Detecção de Invasores em Redes de Computadores Utilizando um Algoritmo Imunológico Artificial de Seleção Negativa

Amanda P. A. Lima[†] **Fernando P. A. Lima**[†] **Carlos R. Minussi**[†]
[†]Departamento de Engenharia Elétrica, Faculdade de Engenharia de Ilha Solteira (FEIS)
Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), Ilha Solteira, SP, BRASIL
E-mails: amandaparra.eng@gmail.com, engfernandoparra@gmail.com, Minussi@dee.feis.unesp.br

Palavras-chave: *Detecção de invasores, Redes de computadores, Sistemas Imunológicos Artificiais, Algoritmo de Seleção Negativa, Análise do fluxo de dados.*

Resumo: *Neste artigo apresenta-se uma ferramenta para detecção de estados de intrusão em redes de computadores utilizando sistemas imunológicos artificiais. Desta forma, baseando-se em um algoritmo de seleção negativa, realiza-se a análise e classificação do sinal em dois estados comportamentais: próprio (condição normal) e não-próprio (invasão). A principal aplicação desta ferramenta é auxiliar os operadores de redes de computadores, durante ataques, bem como proporcionar a assistência necessária para a tomada de decisão. Para avaliar esta metodologia foram realizadas simulações em uma rede de computadores real, onde foi gerada uma base de dados contendo amostras da rede em situações normais e de invasão. Esse conjunto de dados é utilizado para analisar o desempenho do método proposto. Os resultados obtidos mostram precisão e eficiência no diagnóstico de invasores em redes de computadores.*

1 Introdução

Nos dias atuais, utilizar computadores, notebooks e gadgets (celulares, tablets, smartphones, etc.) para se comunicar e transferir informações é cada vez mais comum [12]. Isto porque a maioria das pessoas tem acesso à internet e, de alguma forma, estão no mundo globalizado. Contudo, as empresas, indústrias e comércios se voltaram para o mercado on-line, onde é possível comprar, vender, negociar e se comunicar de forma instantânea, ou seja, ter acesso a dados e informações de forma imediata. Neste sentido, pode-se dizer que a sociedade passa por uma revolução tecnológica.

No entanto, existe uma grande preocupação com a segurança e integridade das informações, ou seja, será que realmente o ambiente é seguro para se comunicar e realizar transações? Esta é uma pergunta complexa de ser respondida.

De uma forma geral, garantir a segurança de uma rede de computadores é uma tarefa muito complexa, pois é necessário monitorar todos os usuários e estar pronto para tomar uma decisão rápida em um momento de falha (ataques e invasões) eliminando o problema e mantendo a integridade das informações. Outro problema é conseguir que os usuários respeitem políticas de utilização e segurança, o que nem sempre acontece, assim propiciando vulnerabilidade na rede ou nas informações.

Uma alternativa para contornar este problema é utilizar sistemas computacionais capazes de identificar anormalidades, situações de invasões e vulnerabilidades em redes de computadores. Estes sistemas de segurança de rede são conhecidos como IDS (*Intrusion Detection Systems*) e IPS (*Intrusion Prevention Systems*), ou seja, sistemas de detecção e prevenção de intrusos em redes de computadores.

De acordo com [13], a utilização de IDS e IPS é cada vez maior, principalmente por empresas. Visando tornar os IDS e IPS mais eficientes, muitos desenvolvedores começaram a utilizar técnicas de sistemas inteligentes, como redes neurais, lógica *fuzzy*, computação evolutiva, inteligência de enxame e sistemas imunológicos artificiais. Neste sentido, a seguir apresentam-se os trabalhos mais relevantes disponíveis na literatura.

Em [4], um modelo de IDS foi proposto com o objetivo de detectar intrusões ou anomalias em redes de computadores usando uma abordagem imunoinspirada baseada em sistemas

DOI: 10.5540/03.2014.002.01.0015

multiagentes. Já em [7], foi proposta uma analogia entre a detecção de intrusos e os sistemas imunológicos concebendo ideias que podem ser incorporadas na construção de um sistema de defesa de uma rede de computadores. Um modelo, denominado CDIS (acrônimo de *Computer Defense Immune System*), é proposto em [1]. Este sistema imunoinspirado foi implementado para a detecção de intrusão e de vírus em computadores. Em [2] e em [9] são apresentadas abordagens baseadas em sistemas imunológicos para detecção de intrusos. O primeiro artigo enfatiza as razões do uso dos SIA's (Sistemas Imunológicos Artificiais) e traça um comparativo entre os métodos utilizados. O segundo artigo descreve, de maneira mais detalhada, as análises do primeiro artigo e traça novas analogias. Em [5] é avaliado um IDS imunoinspirado através de *hackers* gerados por métodos evolucionários.

Neste trabalho, apresenta-se um método de detecção de invasores em redes de computadores utilizando um algoritmo imunológico de seleção negativa. A principal contribuição é a forma de análise, isto é, para identificar comportamentos anormais, o algoritmo analisa somente o fluxo de dados na rede de computadores. Este método pode auxiliar operadores de redes e técnicos de segurança em TI, proporcionado rapidez, confiabilidade e segurança no planejamento de ações corretivas para eliminar situações de ataques invasores em redes de computadores. Para avaliar esta metodologia, foram realizadas simulações em uma rede de computadores real. Nessas simulações, foram geradas amostras da rede em situações normais e de invasão. Este conjunto de dados foi utilizado para analisar o desempenho do método proposto.

2 Segurança Computacional

A segurança em redes de computadores é fundamentalmente importante, pois os ataques aos sistemas tornam-se cada vez mais sofisticados. A preocupação com a segurança é indispensável nesses casos, pois os computadores podem ser utilizados para transações financeiras, comunicação e armazenamento de dados. Assim, existe a possibilidade de ocorrer tais ataques que podem ocasionar em:

- Roubos de informações sigilosas como senhas e números de cartões de credito ou débito;
- Acesso não autorizado a internet;
- Propagação de vírus;
- Disseminação de falsas mensagens;
- Acesso remoto para ocultar a identidade do invasor ou lançar ataques contra outros computadores.

A maioria das transações realizadas em rede, especialmente na internet, refere-se a transações de pagamento eletrônico, acesso bancário ou qualquer outra transação comercial, financeira ou confidencial e com a possibilidade de ocorrer um novo ataque de intrusão, estas podem ser danificadas. Para que tais ataques sejam minimizados, é necessário munir-se de ferramentas de proteção para as redes de computadores [2].

3 Algoritmo de Seleção Negativa

O algoritmo de seleção negativa (ASN) foi proposto por [8] para detecção de mudanças em estados de sistemas. É baseado na seleção negativa de linfócitos T dentro do timo. Este processo trabalha com a discriminação de células próprias e não-próprias. O algoritmo é executado em duas fases, conforme ilustrado nos fluxogramas apresentados na Figura 1 [6].

A fase de censoriamento do ASN consiste-se, basicamente, em gerar um conjunto de detectores. Os detectores são análogos às células tipo T, maturadas capazes de reconhecer agentes patogênicos. A fase de monitoramento consiste-se em monitorar um sistema, visando identificar uma mudança no comportamento do mesmo, e assim classificar esta mudança utilizando o conjunto de detectores criados na fase de censoriamento [4].

DOI: 10.5540/03.2014.002.01.0015

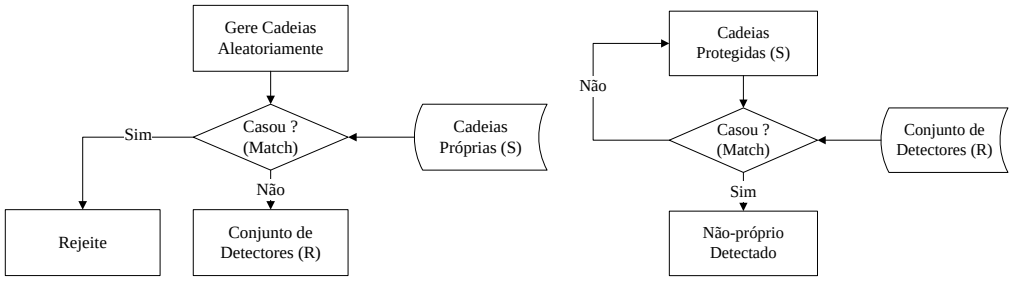


Figura 1: Fluxogramas do ASN.

3.1 Critério de Afinidade

Para avaliar a afinidade entre as cadeias e afirmar que são semelhantes, utiliza-se um critério conhecido como casamento. O casamento pode ser perfeito ou parcial [10]. Neste trabalho utiliza-se o casamento parcial. No casamento parcial, uma quantidade de pontos entre os padrões deve ter o mesmo valor para se confirmar o casamento, sendo a quantidade (taxa de afinidade) definida previamente. A taxa de afinidade representa o grau de semelhança necessário para ocorrer o casamento entre os dois padrões. A taxa de afinidade é definida através da seguinte relação [3]:

$$TAf = \left(\frac{An}{At} \right) * 100 \tag{1}$$

sendo:

TAf : taxa de afinidade;

An : número de cadeias normais no problema (cadeias próprias);

At : número total de cadeias no problema (cadeias próprias e não-próprias).

Através da equação (1), pode-se calcular, de forma correta, o valor da taxa de afinidade para o problema proposto, onde a equação (1) representa uma relação estatística entre todas as amostras do problema.

4 Metodologia Proposta

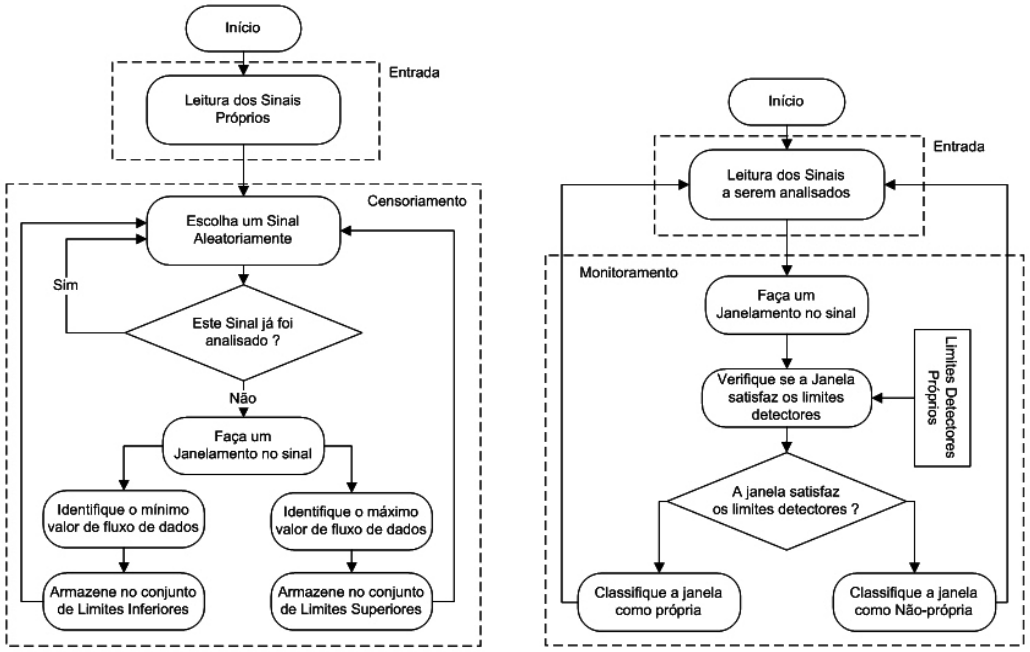
O sistema de detecção de intrusos em redes de computadores, proposto neste artigo, é baseado em análise de séries temporais, *i.e.*, são definidos previamente limites ao qual o fluxo de dados pode variar. Caso o fluxo corrente ultrapasse estes limites, uma situação anormal (invasão) é identificada. O método proposto consiste-se em duas fases, sendo o censoriamento e o monitoramento dos dados. A seguir apresentam-se as fases de censoriamento e monitoramento do sistema de diagnóstico de intrusos em redes de computadores.

4.1 Fase de Censoriamento

Nesta fase são gerados os limites detectores para serem utilizados pelo SIA durante o processo de monitoramento de sinais. Por causa do problema em questão possuir duas classes de padrões específicas, ou seja, a situação normal e a situação de invasão, faz-se necessário que o algoritmo tenha conhecimento somente dos sinais que contemplam a operação normal da rede (próprios), para que com base nestas informações realize a discriminação do que é próprio (normal) e do que é não-próprio (invasão). Sendo assim, a fase de censoriamento para este sistema tem um único passo. Neste passo, definem-se os limites mínimo e máximo a qual um sinal da rede em operação normal pode atingir. Está rotina apresentada na figura 2 (a), que ilustra como é realizado o processo de geração dos limites detectores próprios.

No fluxograma apresentado na figura 2 (a), inicialmente faz-se a leitura de todos os sinais com operação normal da rede de computadores. Analisando estes sinais é identificado o valor

máximo e mínimo de fluxo de dados. Esses valores são definidos como sendo os limites máximo e mínimo, em que se considera que o sinal esta em operação normal.



(a) (b)

Figura 2: Fluxogramas do sistema de detecção de intrusos.

4.2 Fase de Monitoramento

A fase de monitoramento é dividida em dois módulos, os quais são responsáveis por fazer a leitura dos dados e realizar a discriminação próprio/não-próprio. Na figura 2 (b), mostra-se o fluxograma da fase de monitoramento dos sinais.

Nesta fase, faz-se a leitura dos sinais que se deseja analisar e, assim, faz-se um janelamento destes sinais, verificando se as janelas estão dentro dos limites detectores gerados na fase de censoriamento. Caso a janela esteja entre os limites inferior e superior, esta janela é classificada como própria (operação normal). Caso contrário, a janela é classificada como não-própria (estado de invasão), ou seja, o sinal esta violando os limites estabelecidos, e assim é desconhecido pelo sistema. Este processo é repetido em cada sinal, e assim é realizado o monitoramento dos dados.

Ressalta-se que para o sinal ser classificado o número de janelas corretamente classificadas deve ser maior que a taxa de afinidade (*TAf*).

5 Simulações

Para este trabalho foram realizadas simulações em uma rede de computadores real, onde foi capturado e armazenado o fluxo de dados da rede. Para isto, faz-se necessário prover/oferecer recursos (nativos ou de *software*) para rastrear os processos da máquina, ou um *software* capaz de oferecer informações de rede, como um *sniffer*, por exemplo. O sistema operacional Linux, usado nesta abordagem, já oferece esses recursos: o programa *strace*, nativo no Linux rastreia processos e armazena dados destes processos. Assim, é possível rastrear o fluxo de dados da rede de computadores e armazená-lo. Para os testes foram utilizadas duas ferramentas: sendo o *nmap* que detecta endereços IPs (*internet protocol*) ativos e portas abertas em uma rede de computadores, e o *scp* (*secure copy protocol*) que efetua cópias de arquivos em diferentes locais em rede.

DOI: 10.5540/03.2014.002.01.0015

Nas simulações realizadas consideram-se duas situações, *i.e.*, dois cenários, sendo o uso do *nmap* o comportamento anormal (invasão) e o uso do *scp* o comportamento normal. A seguir são apresentados os passos realizados em cada um dos cenários:

Cenário de invasão:

1. Usuário acessa a máquina, fornecendo nome de usuário e senha.
2. Usuário executa o *nmap* procurando várias máquinas em redes diferentes.
3. O processo leva de 1 a 5 minutos para ser concluído.

Cenário normal:

1. Usuário acessa a máquina, fornecendo nome de usuário e senha.
2. Usuário executa o *scp* para enviar arquivo a um servidor.
3. O processo depende do tamanho do arquivo, geralmente enviado a taxas de 5Mbps.

Em cada um dos cenários criados, o fluxo de dados na rede é capturado e armazenado. Partindo desta informação, são realizados os testes.

A rede de computadores utilizada conta com 1 servidor e 12 computadores. Nesta rede, supõe-se que um computador dessa rede foi acessado indevidamente e este computador foi utilizado para realizar uma invasão. Os programas utilizados são o *nmap*, usado remotamente pelo atacante para a busca de outras máquinas, caracterizando uma situação de invasão, e o *scp*, usado regularmente para enviar arquivos ao servidor da rede, caracterizando uma operação normal.

Na tabela 1 apresenta-se a quantidade de simulações realizadas para cada cenário.

Tabela 1. Quantidade de simulações realizadas.

Cenário	Quantidade de simulações
Normal	300
Invasão	300
Total	600

Ressalta-se que o tempo de simulação varia de acordo com a execução do processo, seja normal ou anormal.

6 Aplicações e Resultados

Nesta seção, apresentam-se os resultados obtidos com a aplicação do método proposto na base de dados que foi simulada. Todos os testes foram realizados utilizando um PC Intel Core 2 Duo 1.9 GHz, 2 GB de Memória RAM, e sistema operacional Windows 7 Ultimate 32 bits. O algoritmo foi desenvolvido em MATLAB [11].

No teste realizado, o objetivo foi avaliar o método proposto, verificando a eficiência, precisão do diagnóstico em relação a diferentes conjuntos de limites detectores. Foram gerados três conjuntos de detectores benignos, sendo os conjuntos I, II e III que possuem 30, 60 e 90 padrões detectores, respectivamente. Os conjuntos de detectores gerados utilizam 10%, 20% e 30% das amostras normais, que possuem um total de 300 amostras. A Taxa de afinidade é definida com o valor TAf = 50%. Na tabela 2 apresentam-se os resultados obtidos pelo sistema de diagnóstico.

Tabela 2 - Resultados obtidos pelo método.

Diagnóstico	Conjunto de limites detectores		
	I	*II*	*III*
Amostras testadas	600	600	600
Classificações Normais	368	329	302
Classificações Invasão	232	271	298
Acerto (%)	77,33%	90,33%	99,33%

DOI: 10.5540/03.2014.002.01.0015

Neste teste, foi possível observar que o sistema de diagnóstico apresenta um bom desempenho e que a quantidade de limites detectores influencia diretamente o diagnóstico final. Desta forma sugere-se utilizar o conjunto *III* de limites detectores, pois à medida que a quantidade de detectores aumenta, o diagnóstico se torna mais preciso, isto porque quanto mais conhecimento, mais eficiente é o processo de diagnóstico.

7 Conclusão

Neste artigo foi apresentado um método para detecção de intrusos em redes de computadores utilizando um algoritmo imunológico de seleção negativa. O algoritmo proposto apresentou excelentes resultados obtendo um índice de acerto de 99,33% de acerto em todos os sinais analisados. A fase de geração de detectores é executada de forma *off-line* não acarretando prejuízo ao algoritmo. A fase de monitoramento é realizada rapidamente, com tempo inferior a 100 milésimos de segundo, proporcionado rapidez na tomada de decisão. Desta forma, conclui-se que o sistema de detecção de intrusos proposto, é bastante eficiente, confiável, robusto e seguro, ressaltando a qualidade dos sistemas imunológicos artificiais.

Agradecimentos

Os autores agradecem a CAPES e a FAPESP (Proc. Nº 2011/06394-5) pelo apoio financeiro de pesquisa.

Referências

[1] K. Anchor; P. Williams; G. Gunsch and G. Lamont. The computer defense immune system: current and future research in intrusion detection. Evolutionary Computation, 2002, pp. 1027-1032, (2002).

[2] U. Aickelin; J. Greensmith and J. Twycross. Immune system approaches to intrusion detection - a review. In 3rd International Conference on Artificial Immune Systems, pp. 316–329, (2004).

[3] D. W. Bradley and A. M. Tyrrell. Immunotronics - Novel Finite-State-Machine Architectures with Built-In Self-Test Using Self-Nonself Differentiation. IEEE Transactions on Evolutionary Computation.Vol. 6, pp. 227–238 (2002).

[4] D. Dasgupta. "Artficial Immune Systems and Their Applications". Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1998.

[5] G. Dozier; D. Brown; H. Hou and J. Hurley. Vulnerability analysis of immunity-based intrusion detection systems using genetic and evolutionary hackers. Applied Soft Computing, pp. 547–553, (2007).

[6] L. N. de Castro. "Engenharia Imunológica: Desenvolvimento e Aplicação de Ferramentas Computacionais Inspiradas em Sistemas Imunológicos Artificiais". Tese de Doutorado, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, Brasil, 2001.

[7] S. Forrest and S. Hofmeyr. Engineering an immune system. In Graft, volume 4:5, pp. 5-9, (2001).

[8] S. Forrest; A. Perelson; L. Allen and R. Cherukuri. Self-Nonself Discrimination in a computer, Proc. do IEEE Symposium on Research in Security and Privacy, pp. 202-212 (1994).

[9] J. Kim; P. J. Bentley; U. Aickelin; J. Greensmith; G. Tedesco and J. Twycross. Immune system approaches to intrusion detection — a review. Natural Computing: an international journal, pp. 413–466, (2007).

[10] F. P. A. Lima. "Análise de Distúrbios de Tensão em Sistemas de Distribuição de Energia Elétrica Baseada em Sistemas Imunológicos Artificiais", Dissertação de Mestrado, UNESP, UNESP, Univ Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Ilha Solteira, Março-2013, 169 p.

[11] Matlab (2011). 7.8 Version, Mathworks Company.

[12] G. C. Silva. Detecção de Intrusão em redes de Computadores: Algoritmo imunoinspirado baseado na teoria do perigo e célula dendríticas. Dissertação de Mestrado em Engenharia elétrica, UFMG – Universidade Federal de Minas Gerais, 136 pp., Minas Gerais, Brasil, 2009.

[13] T. Verwoerd and R. Hunt. Intrusion detection techniques and approaches. Computer Communications, pp. 1356–1365, (2002).

