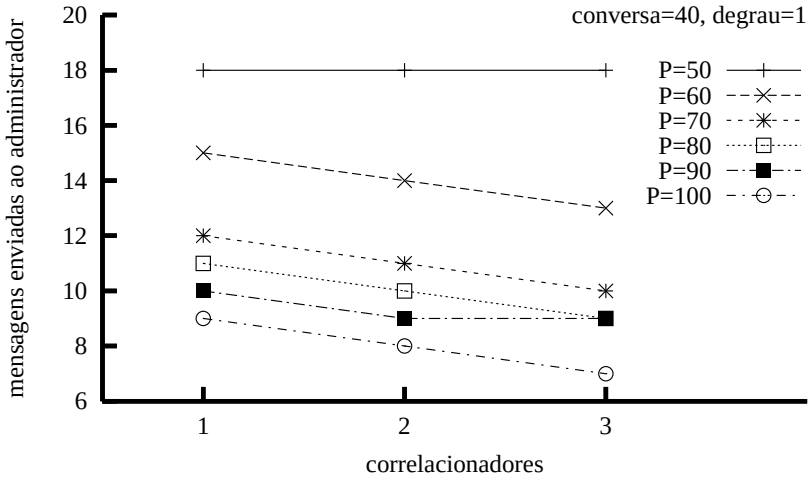

Figura 5. Mensagens emitidas ao administrador variando-se o gatilho de *pânico*

Repetiu-se o experimento anterior com diferentes valores do gatilho *conversa* (50, 70 e 90), mas com *pânico* constante em 100, e degrau remoto igual a 1. Os resultados obtidos por esse experimento são mostrados na Figura 6. Como no experimento anterior, o degrau pequeno atenua o efeito do correlacionamento distribuído. O decremento é computado pela Equação 4 ($limiar_{(t+1)} \leftarrow limiar/3$), e neste caso, a cada mensagem enviada ao administrador, o novo *limiar* do alarme é ≥ 33. Se *conversa*=50, o decremento é tal que são necessários poucos alertas (17) antes que um alarme seja enviado aos vizinhos, enquanto que para os outros dois casos o numero de alertas é 37 e 57, respectivamente. Portanto, para os maiores valores de *conversa* o correlacionamento distribuído é menos freqüente e o efeito de filtragem é mais acentuado na medida em que aumenta o número de correlacionadores.

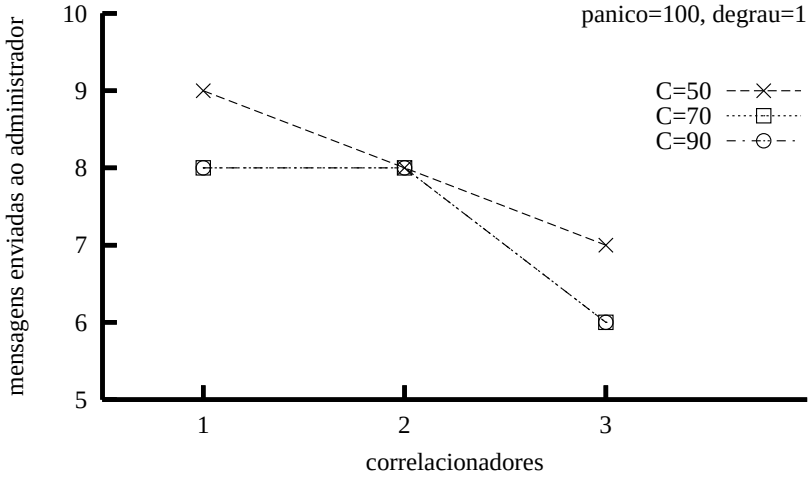

Figura 6. Mensagens emitidas ao administrador variando-se o gatilho de *conversa*

Finalmente, um experimento foi executado com 500 alertas idênticos e igualmente divididos entre 3 correlacionadores. Os 500 alertas foram emitidos para um Nariz, ou 250 alertas para cada um de dois Narizes, ou então 166, 166, 167 alertas para cada um de três Narizes. Nos três casos os valores dos gatilhos *conversa* e *pânico* (C,P) foram

(50,60), (50,70) e (70,100), o decremento é $(\mathit{limiar}_{(t+1)} \leftarrow \mathit{limiar}/3)$, e o degrau para alertas recebidos remotamente é 3. Os resultados são mostrados na Figura 7.

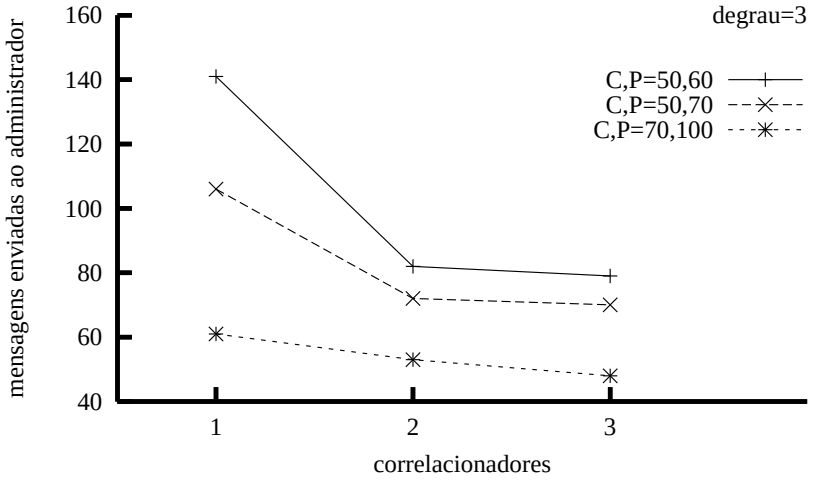

Figura 7. Relação entre número de Narizes, gatilhos e mensagens ao administrador

As curvas mostram que quanto maior a diferença entre os gatilhos de *conversa* e *pânico*, mais acentuada é a filtragem das repetições, e que o efeito de filtragem é proporcional ao número de sensores. A freqüência dos eventos de correlacionamento distribuído é determinada pela diferença entre o decremento e o gatilho de *conversa*. Para C,P=50,60, o limiar pós-pânico é $60 - (60/3) = 40 < 50$, e a diferença entre o novo limiar e o gatilho de *conversa* é 10. Isso significa que uns poucos novos alarmes provocariam o envio do alarme aos vizinhos. Para os outros dois casos (C,P=50,70 e C,P=70,100) a diferença é 3, e talvez um único alarme seria o suficiente para disparar nova rodada de correlacionamento distribuído. Isso explica porque a redução no efeito de filtragem é tão pequena entre os resultados para dois e três sensores.

5. Conclusão

Sistemas de Detecção de Intrusão para Redes são capazes de detectar e relatar atividades consideradas ofensivas à rede. A detecção de intrusão é realizada pela análise de tráfego e quanto mais intenso o tráfego, maior deve ser a capacidade de processamento do SDIR. Os sensores emitem alertas para o administrador da rede, e para reduzir o número de alertas ao mesmo tempo em que aumenta seu conteúdo semântico, os alertas são correlacionados aos alertas previamente inseridos numa base de alertas. Este artigo descreve o SDI-CDA, que é um sistema de detecção de intrusão distribuído que efetua o correlacionamento de alertas de forma distribuída, possibilitando assim o emprego de sensores que executam em máquinas de menor custo e/ou capacidade, reduzindo assim o custo da detecção de ataques.

O mecanismo de correlacionamento distribuído do SDI-CDA é uma extensão de técnicas já conhecidas de correlacionamento de alertas. O SDI-CDA é baseado na distribuição de tráfego para vários pares sensor-correlacionador, e na comunicação entre aqueles para produzir poucos alertas, mas com elevado conteúdo semântico, para serem analisados pelos administradores da rede. Os experimentos efetuados para validação do projeto demonstram claramente o efeito de filtragem de alertas.

A configuração do SDI-CDA é bastante flexível, e para permitir ajustes finos na detecção de atividades suspeitas, a cada classe de alarme são associados quatro parâmetros de configuração que determinam a freqüência com que alarmes serão enviados ao administrador da rede. Estes parâmetros também determinam o grau de cooperação entre os correlacionadores possibilitando que até uns poucos alertas de uma determinada classe produzam uma mensagem para o administrador.

O SDI-CDA necessita de validação *in vivo* quanto a seu desempenho —quantos pares sensor-correlacionador são necessários para uma certa intensidade de tráfego— e quanto a validade dos alertas —pela comparação com um SDIR centralizado, e pela definição de faixas para valores dos gatilhos e degraus. Trabalhos futuros incluem a definição de regras de correlacionamento baseado em tempo e estudos sobre a estabilidade na geração de alarmes em sistemas com grande número de correlacionadores.

Referências

T Champion and M L Denz. A benchmark evaluation of network intrusion detection systems. *Proc Aerospace Conference, IEEE*, 6:2705–2712, 2001.

F Cuppens and A Miége. Alert correlation in a cooperative intrusion detection framework. *Proc IEEE Symposium on Security and Privacy (S&P'02)*, 2002.

J B D Cabrera, X Qin, W Lee, R K Prasanth, B Ravichandran, and R K Mehra. Proactive detection of distributed denial of service attacks using MIB traffic variables – a feasibility study. *7th IFIP/IEEE Int Symposium on Integrated Network Management*, Maio 2001.

Rafael S Campello and Raul F Weber. Sistemas de detecção de intrusão. In *Minicursos do Simp Brasileiro de Redes de Computadores*. SBC, 2001.

R S Campello, R F Weber, V S Serafim, and V G Ribeiro. O sistema de detecção de intrusão Asgaard. In *Workshop de Segurança de Sistemas Computacionais*. SBC, 2001.

Thiago E Bezerra de Mello. Nariz – um sistema de correlacionamento distribuído de alertas. Dissertação de mestrado, Departamento de Informática, UFPR, Junho 2004.

H Debar and A Wespi. Aggregation and correlation of intrusion-detection alerts. In *Proc 4th International Symposium on Recent Advances in Intrusion Detection*, pages 85–103. Springer-Verlag, Outubro 2001.

S. Gibson. Distributed Reflection Denial of Service. Technical report, Gibson Research Corporation, `grc.com/dos/drdos.htm`, 2002.

J Haines, D K Ryder, L Tinnel, and S Taylor. Validation of sensor alert correlators. *IEEE Security & Privacy Magazine*, 1(?):46–56, 2003.

ISS. RealSecure Network Protection. Technical report, Internet Security Systems, 1999. `www.iss.net/products_services/enterprise_protection/rsnetwork/index.php`.

ISS. Gigabit Ethernet intrusion detection solutions. Technical report, Internet Security Systems & Top Layer Performance Testing, 2000.

C Kruegel, F Valeur, G Vigna, and R Kemmerer. Stateful intrusion detection for high-speed networks. *Proc IEEE Symposium on Security and Privacy (S&P'02)*, 2002.

B Laing. Implemeting a network based intrusion detection system. Technical report, Internet Security Systems, 2000.

B Morin, L Mé, H Debar, and M Ducassé. M2D2: A formal data model for IDS alert correlation. In *Recent Advances in Intrusion Detection, 5th International Symposium, RAID 2002*, Outubro 2002.

P A Porras and P G Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In *Proc 20th National Information Systems Security Conference (NIST-NCSC)*, pages 353–365, 1997.

M Roesch and C Green. *Snort Users Manual, Release: 1.9.1*. `www.snort.org/docs/writing_rules/`, 2001.

G E Rhoden, E T L Melo, and C B Westphall. Detecção de intrusões em backbones de redes de computadores através da análise de comportamento com SNMP. In *Workshop de Segurança de Sistemas Computacionais*. SBC, 2002.

M Roesch. Snort – lightweight intrusion detection for networks. In *USENIX LISA Conference*, Novembro 1999.

S Staniford, J A Hoagland, and J M McAlerney. Practical automated detection of stealthy portscans. *Journal of Computer Security*, 10:105–136, 2002.

SQLite. SQLite – an embeddable SQL database engine. Technical report, SQLite.org. `www.sqlite.org`.

R Vaarandi. SEC – a lightweight event correlation tool. *IEEE 2002 Workshop on IP Operations and Management*, pages 111–115, 2002.

A Valdes and K Skinner. Probabilistic alert correlation. In *Recent Advances in Intrusion Detection (RAID 2001)*, number 2212 in LNCS, Setembro 2001.

V Yegneswaran, P Barford, and S Jha. Intrusion detection in the DOMINO overlay system. In *Proc Network and Distributed Systems Security Symp (NDSS)*, Fevereiro 2004.