MODELO HÍBRIDO BASEADO EM REDES NEURAIS E SISTEMAS ESPECIALISTAS PARA DETECÇÕO DE INTRUSOS EM REDES DE COMPUTADORES TCP/IP

M.Sc. André Calazans Barreira , Dr. Rogério Alvarenga[2] e M.Sc Jerônimo Jardim
andre@calazans.net[1], rogerio@ucb.br[2] , j2odias@gmail.com[3]

Resumo - No universo da Segurança da Informação, para se criar e manter um "estado" seguro, aspectos como integridade, confidencialidade e disponibilidade devem ser garantidos. Nesse contexto, os Sistemas de Detecção de Intrusão - SDI para computadores ou rede de computadores, são mecanismos importantes para percepção de ações delituosas que visam ao comprometimento de, pelo menos, um dos três, senão os três aspectos citados acima. Assim, detectar o intruso, de maneira efetiva, pode ser o diferencial para a percepção e diagnose de um ataque. Portanto, eventos avaliados como falsos alarmes (falsos positivos), interpretações incorretas de logs e intrusões percebidas e não registradas por esses Sistemas (falsos negativos) devem ser minimizados. Este artigo apresenta um modelo que busca, por meio através da combinação de técnicas de Sistemas Inteligentes – Redes Neurais Artificiais e Sistemas Especialistas atingir este objetivo.

I. INTRODUÇÕO

SÃO inúmeros os desafios impostos pela globalização dos mercados, principalmente aqueles relacionados a questões tecnológicas. Atualmente não basta a simples conexão a uma grande rede de serviços, é preciso que tal conexão seja rápida e que minimamente esteja disponível. Não é difícil imaginar que a não realização de uma transação, seja ela comercial ou financeira, em tempo hábil, possa comprometer a sobrevivência de uma empresa.

Nesse universo, percebe-se o avanço na construção e manutenção de uma infra-estrutura de rede de computadores e telecomunicações capaz de prover a demanda de serviços criada.

Com a crescente utilização desses serviços, outros fatores foram agregados a essa infra-estrutura, como por exemplo, a confidencialidade. Para alguns, não basta a integridade da conexão e nem sua disponibilidade se o caráter confidencial não estiver presente. É nesse tripé: integridade, disponibilidade e confidencialidade que está constituído o contexto da Segurança da Informação [1].

Visualizar a segurança, como um estado obtido através da implementação e gestão de diversas práticas que também assegurem esse tripé é fundamental para a percepção de seu aspecto dinâmico e contínuo.

Políticas de segurança, Planos de Continuidade de Negócios, Controle de acessos – físicos e lógicos, a utilização de *Firewalls*, Antivírus, Criptografia, Sistemas de Detecção de Intrusão, são alguns elementos que, uma vez implantados nas organizações, podem prover maior grau de segurança.

Cada um desses instrumentos traz consigo suas peculiaridades, o que deve ser levado em consideração quando da sua implementação. Por exemplo: a criptografia utilizada por uma corporação não pode ser "pesada" a ponto de comprometer o tráfego dos dados, inviabilizando assim sua utilização; Planos de Continuidade de Negócio devem contemplar situações de recuperação de desastres, sob pena de não cumprirem sua finalidade, ou ainda, Sistemas de Detecção de Intrusos, cujos "registros" apontem para atitudes não intrusivas, que não registrem as intrusões ou ainda que a induzam falsas interpretações, podem não ser de grande utilidade para o ambiente da segurança corporativa.

Dentro desse escopo, tal modelo espera contribuir com a apresentação e a implementação de um mecanismo híbrido capaz de combinar o que se conhece por técnicas de detecção de intrusão por conhecimento e por comportamento, utilizando técnicas de Inteligência Artificial (Sistemas Inteligentes), como Redes Neurais Artificiais – RNA e Sistemas Especialistas – SE.

II. SISTEMAS DE DETECÇÕO DE INTRUSÕO - SDI

Para *Rebeca e Mell* [2], "intrusão é qualquer tentativa de comprometer a confidencialidade, integridade e disponibilidade de um sistema ou a tentativa de burlar os mecanismos de segurança de um servidor ou da rede." A intrusão pode ter origem em um atacante acessando o sistema via Internet, em um usuário autorizado que tente ganhar privilégios adicionais ou em usuários que façam mau uso dos privilégios que possuem.

Rebeca e Mell [2] definem SDIs como "sistemas de software ou hardware, que automatizam o processo de monitorar eventos ocorridos em uma rede de

computadores, analisando-os em busca de sinais de violação da segurança."

Assim, de acordo com Barreira e Guedes [3], "Sistemas de detecção de intrusão (SDI) têm a função de emitir alertas na ocorrência ou iminência de um ataque. Eles automatizam o processo de monitorar eventos que ocorrem em uma máquina ou em uma rede e analisam estes eventos em busca de sinais de que há falha na segurança."

Seja qual for o SDI, ele conterá, de forma genérica, os seguintes componentes:

a) gerador de eventos (E-box) – é a parte responsável por capturar eventos no meio externo ao SDI e padronizar os dados obtidos. A filtragem de registros de auditoria e a captura de pacotes são exemplos de geração de eventos;

b) analisador de eventos (A-box) – recebe os dados do gerador de eventos e busca padrões que caracterizem um ataque;

c) base de dados de eventos (D-box) – armazena os eventos em um arquivo para análise futura [4].

A idéia inicial para um Sistema de Detecção de Intrusos está presente no documento denominado *Computer Security Threat Monitoring and Surveilance,* que data da década de 80 que trata-se basicamente de um relatório com o propósito de melhorar a segurança dos computadores, em determinado ambiente, sob o foco da capacidade de se vigiar sistemas [5].

Em 1983, no laboratório da SRI Internacional, surge o primeiro protótipo de um SDI, à época, denominado IDES – *Intrusion Detection Expert System,* porém é entre 1984 e 1987, através dos trabalhos de *Dorothy E. Denning* e *P. Neumann,* que um modelo de IDES é proposto e desenvolvido. [6]. O modelo propunha duas técnicas de detecção de intrusão: uma delas baseada em regras previamente definidas, e a outra baseada na verificação de perfis. Nesse momento, nasce o que, mais a frente, define-se como modelos baseados em conhecimento e comportamento respectivamente [13].

Logo após, surge a idéia do SDI Distribuído que culmina com a proposta do primeiro SDI para rede de computadores, o que dá origem à denominação NSDI baseado em rede. Assim o NSM – *Network Security Monitor* - tornou-se inovador, à época, pois abordava a possibilidade de se monitorar um segmento de rede Ethernet [12].

As pesquisas mais recentes apontam, basicamente, para dois caminhos: um deles é a criação de novos modelos, isto é, elementos constitutivos de um SDI são alterados ou têm sua dinâmica modificada, buscando o processo de melhoria, e o outro é a tentativa de se estabelecer padrões, através da análise de perfis refinados que representam o comportamento do usuário, dando, assim, continuidade evolutiva ao proposto lá na década de 80.

A. Classificação de um SDI

Bace e Mell [2] e Weber, Campelo [4], classificam SDI's segundo quatro critérios:

a) Método de Detecção: a detecção de um ataque pode ser baseada em comportamento ou em conhecimento. No primeiro caso, a ferramenta SDI traça um perfil do comportamento considerado normal e alerta quando algo fora deste padrão ocorrer. No segundo caso, o SDI possui uma base de assinaturas, semelhante aos programas antivírus, que contém os padrões de ações de intrusão conhecidos. Ele, então, compara o tráfego monitorado com estes padrões e alerta quando encontra alguma correspondência;

b) Arquitetura: os sistemas de detecção podem ser baseados em rede, quando monitoram o tráfego da rede, mas ignoram que se passa em cada máquina internamente; em host, quando monitoram as máquinas, mas ignoram o que se passa nos elementos de rede ou em outras máquinas, ou híbridos;

c) Comportamento Pós-detecção: pode ser ativo ou passivo;

d) Freqüência de Uso: um SDI pode ser destinado a monitoramento contínuo ou à análise periódica.

III. O USO DE TÉCNICAS DE SISTEMAS INTELIGENTES NA DETECÇÕO DE INTRUSÕO

No início da década de 90, surgiram os primeiros trabalhos que utilizam RNAs como instrumento de percepção da atividade intrusiva. Em 1992, um modelo denominado IDES – *Intrusion Detection Expert System* - é proposto, tendo em sua constituição elementos de RNA's e SE's, problemas com a escalabilidade do sistema e o treinamento do elemento de RNA, além dos testes terem sido realizados somente com os eventos de *logon* e *logout* são características desse modelo [7].

Cannady [8] apresenta resultados sobre a utilidade de uma Rede Neural Artificial, do tipo, MLP – Multi Layer Perceptron no reconhecimento de ataques, como *SYNFlood, SATAN test* e *ISS Scan test*, Satade utilização de RNAs, do tipo MLP – *Multi Layer Perceptron* para a detecção de intrusão, porém aponta problemas com a diversidade de comandos no campo de dados de um datagrama do IP – *Internet Protocol.*

Ainda utilizando RNA e no mesmo ano, outro trabalho é apresentado onde resultados de um NNID – *Neural Network Intrusion Detector* - são apresentados, cujo funcionamento se dá através da percepção das ações intrusivas, baseando-se em perfis que representam a ação de 100 comandos utilizados pelo usuário.

Apresentou taxa de acerto em 93% nos testes com uma taxa de 7% de falso positivo [9].

Em 2001 e 2002 outros trabalhos com a utilização de RNA's são apresentados e não fogem dos, até então, propostos, à exceção da inovação com a utilização do algoritmo de LVQ - *Learning Vector Quantization* [10].

Já em 2003, a utilização de SVM's – *Support Vector Machines* é apresentada e validada sob a coleção de dados intrusivos do DARPA dos EUA - *Defense Advanced Research Projects Agency* - ratificando como resultado a prática da técnica para a utilização em ferramenta de detecção de intrusão em tempo real [11].

IV. O MODELO PROPOSTO

Diz-se que o modelo proposto é híbrido por duas razões: a primeira por combinar duas técnicas de Sistemas Inteligentes – Redes Neurais Artificiais e Sistemas Especialistas; e a segunda por também, combinar dois métodos diferenciados de detecção de intrusão – aqueles baseados em comportamento e em conhecimento. Tal relação pode ser estabelecida de forma direta, isto é, a submissão à RNA está para a detecção em comportamento, assim como a apreciação pelo Sistema Especialista está para a detecção baseada em conhecimento.

Para a aplicação e implementação do modelo foi desenvolvido uma nova ferramenta de detecção, que satisfaz aos requisitos apresentados no item 2 desse artigo, denominada *Newnids*.

Está inscrita em linguagem C e para o Sistema Operacional LINUX.

Assim, a proposta é a seguinte: perceber o tráfego entrante em uma rede de computadores, que usa tecnologia ETHERNET e está baseada em TCP/IP, submetê-lo ao parecer de uma RNA do tipo MLP, cujo resultado será submetido ou não a um Sistema Especialista (ambos formam a *Engine*) o que findará na diagnose se ação é ou não intrusiva.

Pode-se resumir em etapas o fluxo dos pacotes através do modelo:

1) a captura dos pacotes;
2) a decodificação dos pacotes e conseqüente obtenção dos valores que serão submetidos à *Engine* de detecção;
3) O parecer da RNA e, em caso de dúvida, da ação intrusiva, subseqüente submissão ao Sistema Especialista;
4) Registro do diagnóstico, seja ela da RNA ou do SE.

A figura 1 apresenta o modelo.

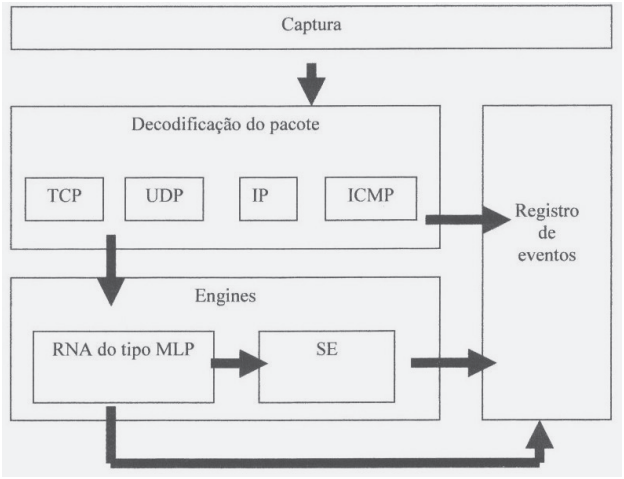

Figura 1 – Representação do fluxo da informação através da ferramenta Newnids.

A captura está baseada na biblioteca *libpcap* sendo similar a outras ferramentas de coleta de tráfego, como TCPDUMP e ETHEREAL, podendo impor a interface de rede à operação em modo promíscuo.

O processo de decodificação obedece ao padrão definido em RFC – *Request for Comment* - para cada protocolo. Desta forma, é possível extrair toda a informação protocolar existente no pacote.

A. Características da RNA utilizada

Para a técnica de detecção por comportamento, foi utilizada uma RNA face a sua capacidade de abstração.

Na detecção por comportamento, o maior desafio é a diminuição dos eventos falsos positivos e as falsas interpretações, e uma grande vantagem está na possibilidade de identificação de novos padrões de ataque.

A RNA é do tipo MLP - *Multi Layer Perceptron* com 16 neurônios na camada de entrada, 7 na camada intermediária e 1 na saída. O neurônio da saída é o responsável pela diagnose, e seu valor pode variar entre 0,000000 e 1,00. Se for menor que 0,3, o pacote de dados é considerado normal. Se estiver entre 0,3000000 e 0,600000, o pacote é considerado suspeito e então precisa, ainda, do parecer do Sistema Especialista para o posicionamento final. E por fim, se ele é maior que 0,600000 é considerado intrusivo.

Para o processo de treinamento foi utilizada a estrutura do software EasyNN, atendendo ao fluxo proposto pela figura 2, tendo a base de registros sido extraída de ambiente criado exclusivamente para a captura de pacotes considerados intrusivos a partir da utilização de algumas técnicas de varredura de portas e *http evasion e insertion*.

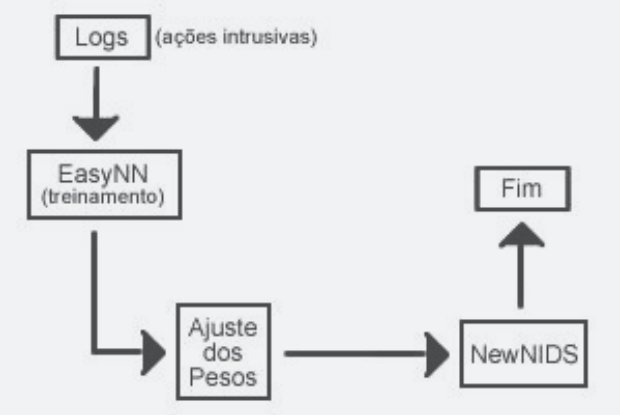

Figura 2 – O processo de treinamento e incorporação dos pesos ao código da ferramenta Newnids

A figura 3 apresenta a curva de aprendizado pertinente a RNA treinada, extraída do software EasyNN.

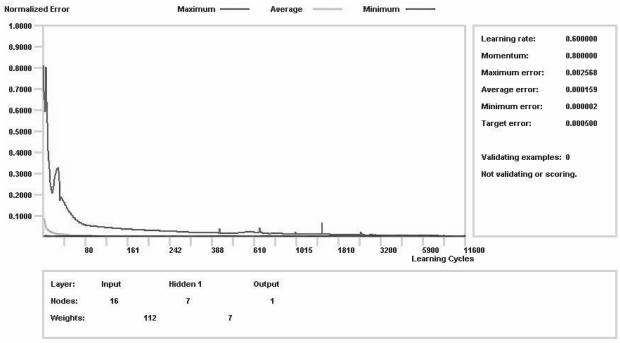

Figura 3 – Curva de aprendizado da RNA gerada pelo EasyNN.

Em qualquer uma dessas avaliações, pode-se efetuar o registro do resultado em logs, onde, através do Newnids, há a indicação de qual dos mecanismos de detecção foi o responsável pelo diagnóstico e o que o levou a tal resultado.

A figura 3 apresenta um registro de parecer da RNA para um pacote normal (RNA OUT: 0.001894).

```
ENGINE RNA: PROTO: 6 FLAGS: 18 IP
HLen:20   IPS:   200.152.161.128:80
IPD: 192.168.0.186:32784 Data Len:
0
ASCII SIG: 10 ICMP CODE: 0 RNA OUT:
0.001894
```

Figura 3 – Exemplo de parecer dado pela RNA.

A figura 4 apresenta a RNA idealizada, onde os neurônios de entrada são representados pelos seguintes campos extraídos de pacote de dados:

a) Protocolo correspondente, na RNA = *proto*. Para o protocolo TCP, o campo receberá valor 06, para o protocolo UDP, 17, e para o ICMP 01, por definição de padrão;

b) Endereço IP de origem, na RNA = *ips1, ips2, ips3 e ips4.* Recebem seus valores obedecendo a uma regra específica;

c) Endereço IP de destino, na RNA = *ipd1, ipd2, ipd3 e ipd4.* Recebem seus valores obedecendo a mesma regra para o IP de origem;

d) Porta TCP de origem, na RNA = *s_port*; recebe qualquer valor entre 0 e 65535, por definição de padrão, dependendo do serviço que se está oferecendo;

e) Porta TCP de destino, na RNA = *d_port*, obedece ao mesmo critério da porta de origem;

f) Flags TCP, na RNA = *flags*;

g) Tamanho do cabeçalho TCP, na RNA = *h_len*;

h) Mensagem ICMP, na RNA = *icmp_cod*;

i) Assinatura dos dados, na RNA = *d_sig*;

j) Tamanho do datagrama, na RNA = *d_len*.

Os endereços IP de origem e destino do pacote estão representados na RNA de forma diferenciada face a problemas de conversão. Assim, obedeceram à seguinte regra:

a) Obtêm-se os valores em *network byte order* para arquiteturas *little endian*, ou seja o bit menos significativo vem primeiro;

b) Esse valor é convertido usando-se a função *nthol()* para um inteiro longo e sem sinal de 32 bits;

c) O resultado é submetido à função *inet_ntoa()* que gera, como saída, o número IP em notação de ponto, que é novamente convertido em um inteiro *long* usando a função *inet_addr()*;

d) Para finalizar, são realizadas 4 operações de deslocamento de bits, de onde se obtém 4 partes numéricas, representativas para cada octeto e que, na RNA, estão identificadas como *ips1, ips2, ips3 e ips4* para o número IP de origem e *ipd1, ipd2, ipd3 e ipd4* para o número IP de destino.

Outro campo que precisou de tratamento diferenciado foi o *payload*, isto é, aquele que contém os dados do pacote. Para este, foi criado um *checkum* através da fórmula: (anterior * sua_posição) + (atual * sua_posição) + (posterior * sua_posição), sendo esta aplicada a cada byte do vetor responsável deste campo. Esse resultado esta armazenado na RNA sob o nome de *d_sig*.

B. O Sistema Especialista

Ferramentas de detecção de intrusos baseadas em conhecimento utilizam-se de bases de regras para a efetiva percepção da ação delituosa. Constroem essa base de regras a partir do conhecimento e interpretação

de ataques registrados à rede de computadores ou *hosts*. Assim, aquilo que já é conhecido como intrusivo é consignado ao conjunto de regras, o que possibilita a criação de uma base de conhecimento.

A desvantagem nesse tipo de detecção está no caráter estático das regras, o que impede, por exemplo, a compreensão de um novo padrão de ataque, porém o número de falsos positivos tem se demonstrado menor.

No caso especifico do modelo proposto, utiliza-se um Sistema Especialista baseado em regras. Tais regras podem ser originadas, por exemplo, pelas informações contidas nas regras da ferramenta SNORT, disponível em *www.snort.org*, ou ainda, contemplar especificidades definidas pelo usuário.

Elas estão em um arquivo próprio que é consultado e carregado quando da inicialização da ferramenta.

A tabela 1 apresenta o formato de uma regra.

TABELA I
Formato de uma regra da ferramenta Newnids

	Campo	Valor
Se	Protocolo	
E	Número Ip do Servidor	
E	Número da porta TCP	
E	Mensagem a ser gravada no evento	
E	Fluxo do pacote	
E	Conteúdo procurado no *payload*	
Então	Categorização do ataque	

V. LIMITAÇÕES IMPOSTAS AO MODELO

Não foram focadas, no modelo proposto, dificuldades já relacionadas na literatura, como ”inibidoras” da efetividade de um SDI, tais como:

a) A percepção e captura em redes de alta velocidade;

b) A questão do tráfego criptografado;

c) O posicionamento de um SDI;

d) Características de desempenho da ferramenta de SDI em rede.

Backbones que utilizem tecnologias de rede do tipo ATM e FDDI também não foram contemplados.

VI. AS VANTAGENS DO MODELO

Em um primeiro momento, observam-se as seguintes vantagens na aplicação do modelo:

a) A combinação da utilização dos dois métodos de detecção de intrusos, permite maximizar os acertos e minimizar os erros, equação essa extremamente importante quando se fala em percepção da atividade intrusiva;

b) A possibilidade de se permitir um caráter exclusivo à aplicação, isto é, o usuário familiarizado com as variáveis envolvidas pode retreinar a RNA concebida e criar suas próprias regras, personificando, assim, a ferramenta;

c) A possibilidade de se minimizar a intervenção humana na gestão diária de um SDI.

VII. TRABALHOS FUTUROS

De pronto, quatro iniciativas poderiam contribuir para a continuidade e melhoria do modelo apresentado:

a) A inclusão de análise por estado, isto é, a percepção de todo um *handshake* em uma conexão TCP como um conjunto, já que a proposta inicial contempla a análise de pacote a pacote;

b) A criação de RNA diferentes e independentes para cada protocolo pode aumentar o refinamento da ferramenta sem impactar na performance de análise do tráfego;

c) A substituição da RNA do tipo MLP por uma do tipo ART e / ou KOHONEN, alcançando, assim os benefícios impostos pelas redes do tipo *SOM's – Self Organize Maps*;

d) A não submissão ao elemento neural do endereçamento IP;

e) O desenvolvimento em modo ”kernel use” aproveitando as tecnologias existentes para esse modo naquilo que diz respeito à análise do tráfego em redes de alta velocidade, bem como a implementação da análise de estado de uma conexão TCP.

VIII. CONCLUSÕO

O modelo foi avaliado sob dois aspectos. O primeiro, quanto à atividade intrusiva, e o outro, quanto à percepção do tráfego normal. Para a percepção da atividade intrusiva, foram utilizadas técnicas de varredura de portas e http *evasion* e *insertion* onde se obteve 100% de detecção, à exceção dos pacotes UDP que, por definição, foram dirigidos diretamente ao SE, inexistindo, assim, falsos negativos. Já a submissão à atividade normal visava basicamente à detecção da presença de falsos positivos, cujo resultado aproximou-se de 1,02% médio dos pacotes, valor considerado bastante bom diante do aferido médio para técnicas de

http *evasion* e *insertion*, através de outras ferramentas, como o SNORT (33,35%) e Firestorm (42,14%) e para a técnica de varredura de portas 4,71% para o SNORT e 12,93 para o Firestorm[14].

Evidenciou-se que o modelo proposto utiliza o potencial de generalização, obtido naturalmente pela rede neural durante a aprendizagem dos padrões de ataques já classificados, aumentando a eficácia da rede para técnicas derivadas das formas de ataque já conhecidas.

Quanto aos incertos (assim classificados pela engine RNA), o sistema especialista atua como um certificador, identificando, através da sua base de conhecimento, a qualidade dos dados, buscando reduzir incertezas.

Portanto, a combinação de técnicas de detecção de intrusão com representação neural e simbólica pode constituir maior qualidade no processo de detecção de intrusão.

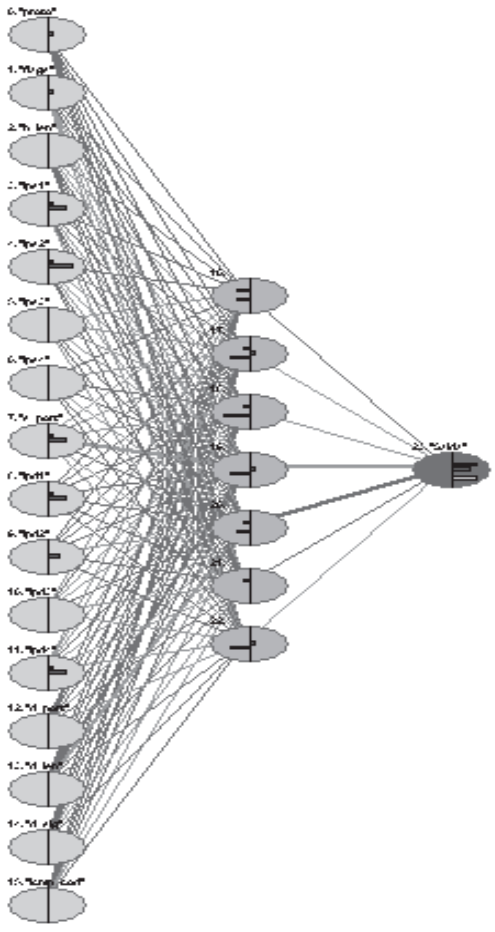

Figura 4 – A Rede Neural Artificial do Newnids

IX. REFERÁNCIAS BIBLIOGRÁFICAS

[1] NBR ISO/IEC 17799. Tecnologia da Informação – Código de prática para a gestão da segurança da informação. ABNT, 2001.

[2] BACE, Rebecca; MELL, Peter. Intrusion Detection Systems. NIST, 2001. (Disponível em http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf - acessado em 16.11.2003.)

[3] BARREIRA, André; GUEDES, William. Estudo de Caso de Implementação e Manutenção de SDI de Domínio Público. 2001. Monografia (Pós-Graduação Lato Sensu em Segurança de Redes de Computadores), UCB, Brasília-DF.

[4] BARREIRA, André; Dissertação de Mestrado. Modelo Híbrido Baseado em Sistemas Inteligentes para Detecção de Intrusos em Redes TCP/IP. Pós-Graduação Strictu Sensu em Gestão do Conhecimento e da Tecnologia da Informação; Orientação : Rogério Alvarenga, DSc; UCB, Brasília - DF, 2006.

[5] ANDERSON, James P. Co. Computer Security Threat Monitoring and Surveillance. 1980. Disponível em: http://csrc.nist.gov/publications/history/ande80.pdf - consultado em 15/01/04.

[6] SRI. Intrusion Detection – History. 2002. Disponível em http://www.sdl.sri.com/programs/intrusion/history.html - consultado em 17/01/04

[7] DEBAR, H., BECKER, M., e SIBONI, D. A Neural Network Component for a Intrusion Detection System. In Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy. 1992. pp 240-250.

[8] CANNADY, J. Artificial Neural Networks for Misuse Detection. 1998. Disponível em http://citeseer.ist.psu.edu/cannady98artificial.html – consultado em 17/01/2004.

[9] RYAN, Jake; LIN, Meng-Jang; MIKKULAINEN, Risto. Intrusion Detection with Neural Networks. 1998. Disponível em http://citeseer.ist.psu.edu/ryan98intrusion.html - consultado em 30/03/04

[10] MARLIN, Jack; RAGSDALE, Daniel; SURDU, John. A Hybrid Approach to the Profile Creation and Intrusion Detection. IEEE Proceedings of the DARPA Information Survivability Conference and Exposition, 2001.

[11] MUKKAMALA, Srinivas; SUNG, Andrew. Feature Ranking and Selection for Intrusion Detection Systems Using Support Vector. 2003. Disponível em http://citeseer.ist.psu.edu/583136.html - consultado em 22.03.04.

[12] HEBERLEIN, Tood et al. A Network Security Monitor. IEEE Computer Society. Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy.1990, pp. 296-303, pp. 296-303.

[13] DENNING, Dorothy E. An Intrusion-Detection Model. IEEE Transactions on Software Engineering, vol. SE-13, nº 2. 1987, 222-232. Disponível em: http://www.cs.georgetown.edu/~denning/infosec/SDI-model.rtf - consultado em 17/01/04

[14] FAGUNDES, Leonardo. Metodologia para avaliação de sistemas de detecção de intrusão. 2002. Monografia (Bacharelado em Informática), Universidade do Vale do Rio dos Sinos, São Leopoldo-Brasil.

[15] WEBER, Raul Fernando; CAMPELLO, Rafael Saldanha. Sistemas de Detecção de Intrusão. Instituto de Informática – UFRGS, 2001 (Disponível em http://www.inf.ufrgs.br/~gseg/producao/minicurso-SDI-sbrc-2001.pdf - consultado em 16.11.2003).