Algoritmo Imunoinspirado Aplicado a Segurança Computacional

Thiago Giroto Milani, Fabricio Aparecido Breve
Universidade Estadual Paulista "Julho de Mesquita Filho"- UNESP
Rio Claro, Brasil
tmilani@rc.unesp.br, fabricio@rc.unesp.br

***Resumo*—Com o grande crescimento da área de informática e inovação tecnológica (era digital) cresce cada vez mais a necessidade de dispositivos e algoritmos capazes de aprender e reconhecer padrões. Segurança computacional se torna cada vez mais essencial com toda essa evolução, pois assim como a tecnologia cresce, os incidentes de segurança crescem duas vezes mais rápido. Com isso surge a necessidade de integrar essas duas vertentes da evolução, inteligência computacional e segurança de computadores, trazendo dispositivos e ferramentas capazes de reconhecer padrões de incidentes de segurança através da inteligência computacional.**

Área: Inteligência Computacional

I. Introdução

Recentemente vemos um grande avanço na utilização de algoritmos e modelos computacionais para resolver problemas ligado a biologia. Isso influenciou o crescimento de pesquisas na área de biologia computacional e bioinformática, sendo cada vez mais frequente a criação de grupos e eventos internacionais e nacionais ligados ao assunto. Conforme comentado por [5]

Cada vez mais os usuários de computador têm-se deparado com problemas mais sérios de segurança de computadores e redes. Com o crescimento da internet desde sua criação, e cada vez mais serviços e aplicações para ela, acabou sendo um bem essencial, e de extrema necessidade, trazendo assim mais destaque para pessoas mal-intencionadas disseminar vírus e *malware* com intenção de roubar ou atacar algum usuário ou empresa. São cada vez mais comuns notícias de invasão de sites.

Existem várias ferramentas de detecção de intrusão no mercado, porém poucas incorporam técnicas de aprendizado para o aprimoramento automático. Atualmente as ferramentas disponíveis em geral apresentam problemas de desempenho e são principalmente baseadas em comparação em assinaturas com banco de dados já existentes ou gerados pelo sistema.

Para se obter um maior desempenho é preciso uma maior base de dados de ataques, porém com um grande custo em eficiência. Outro grande problema com essas ferramentas é o grande número de falsos positivos gerados.

Além de já trabalhar com segurança computacional a algum tempo, com experimentos utilizando *honeypot* uma motivação pessoal para este artigo é a grande quantidade de ataques e mensagens de spam que são disseminados todos os dias, além dos recentes acontecimentos em escala global como o *malware wannacry*, o qual ocasionou a paralisação de diversos serviços essenciais totalmente dependentes da tecnologia e internet.

O objetivo da pesquisa é analisar algoritmos de segurança computacional imunoinspirados. Especificamente à pesquisa de algoritmos imunoinspirados aplicados a análise, classificação e reconhecimento de padrões em mensagens de *spam*.

II. Conceitos e técnicas

A.Detecção e Contenção de Redes de Computadores

Os sistemas de detecção de intrusão mais conhecidos são os *IDS* (*Intrusion Detection System*) que segundo [4] podem ser divididos da seguinte forma:

HIDS – Host-Based Intrusion Detection System: Monitora o sistema utilizando informações locais, como arquivos de *logs* ou agentes de auditoria. Ele pode ser capaz de monitorar acessos e alterações em arquivos e processos no sistema, entre outros aspectos. Exemplos de HIDS são o *Tripewire*, o *AIDE*, *OSSEC* e o *Sentrytools*.

NIDS – Network-Based Intrusion Detection System: Monitora o tráfego da rede, geralmente utilizando a interface da rede em modo promíscuo, como se fosse um *sniffer*. Exemplo de NIDS são o *Snort* e o *AAFID*.

Hybrid IDS – Hybrid Intrusion Detection System: Utiliza monitoração do sistema e de redes ao mesmo tempo para prevenir ataques. Com isso se tem o melhor dos sistemas HIDS e NIDS. Exemplo nessa categoria é o *Prelude*.

B.(SIAs) Inspirados na Teoria da Redes Idiotípica

Os algoritmos de rede idiotípica baseiam-se no processo de regulação imune proposto a partir das ideias apresentadas em [10]. Existem diversos algoritmos inspirados na rede idiotípica, um dos mais conhecido é o aiNet [11]. Conforme mostrado na imagem a baixo. As características dessa classe de algoritmos os tornam adequados para problemas envolvendo clusterização e reconhecimento de padrões.

VII Workshop do Programa de Pós-Graduação em Ciência da Computação: "Interação entre Academia e Empresa", Unesp, Rio Claro, 14 e 15 de setembro de 2017.

```
1. Inicialização:  crie uma população inicial aleatória de anticorpos da
   rede;
2. Apresentação antigênica:  para cada padrão antigênico, faça:
   2.1 Seleção e expansão clonal:  para cada elemento da rede, determine
       sua afinidade com o o antígeno apresentado.  Selecione um número
       de elementos de alta afinidade e reproduza-os (clonalmente)
       proporcionalmente à afinidade;
   2.2 Maturação de afinidade:  aplique mutação a cada clone de forma
       proporcionalmente inversa à sua afinidade.  Selecione novamente um
       número de clones com alta afinidade e coloque-os em um conjunto de
       memória clonal;
   2.3 Interações clonais:  determine as interações da rede (afinidade)
       entre os elementos do conjunto de memória clonal;
   2.4 Supressão clonal:  elimine os clones de memória cuja afinidade
       seja inferior a um dado limite pré-especificado.
   2.5 Metadinâmica:  elimine todos os clones de memória cuja afinidade
       com o antígeno é inferior a um determinado limite;
   2.6 Construção da Rede:  incorpore os clones restantes da memória
       clonal com a rede de anticorpos;
   2.7 Interação da Rede:  determine a similaridade entre cada para dos
       anticorpos da rede;
   2.8 Supressão da Rede:  elimine todos os anticorpos da rede cuja
       afinidade seja inferior a um dado limite;
3. Ciclo:  repita o passo 2 até que uma dada condição de parada seja
   satisfeita.
```

Fig. 1. Pseudo Código de SIAs Inspirado na Rede Idiotípica

Nesse trabalho os autores desenvolvem um classificador a partir de um sistema dinâmico não-linear baseado em uma rede de anticorpos modelado por equações diferenciais.

III. METODOLOGIA DE DESENVOLVIMENTO

Segundo [3], a ideia de utilizar SIAs em segurança de computadores surgiu de forma relativamente precoce, durante a evolução dos estudos em SIAs. Inicialmente as preocupações eram diferentes e os estudos focados em outras áreas.

Uma grande visão de SIAs para detecção de intrusão pode ser encontrada em [15]. Dois fatos observados por esses autores na época da publicação foram: i) todos os trabalhos avaliados por eles eram baseados em modelos com distinção *self* X *nonself*; ii) os trabalhos em sua grande maioria eram em seleção negativa.

Obviamente, novas abordagens surgiram após as publicações, porém "IDS Imunoinspirados" ainda têm muito espaço para crescer e muitas áreas a serem exploradas.

A detecção de SPAM utilizando SIAs ainda é pouco explorada. O primeiro modelo conhecido para classificação de mensagens de e-mail utilizando SIA foi proposto em [16]. O algoritmo atribui um peso para cada detector (linfócito), que é incrementado quando ocorre o reconhecimento do *spam* e decrementa em caso de mensagens legítimas. Conforme [3] aplicado a um conjunto de 1200 mensagens, conseguiu identificar 90% de *spam* e 99% das mensagens legítimas, após um treinamento de 1600 mensagens de *spam* e 1200 mensagem legítimas.

Outros trabalhos mais recentes, conseguiram índices maiores que 99% conforme mostrado em [3].

IV. CONSIDERAÇÕES FINAIS

Por fim o trabalho visa o desenvolvimento de um algoritmo baseando em sistemas imunológicos artificiais inspirado na rede idiotípica para a classificação e reconhecimento de padrões em mensagens de *spam*, tendo como principal comparativo para os experimentos o algoritmo e testes mencionado no artigo, "Algoritmos Imunoinspirados Aplicados em Segurança Computacional: Utilização de Algoritmos Inspirados no Sistema Imune para Detecção de Intrusos em Redes de Computadores" de J. Q. Uchôa (2009).

REFERÊNCIAS

1. S. Forest, S. A. Holfmeyr, A. Somayaji, "Computer Imunology" Comunications of ACM, Vol. 40, ed. 10, pag. 88 – 96, 1997;
2. S. Forest, A. S. Perelson, L. Allen, R. A. S. Cherukuri, "Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy.", Los Angeles: IEEE Computer Society Press 1994, p. 202 – 12;
3. J. Q. Uchôa, "Algoritmos Imunoinspirados Aplicados em Segurança Computacional: Utilização de Algoritmos Inspirados no Sistema Imune para Detecção de Intrusos em Redes de Computadores" UFMG – Belo Horizonte, Tese de Doutorado em Bioinformática, 2009;
4. E. T. Nakamura, P. L. Geus "Segurança em Redes" São Paulo: Berkeley, 2002;
5. H. Kitano, "Conputatinal Systems Biology" Nature, v. 420, p. 206 – 210, 2002;
6. H. M. Nussenzveig "Introdução a Complexidade" In H. M. Nussensveig (ed) "Complexidade e Caois" Rio de Janeiro UFRJ/Copeo, 2003
7. N. Petrovisky, V. Brusc "Computacoinal Imunology: The comming of age", Immunol Cell. Bio, vol. 80, n 3, p. 54 – 248, 2002;
8. A. K. Chakraborty, L. M. Dustin, A. S. Shawn, "Silico Models for Cellular and Molecular Immunology: Successes, Promises and Chalenges", Nature Immunology, v4, n. 10, p. 6 – 933, 2003;
9. J. D. Farmer, N. Peckerd, A Perlson, "The Imune System, Adaptation and machine learning", Physica D, v. 22, p. 187 – 204, 1986;
10. N. K. Jerne, "Twards a Network Theory Of The Immune System. Ann. Immunol." Inst. Pasteur, v. 125, n. 1-2, p. 373 – 89, 1974;
11. L. N. De Castro, J. F. Zuben, "An Evolutionary imune network for data clustering" In Proc. Of the IEEE SBRN (Brazilian Symposium on Artificial Neural Networks). Rio de Janeiro: SBRN, 2000, p. 84 – 89;
12. L. N. De Castro, J. F. Zuben, "Learning and optimization using the clonal selection principle", IEEE Transaction on Evolution Computation Special Issue on Artificial Immune Systems, IEEE, v. 6, p. 239 – 251, 202;
13. A. K. Abbas, A. H. Lichtman, J. S. Pober, "Imunologia Celular e Molecular" 4. ed. Rio de Janeiro, 2003;
14. J. Greensmith, U. Aickelin, S. Cayzer, "Introducing Dendritic Cells as Noval Immune-Inspired Algorithim for Anomaly Detection." In: Proceeding of the 4th Internation Conference on Artificial Immune System (ICARIS 2005). Banff, Canada. Springer – Verlag, 2005. (Lincs, 3627), p. 153 – 167;
15. U. Aickelin, J. Greensmith, J. Twycross, "Immune System Aproaches to Intrusion Detection" – a review. In G. Nicosia, V. Cutello, P. J. Bentley, J. Timmis. (Ed.) Artificial Immune Systens, Third International Conference, ICAIS 2004, Catarina, Sicily, Italy, September 13-16, 2004. Catarine Springer, 2004. (Lecture Notes in Computer Science, v. 3239), p. 316 – 329;
16. T. Oda, T. White, "Increasing the Accuracy on a Spam-Detecting Artificial Immune System". In: Proceedings of the Congress on Evolutionary Conputation (CEC 2003), Canberra, Autralia, Decenber, 2003, Australia: IEEE, 2003, v.1, p. 390 – 396;