Inteligencia Artificial 51 (2013), 1-8

INTELIGENCIA ARTIFICIAL

http://journal.iberamia.org/

Aplicación de técnicas de Inteligencia Artificial en la Seguridad Informática: un estudio

Adrian Hernández Yeja y Jenny de la Rosa Pasteur y Odaysa Rodríguez Huice

Universidad de las Ciencias Informáticas
Carretera a San Antonio, KM 2 1/2, Boyeros, La Habana, Cuba
{ayeja,jdelarosa,ohuice}@uci.cu

Abstract Information Security is evolving and dynamic. Application of Artificial Intelligence techniques becomes an essential practice in the treatment and detection of threats to which organizations are exposed. This article focuses on a literature review concerning the application of AI techniques in computer security, with emphasis on Intrusion Detection Systems, detection of unwanted mail or spam, antivirus and other applications where the use of Artificial Intelligence is considered important.

Resumen La Seguridad Informática se encuentra en constante evolución y dinamismo. La aplicación de técnicas de Inteligencia Artificial se convierte en una práctica indispensable en el tratamiento y detección de amenazas a que se encuentran expuestas las organizaciones. Este artículo se enfoca en un estudio bibliográfico relacionado con la aplicación de técnicas de Inteligencia Artificial en la Seguridad Informática, enfatizando en los Sistemas Detectores de Intrusos, detección de correo no deseado o spam, antivirus, así como otras aplicaciones en las que la utilización de la Inteligencia Artificial se considera importante.

Keywords: Information Security, Artificial Intelligence, Intrusion Detection Systems, spam, antivirus.
Palabras clave: Seguridad Informática, Inteligencia Artificial, sistemas de detección intrusos, spam, antivirus.

1 Introducción

La Seguridad Informática se ha convertido en una cuestión indispensable en la sostenibilidad y desarrollo de cualquier organización, pues la información en la mayoría de los casos tiene un valor inestimable. El término Seguridad Informática tiene en cuenta 3 principios fundamentales que lo sustentan y que deben ser la base de cualquier sistema informático [1]: confidencialidad, integridad y disponibilidad.

En la actualidad, son variadas las formas en que se encuentran expuestos los datos a los ataques producto de vulnerabilidades presentes en los sistemas, por lo que las alternativas para enfrentar tal situación se han perfeccionado a lo largo de los años y de muy diversas formas. En este sentido, la Inteligencia Artificial ha demostrado una probada aplicación en diferentes áreas de la Seguridad Informática como su utilización en redes mediante la detección de intrusos y bloqueo de correos no deseados o spam, análisis forense, antivirus, etc., lo que sin duda ha permitido un elevado nivel de desempeño de las organizaciones en vista a la protección de la información. Las técnicas de Inteligencia Artificial dan apoyo a sistemas generales que operan automática, adaptativa y proactivamente [2].

En este artículo se pretende realizar un estudio de técnicas fundamentales de Inteligencia Artificial aplicadas a áreas sensibles de la Seguridad Informática. La estructura del documento se describe a continuación: en la sección 2 se presentan aplicaciones de técnicas de Inteligencia Artificial en los Sistemas Detectores de Intrusos o IDS; en

ISSN: 1988-3064(on-line)

la sección 3 se trata igualmente el correo no deseado o spam; en la sección 4 se analizan otras aplicaciones interesantes. Por último se brindan las conclusiones de la investigación.

2 Sistemas Detectores de Intrusos (IDS)

La detección de intrusos se ha convertido en parte integral de los procesos de seguridad de la información desde que ellos pueden implementar y administrar controles identificados de la seguridad de la información [3]. Son variadas las técnicas de Inteligencia Artificial las que se han aplicado en estos sistemas informáticos, en todos los casos se busca la optimización y detección más eficaz de intrusiones. La Inteligencia Artificial puede reducir el esfuerzo humano requerido para construir Sistemas Detectores de Intrusos y puede mejorar su rendimiento [4].

J. Frank realiza un análisis en [4] con respecto a los IDS en áreas fundamentales como la clasificación (proceso de identificar atacantes e intrusos) y la reducción de datos (análisis de una colección de datos para identificar sus componentes más importantes). Se discuten métodos de Inteligencia Artificial que son aplicados a estas áreas fundamentales de los IDS.

En [5] se plantea el progreso en la creación de la implementación de un Sistema Basado en Casos (CBS) utilizando el conocido IDS Snort, el cual consta por defecto de un sistema basado en reglas. Se plantean las limitaciones del sistema que presenta el mismo como son las molestas alertas que constantemente brinda y cómo el SBC puede ser utilizado como una técnica sofisticada que mejora las dificultades de la herramienta de seguridad.

El estudio que se realiza en [6] se enfoca en otras técnicas de Inteligencia Artificial aplicada a los IDS como son las Máquinas de Vectores de Soporte (SVMs), Redes Neuronales Artificiales (ANNs), Regresión Multivariada Adaptativa utilizando Splines (MARS) y Programas Genéticos Lineales (LGPs). Se establecen comparaciones críticas basadas en experimentos realizados de parámetros esenciales en los IDS en cuanto a la precisión, tiempo de formación y tiempo de prueba de los mismos, utilizando las técnicas de Inteligencia Artificial anteriormente descritas. Los resultados finales de la investigación fueron interesantes, pues permiten realizar un análisis en torno a la efectividad en la aplicación de las técnicas que se estudiaron:

- LGPs superó a MARS, SVMs y ANNs en términos de detección precisa a expensas del tiempo.
- MARS fue superior a SVMs con respecto a la clasificación de las clases más importantes (acceso no autorizado a privilegios de súper usuario y acceso no autorizado a máquinas remotas) en términos de severidad del ataque.
- SVMs superó a ANNs en importantes aspectos de escalabilidad (SVMs puede trabajar con un gran número de patrones, mientras que ANNs toma un gran tiempo en lograr o fallar en cuanto a convergencia si el número de patrones tiende a crecer); SVMs funciona en orden de magnitud más rápido.

Otro estudio comparativo de diferentes técnicas de Inteligencia Artificial aplicadas a los IDS desde el punto de vista de rendimiento en Redes Neuronales se presenta en [7], basándose en nueve clasificaciones de las mismas: Multicapa Perceptrón (MLP), Redes Neuronales Modulares (MNN), Redes Recurrentes (RN), Feed Forward Generalizado (GFF), Redes Jordan/Elman (JEN), Redes de Análisis de Componentes Principales (PCA), Función Base Radial (RBF), Mapas Auto Organizados (SOM), Redes Recurrentes de Tiempo Rezagado (TLRNs). Se presentan los resultados de los experimentos realizados, resaltando cómo MNN, MLP y MNN obtuvieron los mejores resultados.

En [8] se realiza otro estudio relacionado con las Redes Neuronales, en este caso del tipo supervisada para la detección de ataques remotos a locales (R2L). Los experimentos realizados indican que la técnica utilizada tiene comparativamente una baja tasa de falsos positivos (detección de amenazas que no representan un problema de seguridad) y falsos negativos (no detección de amenazas), de vital importancia estos aspectos en la calidad de cualquier sistema computacional. Además la solución se considera óptima en relación a la literatura consultada por los autores.

Una metodología para aplicar Algoritmos Genéticos en IDS se discute en [9], en especial para la detección de complejos comportamientos anómalos. Se describen algunos factores que afectan a los Algoritmos Genéticos en su aplicación con los IDS, así como las limitaciones de los Sistemas Basados en Reglas que presentan

comúnmente estas aplicaciones informáticas. La propuesta incluye una combinación de Algoritmos Genéticos con Sistemas Basados en Reglas, en donde los primeros pueden ser utilizados para generar reglas que se correspondan solo con conexiones anómalas.

Una novedosa técnica para la detección de intrusiones mediante el uso de la teoría Rough Set[1] se presenta en [11], vinculado con Algoritmos Genéticos (aprovechando que la vinculación de ambos métodos es una alternativa probada y conocida de Minería de Datos para el análisis de la información), todo en combinación con Redes Neuronales Artificiales finalmente. Rough Set y los Algoritmos Genéticos se aplican para buscar el conjunto de datos reducidos, luego, los resultados se utilizan por una Red Neuronal Supervisada en el IDS.

Por otro lado, en [12] se propone un modelo de detección proactiva y modelo dinámico basado en el Análisis de Tendencias, Lógica Difusa y Redes Neuronales, los que pueden ser utilizados en los IDS por parte de las organizaciones. El estudio se focaliza en que el comportamiento de los intrusos puede ser agrupado en fases comunes genéricas de la intrusión y que todas las acciones de los usuarios pueden ser monitorizadas en términos de estas fases. De igual forma, este estudio se centra en la detección híbrida de intrusiones: anómalas (construcción de perfiles de comportamiento normal de los usuarios) y de mal uso (representación específica de patrones en intrusiones). Se destacan 2 componentes de bajo y uno de alto nivel. El primer componente de bajo nivel se denomina motor difuso y es el que implementa el enfoque de la mala detección. Este componente difiere de estudios anteriores en que la mala detección no se realiza buscando patrones particulares de ataques sino que busca malas detecciones generales de recursos y objetos. El segundo componente de bajo nivel se denomina motor neuronal e implementa el enfoque en la detección anómala. El componente de alto nivel muestra las salidas de los 2 motores de bajo nivel.

Matti Manninen en [13], compara soluciones de Inteligencia Artificial aplicadas a los IDS con respecto a soluciones tradicionales en los mismos, analizando cómo las que son basadas en Inteligencia Artificial pueden ser más eficaces. Se reflejan diferentes técnicas de Inteligencia Artificial que pueden ser utilizadas en los mismos, entre ellas: Lógica Difusa, Razonamiento Probabilístico, Redes Neuronales y Algoritmos Genéticos. Se hace constatar que las Redes Neuronales son la alternativa más popular en su utilización en los IDS como técnica de Inteligencia Artificial, también se señala que las alternativas basadas en Inteligencia Artificial son más precisas y fáciles de configurar con respecto a las técnicas tradicionales.

La Minería de Datos también aporta muchos elementos en los IDS. Esto se demuestra en [14] , donde se analiza la combinación de la Minería de Datos con otras formas de aprendizaje de las computadoras. En [15] se realiza un estudio profundo de técnicas de Minería de Datos aplicadas a los IDS, en donde se refleja la aplicación de la misma a tablas sencillas de base de datos relacionales. Otros estudios interesantes e intensivos en este aspecto se encuentran en [16] [17] y [18].

Varun Chandola y otros autores ponen de manifiesto en [19] la aplicación de una suite de algoritmos de Minería de Datos denominada MINDS (Minnesota Intrusion Detector System) en un IDS. Los módulos de la suite incluyen varios elementos para coleccionar y analizar gran cantidad de tráfico de red, se incluye la detección de comportamiento anómalo, resúmenes y detección de escaneos. Según los autores, la clave del desafío en el diseño de un método de Minería de Datos en una aplicación concreta reside en la necesidad de integrar el conocimiento experto en el método. En base a este pensamiento se diseñó MINDS.

3 Correo no deseado (Spam)

El correo spam se ha convertido en un problema de seguridad serio en los últimos años debido a entre otras muchas razones por su capacidad de consumo excesivo de recursos computacionales que requiere su procesamiento. Se han creado variados métodos para eludir las aplicaciones anti-spam. Como una alternativa eficiente y probada a este problema, las técnicas de Inteligencia Artificial han permitido el enfrentamiento al mismo. Las investigaciones en este sentido corroboran el progreso científico que han tenido las aplicaciones anti-spam en el mundo informático.

[1] Herramienta formal para el modelado y procesamiento de información incompleta de la información de los sistemas [10]. Esta herramienta es muy útil en análisis de datos y generación de reglas [11].

Una revisión general de sistemas inteligentes utilizados en la detección y filtrado de correo spam se realiza en [20], donde se resaltan modelos basados en la colaboración de usuarios y modelos basados en el análisis de contenido. Se analiza la complejidad de la detección de spam y se analizan aproximaciones empleadas en la detección de spam basadas en distintas heurísticas o en la observación concreta de atributos extraídos de los correos electrónicos. Se destacan técnicas como Naïve Bayes y algunas de sus variantes, el cual es uno de los algoritmos más conocidos propuesto para la clasificación de textos mediante modelos de aprendizaje automático. Otra de las técnicas para la detección de spam que se analiza son las SVM, las que son especialmente apropiadas para problemas de categorización de texto y han sido utilizadas con éxito en el ámbito de la detección y filtrado de correos spam. También se enfocan otras técnicas como Boosting de Árboles de Decisión, Ripper y Rocchio (basado en reglas), Chung Kwei (basada en patrones de reconocimiento), ECUE (modelo para la detección de correo spam que hace uso de un sistema de razonamiento basado en casos), Indexado por Semántica Latente y SpamHunting (sistema de razonamiento basado en instancias).

Una técnica de extracción de características en correos para la detección de spam basada en Sistemas Artificiales Inmunes y Redes Neuronales con Backpropagation se presenta en [21]. Cuando las características son extraídas, se usan como entrada al modelo de detección spam, que presenta una Red Neuronal. Los resultados experimentales del estudio son excelentes y demuestran la validez y rigor investigativo realizado.

En [22] se propone un enfoque para la detección de spam basado también en Sistemas Artificiales Inmunes vinculado con SVM. Con la utilización de estas técnicas se dota al sistema de la capacidad de ser dinámico y adaptativo, lo que permite cambiar el entorno de búsqueda de spam de acuerdo a las necesidades de la organización.

Manjusha y Rakesh en [23] combinan las redes bayesianas y las neuronales para la detección de spam. Las Redes Neuronales son entrenadas mediante un Algoritmo Genético.

4 Antivirus

La aparición de nuevos códigos malignos exige un constante proceso de actualización de las grandes bases de firmas de los antivirus, en los que se está acercando el momento en que se haga insostenible la enorme cantidad de información que se procesa por los motores de búsqueda. El desarrollo de sistemas antivirus, vinculado con la Inteligencia Artificial, ha abierto un nuevo marco en el desarrollo de los mismos, con la aplicación de técnicas novedosas que optimizan y agilizan la búsqueda y eliminación de programas malignos.

Las técnicas fundamentales de la Inteligencia Artificial que se emplean en los sistemas de detección de virus están enfocadas en [24]:

- Tecnología heurística (el primero y más importante campo de aplicación).
- Técnicas de Minería de Datos.
- Redes Neuronales Artificiales.
- Tecnología Agente.
- Tecnología Artificial Inmune.

En [25] se realiza una descripción y aplicación práctica de técnicas de aprendizaje de los sistemas detectores de virus, en especial para los del tipo metamórficos[2] que necesitan técnicas avanzadas de detección al límite para su reconocimiento.

Un estudio realizado en torno a la detección de gusanos informáticos utilizando técnicas de Inteligencia Artificial se presenta en [26]. Los autores reflejan la aplicación de las Redes Neuronales Artificiales en la detección de estas peligrosas aplicaciones informáticas en ambientes del Sistema Operativo Microsoft Windows®, aprovechando las ventajas de las mismas en la búsqueda de patrones en problemas altamente no lineales y su rápida clasificación. Se demuestran las ventajas computacionales en ambientes en tiempo real de las Redes

[2] Es un tipo de virus informático que varía su estructura completamente mediante la utilización de técnicas de ofuscación de código para mutar por sí mismos.

Neuronales Artificiales con respecto a otros métodos de detección de gusanos informáticos. Otra investigación relacionada con la búsqueda de gusanos informáticos desconocidos pero con la utilización de Minería de Datos se discute en [27], en donde el reconocimiento de códigos malignos no se realiza necesariamente mediante instancias de códigos malignos sino a través de métricas en el ordenador a escanear. En [28] también se utiliza la Minería de Datos para la detección de códigos malignos; se diseña un framework o marco de trabajo que encuentra patrones en un conjunto de datos y los utiliza para detectar nuevos binarios malignos. Los resultados del estudio demostraron tasas de detección que duplicaron las de métodos de detección de ejecutables malignos con métodos tradicionales.

Un novedoso método de detección de virus, basado en la técnica Razonamiento Basado en Casos se presenta en [29], en la cual se manifiesta como principales ventajas del sistema la detección de virus que no existan en la base de firmas, así como la actualización del antivirus, para el cual no es necesaria su conexión a Internet. Aunque el procedimiento no es comparable aún con métodos tradicionales de detección de virus, marca un hito en la utilización de la técnica CBS en el ambiente de detección genérica de virus.

5 Otras aplicaciones

Aunque se han expresado en ideas anteriores algunas de las aplicaciones más comunes de las técnicas de Inteligencia Artificial en la Seguridad Informática, existen otros campos de utilización sensibles en los que los algoritmos de Inteligencia Artificial son imprescindibles y útiles.

En [30] se presenta y evalúa un Algoritmo Genético basado en el enfoque heurístico de posibilitar a las organizaciones la posibilidad de elegir el perfil de seguridad mínimo tratando de cubrir el mayor número posible de vulnerabilidades que existen en la misma. Esta investigación permite el conocimiento de las particularidades desde el punto de vista de vulnerabilidades que presenta determinada organización y no como se trata en la mayoría de los casos, en donde se estudian vulnerabilidades específicas o basadas en otros entornos que no aplican a las necesidades o peculiaridades de la entidad. Otro estudio relacionado con el control de la seguridad de las organizaciones se discute en [31]. Se presenta una arquitectura y diseño de un sistema inteligente de administración de la Seguridad Informática para la monitorización, control y toma de decisión, permitiendo la construcción de un sistema experto capaz de tener el conocimiento acerca de amenazas, políticas, procedimientos y riesgos de la organización. Esta propuesta incluye la conjugación de diferentes técnicas de Inteligencia Artificial trabajando armónicamente. El sistema tiene la capacidad de ser adaptativo y capaz de descubrir y construir nuevos conocimientos relacionados con el dominio de la Seguridad Informática. De forma similar en [32] se presenta un sistema para capturar, compartir y reusar el conocimiento de seguridad en una organización, mediante la utilización de un sistema basado en casos; en la propuesta, cuando se necesita resolver algún flujo de seguridad en cualquier fase del desarrollo de software (análisis, diseño, implementación, pruebas), se realiza una consulta a la base de conocimientos del sistema en busca de similitudes en la misma que puedan resolver el problema a resolver. El ciclo de vida del conocimiento incluye 3 fases: creación, retención y uso del conocimiento.

En la seguridad VoIP (Voice over Internet Protocol), la Inteligencia Artificial también enfoca la aplicación de sus técnicas como analizan los autores en [33]. Se expresa la combinación de 2 métodos para la seguridad de llamadas sobre VoIP (Voice over Internet Protocol). Uno de los métodos es un esquema de autenticación con contraseña remota para voz sobre el protocolo que utiliza Redes Neuronales. Este esquema permite que el servidor no almacene o mantenga la contraseña o tabla de verificación. El servidor solo almacena los pesos de clasificación de la red. Esto permite que el servidor pueda autenticar la validez del usuario en tiempo real. El otro método consiste en el uso del algoritmo criptográfico AES para encriptar y desencriptar los paquetes de voz.

La identificación de vulnerabilidades es un aspecto importante en la Seguridad Informática, pues permite el tratamiento proactivo a las amenazas a las que se exponen los usuarios u organizaciones. La Inteligencia Artificial también ayuda en este aspecto. En [34] se presenta un método para la identificación de vulnerabilidades en programas ejecutables mediante análisis Fuzzy[3]. Se utilizan 2 procedimientos, en el primero se combinan el análisis estático y dinámico para obtener el comportamiento general, interfaz y regiones de interés del código. Luego se utiliza un Algoritmo Genético para dirigir de forma inteligente la generación de los datos de prueba y

[3] Técnica de caja negra que realiza pruebas en la entrada del software mediante la generación de datos aleatorios.

mejorar el objetivo de la prueba. Por otro lado, en [35] se realiza una investigación relacionada con la protección de aplicaciones Web, específicamente hacia las inyecciones SQL (SQLi) utilizando Redes Neuronales Artificiales. El estudio puede ser aplicado igualmente hacia la protección contra XSS (Cross Site Scripting) y otros tipos de vulnerabilidades del tipo inyección de flujo. En la propuesta se utilizan 2 fases: fase de entrenamiento y fase de trabajo. En la primera se utiliza un conjunto de datos normales y maliciosos para el entrenamiento de la red neuronal con Matlab®. Luego de entrenada la red neuronal se integra con un Firewall de Aplicación Web (WAF) para proteger aplicaciones web durante la fase de trabajo.

La seguridad en redes es un tema recurrente en cualquier ámbito de la Seguridad Informática. Liu y Man en [36] utilizan Redes Bayesianas (RB) para la modelación de vulnerabilidades en redes y determinación cuantitativa del nivel de seguridad de las redes. En este estudio las RB se utilizan para modelar todos los pasos de un ataque potencial atómico en la red. Cada vértice representa una propiedad única de violación del estado de seguridad y cada arista corresponde a una explotación de uno o más vulnerabilidades expuestas. Los pesos de las aristas corresponden la probabilidad de explotar una vulnerabilidad. Otra investigación que trata el tema de la seguridad en redes utilizando Redes Bayesianas pero del tipo dinámica se presenta en [37], donde se realiza una investigación para desarrollar coherentes, lógicas y aplicables métricas de seguridad para redes de computadoras, en la que se incorporan factores temporales relevantes como la disponibilidad de códigos explotables o parches en un grafo de ataque basado en métricas de seguridad. El modelo está asociado con el estándar de puntuaciones CVSS (Common Vulnerability Scoring System), con el fin de que el modelo pueda llevar a un conocimiento aplicable. El trabajo se apoya en la hipótesis de que las amenazas que puede poseer una vulnerabilidad pueden cambiar con el tiempo y más en ambientes dinámicos de redes.

La utilización de la encriptación e Inteligencia Artificial se vinculan en [38]. Se propone un mecanismo de encriptación asimétrica basado en Redes Neuronales Artificiales. En este sentido el esquema de creación de llave pública se basa en una Red Neuronal Multicapa que utiliza el algoritmo Backpropagation. El esquema de encriptación y creación de llave privada se basa en el álgebra booleana.

El análisis forense como ciencia que se encarga de descubrir fuentes de violaciones de seguridad de la información también se acopla a las aplicaciones de la Inteligencia Artificial por sus características de procesamiento denso y confuso de datos. En [39] se analizan RNA y SVM en una herramienta de análisis para garantizar la seguridad de la información mediante la actualización de las brechas de seguridad recientemente identificados. Se demuestra que las SVM son superiores a las RNA para el análisis forense en la red, en cuanto a escalabilidad, tiempo de entrenamiento, tiempo de ejecución y precisión de predicción. También se trató el tema relacionado de la clasificación de la importancia de las características de entrada. Se presentan 2 métodos para la clasificación de características, el primero es independiente de la herramienta de modelado, mientras que el segundo método es específico para SVM.

6 Futuro de la aplicación de técnicas de Inteligencia Artificial en la Seguridad Informática

El futuro de la Inteligencia Artificial aplicada a la Seguridad Informática se torna interesante y necesario. Los modernos programas maliciosos se convierten en un desafío informático que necesita un procesamiento inteligente de grandes volúmenes de datos no estándares. Los ataques se profesionalizan cada vez más y la Inteligencia Artificial representa el medio ideal para enfrentar tales problemas.

Las tendencias cibercriminales son cada vez más peligrosas y sofisticadas. Se plantea la necesidad de utilizar sistemas detectores de intrusos con conceptos neurobiológicos de forma que permitan simular el cerebro humano para una mejor detección de ataques. En [40] se realiza un estudio de las perspectivas futuras de la Inteligencia Artificial en la detección de Intrusos, destacándose cómo determinadas técnicas de Inteligencia Artificial podrán mejorar las técnicas de comprensión de estos sistemas, así como permitir una clasificación jerárquica de los diferentes tipos de ataques.

7 Conclusiones

Este artículo ha presentado un estudio de aplicaciones fundamentales de la Inteligencia Artificial en la Seguridad Informática, en temas muy sensibles y de vital importancia como la detección de intrusos, correo no deseado (spam), antivirus, así como otras aplicaciones importantes.

El dinamismo que exige el tratamiento de la Seguridad Informática en cualquier nivel supone la utilización de técnicas avanzadas y sofisticadas. El ascenso constante que ha experimentado la Inteligencia Artificial permite una unión perfecta con muchos elementos de la Seguridad Informática. Los estudios que se realizan en el presente y futuro cercano avizoran la solución de problemas críticos que con la utilización de algoritmos tradicionales son muy difíciles o su complejidad es muy alta para su solución.

La revisión bibliográfica que se ha realizado en este artículo demuestra la utilidad de la Inteligencia Artificial en la Seguridad Informática, sin embargo, aún existen algunos aspectos en los que se hace necesario el estudio y profundización en vista a la protección cada vez mejor y efectiva de la información.

Referencias

[1] C. P. Pfleeger y S. L. Pfleeger, *Security in computing*, 4o ed. New Jersey: Prentice Hall, 2003.

[2] E. Cohen, *Information and Beyond: Part I*. *Informing Science*, 2007.

[3] R. G. Bace, Intrusion detection. Sams Publishing, 2000.

[4] J. Frank, «Artificial intelligence and intrusion detection: Current and future directions», 1994, vol. 10.

[5] D. G. Schwartz, S. Stoecklin, y E. Yilmaz, «A case-based approach to network intrusion detection», 2002, vol. 2, págs. 1084-1089 vol. 2.

[6] S. Mukkamala y A. H. Sung, «A Comparative Study of Techniques for Intrusion Detection», *Tools with Artificial Intelligence, IEEE International Conference on*, vol. 0, pág. 570, 2003.

[7] M. Abdel-Azim, A. I. Abdel-Fatah, y M. Awad, «Performance analysis of artificial neural network intrusion detection systems», 2009, pág. II-385-II-389.

[8] A. Iftikhar, A. Azween, y S. A. Abdullah, «Remote to Local Attack Detection Using Supervised Neural Network», 2010.

[9] W. Li, «Using genetic algorithm for network intrusion detection», *Proceedings of the United States Department of Energy Cyber Security Group*, págs. 24-27, 2004.

[10] Z. Pawlak, «Rough sets», *International Journal of Parallel Programming*, vol. 11, nº. 5, págs. 341-356, 1982.

[11] J. R. Rabunal y J. Dorado, «Intrusion Detection Using Modern Techniques: Integration of Genetic Algorithms and Rough Sets with Neural Nets», in *Artificial neural networks in real-life applications*, Idea Group Pub, 2006.

[12] M. Botha, R. Von Solms, K. Perry, E. Loubser, y G. Yamoyany, «The utilization of artificial intelligence in a hybrid intrusion detection system», *Proceedings of the 2002 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*. South African Institute for Computer Scientists and Information Technologists, págs. 149-155, 2002.

[13] M. Manninen, «Using Artificial Intelligence in Intrusion Detection Systems», *Helsinki University of Technology*, 2002.

[14] S. Noel, D. Wijesekera, y C. Youman, «Modern intrusion detection, data mining, and degrees of attack guilt», *Applications of Data Mining in Computer Security*, págs. 1-31, 2002.

[15] K. Julisch, «Data mining for intrusion detection», *Applications of data mining in computer security*, págs. 33-58, 2002.

[16] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, y S. Stolfo, «A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data», *Applications of Data Mining in Computer Security*, vol. 6, págs. 77-102, 2002.

[17] A. Honig, A. Howard, E. Eskin, y S. Stolfo, «Adaptive model generation: an architecture for deployment of data mining-based intrusion detection systems», 2002.

[18] B. Liebald, D. Roth, N. Shah, y V. Srikumar, «Proactive intrusion detection», 2008, págs. 772-777.

[19] B. Thuraisingham, «Data mining and cyber security», 2003, pág. 2.

[20] J. R. Méndez, F. Fdez-Riverola, F. Díaz, y J. M. Corchado, «Sistemas inteligentes para la detección y filtrado de correo spam: una revisión», *Inteligencia Artificial, Revista Iberoamericana de Inteligencia Artificial*, vol. 34, págs. 63-81, 2007.

[21] B. Sirisanyalak y O. Sornil, «Artificial Immunity-Based Feature Extraction for Spam Detection», *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, ACIS International Conference on*, vol. 3, págs. 359-364, 2007.

[22] G. Ruan y Y. Tan, «Intelligent detection approaches for spam», in *Natural Computation, 2007. ICNC 2007. Third International Conference on*, 2007, vol. 3, págs. 672-676.

[23] M. K y R. Kumar, «Spam Mail Classification Using Combined Approach of Bayesian and Neural Network», *Computational Intelligence and Communication Networks, International Conference on*, vol. 0, págs. 145-149, 2010.

[24] X. Wang, G. Yang, Y. Li, y D. Liu, «Review on the application of artificial intelligence in antivirus detection systemi», in *Cybernetics and Intelligent Systems, 2008 IEEE Conference on*, 2008, págs. 506-509.

[25] S. Venkatachalam, «Detecting undetectable computer viruses», San Jose State University, 2010.

[26] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, y Y. Elovici, «Application of artificial neural networks techniques to computer worm detection», 2006, págs. 2362-2369.

[27] R. Moskovitch et al., «Detection of unknown computer worms activity based on computer behavior using data mining», in *Computational Intelligence in Security and Defense Applications, 2007. CISDA 2007. IEEE Symposium on*, 2007, págs. 169-177.

[28] M. G. Schultz, E. Eskin, F. Zadok, y S. J. Stolfo, «Data mining methods for detection of new malicious executables», in *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*, 2001, págs. 38-49.

[29] A. Berkat, «Using Case-Based Reasoning (CBR) for detecting computer virus», *International Journal of Computer Science* 8, 2011.

[30] M. Gupta, J. Rees, A. Chaturvedi, y J. Chi, «Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach», *Decision Support Systems*, vol. 41, nº. 3, págs. 592-603, 2006.

[31] M. Hentea, «Intelligent System for Information Security Management: Architecture and Design Issues», *Informing Science: International Journal of an Emerging Transdiscipline*, vol. 4, nº. 1, págs. 29-43, 2007.

[32] C. A. Visaggio y F. de Rosa, «A System for Managing Security Knowledge using Case Based Reasoning and Misuse Cases», *Journal of Universal Computer Science*, vol. 15, nº. 15, págs. 3059-3078, 2009.

[33] A. Galande, D. Londhe, y M. Balpande, «Security in Voip Network Using Neural Network and Encryption Techniques», *International Conference on Information and Network Technology*, 2011.

[34] G.-H. Liu, G. Wu, Z. Tao, J.-M. Shuai, y Z.-C. Tang, «Vulnerability Analysis for X86 Executables Using Genetic Algorithm and Fuzzing», *Convergence Information Technology, International Conference on*, vol. 2, págs. 491-497, 2008.

[35] A. Moosa, «Artificial Neural Network based Web Application Firewall for SQL Injection», *World Academy of Science, Engineering and Technology*, nº. 64, págs. 12-21, 2010.

[36] Y. Liu y H. Man, «Network vulnerability assessment using Bayesian networks», in *Proceedings of SPIE*, 2005, vol. 5812, pág. 61.

[37] M. Frigault, L. Wang, A. Singhal, y S. Jajodia, «Measuring network security using dynamic bayesian network», in *Proceedings of the 4th ACM workshop on Quality of protection*, 2008, págs. 23-30.

[38] K. Shihab, «A backpropagation neural network for computer network security», *Journal of Computer Science*, vol. 2, nº. 9, págs. 710-715, 2006.

[39] S. Mukkamala y A. H. Sung, «Identifying significant features for network forensic analysis using artificial intelligent techniques», *International Journal of Digital Evidence*, vol. 1, nº. 4, págs. 1-17, 2003

[40] Frank, J. (1994, October). Artificial intelligence and intrusion detection: Current and future directions. In *Proceedings of the 17th National Computer Security Conference* (Vol. 10, pp. 1-12).