SEGURIDAD INTELIGENTE

Intelligent security

RESUMEN

Este artículo presenta hace una revisión de la aplicación de diferentes técnicas de inteligencia artificial aplicadas a la seguridad en sistemas informáticos. Se explica brevemente cada una de ellas y analizan la forma de aplicación y las ventajas conseguidas. Igualmente se muestran algunos proyectos realizados y la forma en que confluyen en ellos estas dos vertientes.

PALABRAS CLAVES: Inteligencia artificial, seguridad en cómputo, IDS.

ABSTRACT

This article presents a revision of the application of different techniques of artificial intelligence applied to the security in computer science systems. Is explained briefly each and analyze the obtained form of application and advantages. Also some projects are showed and the form in which these two approaches come together.

KEYWORDS: *Artificial intelligence, security in calculation, IDS*

NESTOR DARIO DUQUE MENDEZ
Ph.D. (c) Ingeniería - Sistemas
Profesor Asociado
Universidad Nacional de Colombia
Sede Manizales
ndduqueme@unal.edu.co

JULIO CESAR CHAVARRO PORRAS
Ph.D. (c) en Ingeniería - . Área de énfasis: Ciencias de la computación
Profesor Asistente
Universidad Tecnológica de Pereira
jchavar@utp.edu.co

RICARDO MORENO LAVERDE
M.Sc. en Administración Económica y Financiera
Profesor Asociado
Universidad Tecnológica de Pereira
rmoreno@utp.edu.co

1. INTRODUCCIÓN

El papel importante asociado a los sistemas de información, el valor conferido a la información y el conocimiento que de ellos se puede extraer, coloca en el centro de la discusión el asunto de la seguridad de los sistemas informáticos. No sólo hay que tener buenos sistemas hay que tener sistemas seguros, con protecciones razonables contra ataques a la privacidad, la continuidad y la confiabilidad. Se espera diseñar y construir sistemas de seguridad que actúen permanente y automáticamente. La inteligencia artificial (IA) que ha permeado casi todas las actividades humanas, también en este campo puede contribuir con enfoques bioinspirados a lo que se les reconoce gran potencial.

Para entender los caminos recorridos y los diferentes enfoques es necesario hacer una revisión del estado del arte, donde se muestre las diferentes técnicas inteligentes aplicadas a la seguridad de cómputo y los resultados obtenidos con las mismas, a la vez que deje ver los espacios abiertos en la temática.

Esta revisión se realiza recorriendo cada una de las técnicas de IA explorando las aplicaciones reportadas y simultáneamente mostrado algunos enfoques propios de dichas aplicaciones. Se ha tomado como base el trabajo previo realizado y consignado en [1].

2. MARCO CONCEPTUAL

2.1. Inteligencia Artificial

La IA es el estudio de la conducta inteligente. Una de sus metas es entender la inteligencia humana. La otra es producir maquinas útiles [2]. Los objetivos de la Inteligencia artificial pueden, entonces, resumirse en el estudio del proceso de pensamiento y la conducta inteligente de los humanos y producir maquinas o sistemas que representen estos procesos. Como modelo de forma inteligente tradicionalmente se ha pensado en el hombre, pero recientes trabajos tratan de conseguir mejores comportamientos apoyados en características de otras especies, como inspiración para la resolución de estos problemas obteniendo el gran conocimiento ganado en muchos años de evolución.

2.2. Seguridad Informática

La Seguridad en Cómputo puede entenderse como las políticas y medidas tomadas a nivel administrativo y técnico para proteger los recursos informáticos. Los ejes que orientan las actividades de seguridad son la continuidad y disponibilidad de los sistemas, la seguridad física, la privacidad y confidencialidad, la confiabilidad e integridad y la eficiencia, efectividad y economía.

Los riesgos a que están expuestos los sistemas de cómputo pueden enmarcarse dentro de accesos no autorizados, divulgación de información importante, denegación de servicios, perdida de recursos, vandalismo y sabotaje. Las amenazas afectan principalmente al hardware, al software y a los datos. Estas se deben a fenómenos de interrupción, interceptación, modificación y generación [3].

Fecha de Recepción: 31 Mayo de 2007
Fecha de Aceptación: 24 Julio de 2007

Dentro de las características que se esperan de los sistemas y a las cuales debe contribuir la seguridad se tiene: autenticación, autorización, no-repudiación y

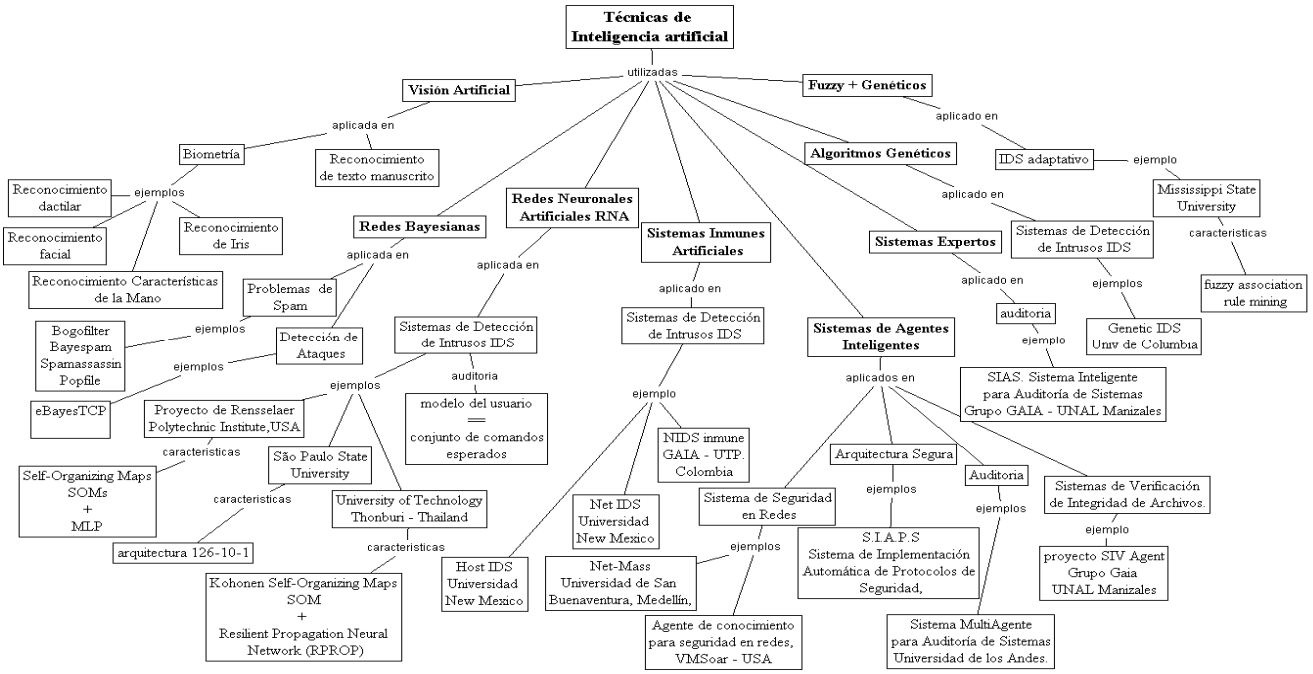

Figura 1. Técnicas de inteligencia artificial aplicadas a seguridad en cómputo

auditabilidad. Entre los mecanismos de seguridad informática tienen fuerte presencia las firmas digitales, los certificados digitales, los algoritmos de encriptación simétrica y asimétrica, los sistemas detectores de intrusos IDS (Intrusion Detection Systems), el control de integridad de archivos y los logs de auditoria. En particular en el análisis en redes, los sniffers (analizadores de protocolos llevando la interfaz a modo promiscuo y visualizando todo el tráfico a través de ella) y scanners (herramienta de seguridad que permite explorar los puntos vulnerables del sistema o de la red).

3. REVISION DE PROPUESTAS

La figura 1 muestra las diferentes técnicas de inteligencia que están siendo utilizadas en los sistemas de seguridad en sistemas informáticos. Para cada técnica se especifican algunas de las aplicaciones específicas, con algunas de las características distintivas y algunos casos ejemplo.

Como se aprecia el espectro es bastante amplio, tanto por las técnicas como por los esquemas de seguridad apoyados: biometría, sistemas de soporte de decisiones, filtrado de correos, auditoría, integridad de archivos, pero sin duda gran relevancia se ha dado a los sistemas detectores de intrusos (IDS).

3.1. Visión artificial.

Que cumple un importante papel en la adecuación de los métodos de autenticación pasando de la propuesta inicial donde la autenticación se realizaba con lo que se sabía (clave) a un esquema más robusto donde se hace con lo propio del individuo (huellas dactilares, configuración de retina, etc.). Estos mecanismos ya están siendo utilizado masivamente en diversos ambientes.

3.2 Redes bayesianas.

La lógica bayesiana, creada por el matemático inglés Thomas Bayes en 1763, se basa en las estadísticas y las probabilidades condicionales para predecir el futuro. La clasificación bayesiana, es una técnica no supervisada de clasificación de datos.

El correo indeseable o correo basura, más conocido como SPAM es un problema creciente que afecta todos los servidores y clientes de correo electrónico. El spam representa el 60% del correo que se transmite por Internet y con tendencia a subir. Mensajes no deseados o no solicitados llenan los buzones de los usuarios permanentemente, con contenidos irrelevantes, con publicidad indiscriminada, intentos de fraude (Nigerian investment), virus, cadenas, chistes, entre otros [4].

A pesar de la tendencia a la alza Paul Graham [5] plantea que los filtros basados en el contenido son la mejor forma en contraste con los filtros por dirección del emisor. Su propuesta está basada en la técnica de inteligencia artificial llamada lógica bayesiana. Las redes bayesianas pueden determinar palabras con alta probabilidad de ser parte de un mensaje basura y a través de un algoritmo filtrar los mensajes que contengan estas palabras y dinámicamente aprender para refinar su actuación. Para esto se debe entrenar el sistema marcando las palabras buenas y malas en los correos recibidos. Las pruebas con filtros bayesianos reconocen el 99,5% de correo basura.

Estas mismas virtudes se han aplicados para la detección

de ataques. En [6] se presenta un modelo, eBayesTCP, para detección de ataques, adaptativo, de alto desempeño usando el método Bayesiano como técnica de inferencia, para analizar el tráfico. Las clases de ataques son incorporadas como hipótesis del modelo que son reforzadas adaptativamente. Una característica llamativa de este trabajo es que tanto la técnica basada en marcas como la estadística dan a través de la adaptación una potente generalización.

3.3. Sistemas Inmunes Artificiales

El interés de los investigadores en sistemas computacionales por los sistemas inmunes crece debido a la esperanza de que su estudio sugiera nuevas soluciones a problemas o por lo menos otras formas de ver esos problemas. Algunas interesantes propiedades de los sistemas inmunes: la detección distribuida, la detección imperfecta, la diversidad, la disponibilidad, autonomía, detección en múltiples capas y la adaptabilidad apoyada en el aprendizaje y la memoria. Estas propiedades hacen que el sistema sea escalable, resilente a cambios, robusto, muy flexible y un degradación suave [7], [8]. Todas estas características altamente deseables en cualquier sistema computacional, sin duda. La actuación del sistema inmune se puede ver como el problema de distinguir entre elementos peligrosos y los no peligrosos, algo similar a lo esperado de la seguridad computacional.

En particular buenos resultados se han presentado en sistemas detectores de anomalías. Un sistema de detección de intrusos es un mecanismo cuyo objetivo es detectar, identificar y responder ante una intrusión. En [9] se presenta un IDS en host en donde se define lo correcto o propio en términos de unas cortas secuencias de llamadas al sistema, ejecutadas por procesos privilegiados en el sistema operativo de red. Las pruebas mostraron que estas cortas secuencias permiten distinguir las conductas normales de las anormales. La estrategia usada fue recolectar datos de conductas normales para cada programa de interés (cada información es particular para cada arquitectura, versión de software y configuración, políticas de seguridad y patrones de uso). Esta base de datos es usada para monitorear la conducta de los programas. La forma de la secuencia de las llamadas al sistema define si es una situación normal o anormal, comparada con datos recolectados en condiciones normales sobre los subprocesos individualmente.

En la Universidad de New México [10] se ha diseñado y probado un IDS distribuido que monitorea tráfico en redes TCP/IP. Cada paquete es caracterizado por un tripla (Origen, destino, servicio). El IDS monitorea la red para ocurrencias de triplas no comunes, que representan tráfico inusual. Pero como desventajas presenta su alto costo computacional, su poca posibilidad de escalamiento y el hecho de correr en una sola máquina dedicada a esta tarea. Estas limitaciones pueden ser resueltas distribuyendo el IDS sobre la red, haciéndolo robusto, flexible y eficiente y los sistemas inmunes muestran interesantes soluciones a problemas similares. Este IDS depende de varias características inmunológicas, entre las más sobresalientes, la detección negativa con censura y la realización de coincidencias parciales con mascaras de permutación. Con la detección negativa, el sistema conserva un sistema de detectores negativos, que emparejan sucesos de patrones anormales o inusuales (en este caso, los patrones son representaciones binarias de la secuencia de las triplas del paquete). Los detectores se generan aleatoriamente y se censuran (suprimen) si coinciden con patrones anormales.

3.4. Sistemas Expertos.

Los Sistemas Expertos (SE) se pueden definir como software que simula el proceso de aprendizaje, de memorización, de razonamiento, de comunicación y de acción de un experto humano en una determinada área de dominio, convirtiéndose en un consultor que pueda sustituirlo y/o apoyarlo en la toma de decisiones acertadas. Es el clásico representante del paradigma simbólico.

Reseñamos el trabajo propio, desarrollado en el marco del Grupo de Ambientes Inteligentes Adaptativos GAIA de la Universidad Nacional de Colombia Sede Manizales. Esta propuesta está orientada a la automatización del proceso de auditoria de sistemas bajo el enfoque orientado a riesgos. El Sistema Inteligente para Auditoría de Sistemas (SIAS) toma como punto de partida la metodología de análisis de riesgos con base en la cual construye el sistema inteligente, defiendo las reglas y los hechos que requiere un auditor humano para aplicar dicha metodología [11]. El sistema es implementado en un ambiente Internet buscando mayor accesibilidad y como otro elemento a resaltar está el hecho que todos los componentes de software utilizados están bajo licencias de software libre. La figura 2 permite ver la arquitectura del sistema.

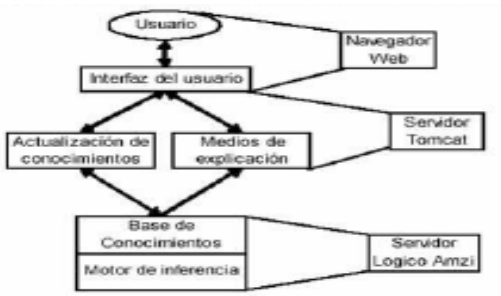

Figura 2. Arquitectura del Sistema Inteligente apara Auditoría de Sistemas SIAS

3.5. Algoritmos Genéticos AG

Los algoritmos genéticos son heurísticas basadas en los principios de evolución natural y genética, introducidos por J. Holland en los años 70. Un elemento importante es que pueden operar sobre un espacio de búsqueda concurrentemente permitiendo que no sean atrapados en

un óptimo local. Los Algoritmos Evolutivos requieren que se les especifique la codificación de los individuos y una función de evaluación que mida la aptitud de cada individuo.

En [12] se propone un novedoso enfoque para detectar intrusiones usando AG. Con fines experimentales, el algoritmo genético se diseño para aprender como detectar intrusiones maliciosas y separar éstas de las normales. Los resultados de las pruebas prometen que este método permite alta tasa de detección de conductas maliciosas y una baja rata de falsos positivos de conductas normales clasificadas como maliciosas. El algoritmo genético fue diseñado para que cada individuo de la población represente una posible conducta. El AG usado aísla 41 diferentes características de conexión de usuarios clasificados. Dentro de los atributos analizados están: Tipo de protocolo (TCP, ICMP y UDP) y cada resultado fue etiquetado como normal o malicioso.

Llama la atención la forma ñeque redefine la función fitness (*F*) de un individuo (*di*) de la población, esta depende de cuántos ataques fueron correctamente detectados y cuántas conexiones normales se clasificaron como ataques. $F(di) = (a/A) – b/B$. Donde *a* es el numero de ataques detectados correctamente, *A* es el número total de ataques, *b* es el número de falsos positivos y *B* es el número total de conexiones normales. Al final se obtuvo una precisión del 97.8 %

3.6. Fuzzy + Genéticos

En [13] se propone, en estado experimental, un marco para IDS adaptativos apoyado en minería de datos. El objetivo es identificar patrones de intrusiones conocidas o diferenciar las actividades normales de las anormales. Los algoritmos de minería de datos se usan para auditar los datos comparando las actividades corrientes con un perfil normal previamente caracterizado. El IDS debe estar en capacidad de adaptarse a los cambios en los patrones. Se propone un marco general para un modulo adaptativo para detección de anomalías que usa fuzzy association rule mining, El algoritmo genético es propuesto para sintonizar los parámetros de las funciones de membresía fuzzy, luego la minería con reglas de asociación fuzzy son aplicadas a un perfil normal. Durante cada ventana de tiempo los datos en la parte incremental son minados y comparados con el conjunto de reglas del perfil. Se pueden presentar tres posibilidades: Si la similaridad está encima del umbral (threshold) no es necesaria la actualización y el sistema continúa con el perfil corriente. Si está por debajo con cambio negativo la intrusión puede ser señalada y no se actualiza el perfil. Si la similaridad está por debajo del umbral con cambio gradual el perfil se actualiza con los datos en la actual ventana de tiempo.

3.7. Redes Neuronales Artificiales RNA

Las redes neuronales tratan de captar la esencia de procesos biológicos y aplicarlos a nuevos modelos de computación. La neurona artificial es un modelo simplificado de neurona biológica. La interconexión entre neuronas decide el flujo de información en la red y junto con los pesos y las funciones de salida de cada neurona definen el comportamiento global de la red neuronal artificial. Esto hace que las redes neuronales estén formadas por un gran número de elementos de cómputo lineales y no lineales (neuronas) complejamente interrelacionados y organizados en capas. Las redes neuronales por su estructura distribuida masivamente paralela y la habilidad de aprender y generalizar, están capacitadas para resolver problemas complejos. Estas características han sido aprovechadas por muchos proyectos orientados a la seguridad.

De las técnicas de inteligencia artificial esta es la más utilizada en los sistemas detectores de intrusos, como se aprecia en la figura 1, por lo cual se hace un análisis especial a este tópico. Existen varios modelos y arquitecturas con ventajas y desventajas específicas para diferentes fines.

Las tablas 2 a 4 muestran diferentes tipos de redes neuronales, la configuración aplicada y los resultados esperados.

3.7.1. Redes Tipo Perceptron multicapa MLP.

a. Orientadas a detectar uso indebido

Ref	[14]	[15]
Entradas	Ordenes usuario	Puertos, direcciones, código ICMP, tipo ICMP, Datos, longitud de datos.
Salidas	Anomalía o normal	Normal o Ataque
Algoritmo Entrenam	backpropagation	backpropagation
Arquitectura	100-30-10	9-?-?-2
Observac		360 firmas de ataque. Ataques DoS, escaneo de puertos, penetración al sistema
Resultados	Detecc 93% Falsos 7%	Falso 0,69929%, Detec 97,55%.

Tabla 1. Redes MLP Orientadas a detectar uso indebido.

b. Orientadas a detección de anomalías

Ref	[16]	[17]
Entradas	9 encabezado + 393 caracteres de contenido	cabecera de protocolos
Salidas	Normal o ataque	Normal o ataque
Algoritmo Entrenam	Trairp	backpropagation
Arquitectura	402-401-1	29-30-2
Observac	Tos, len, ttl, Sport, Dport, Seq, ack, TCPFlags, Win	
Resultados	Detecc Paq Normal 83,78%, Paq Pelig 100%. Falso Negativo 4%.	Detecc 91.4773%. Falsos positivos 6,9929 %.

Tabla 2. Redes MLP Orientadas a detección de anomalías.

3.7.2. Redes Tipo Mapas Autoorganizados SOM.

Por su forma de trabajo están siendo usadas en detección de anomalías

Ref	[18]	[19]	[20]
Entradas	Datos del protocolo	protocolo de comunicación	Tipo de protocolo y servicio, banderas de protocolo
Salidas		DoS y Penetración	
Entrenam	distancia que hay entre la muestra de entrenamiento y la neurona de entrada	cálculo del error de cuantización	
Arquitectura	Tres capas		Tamaño del cluster para el SOM 3*5.
Observac	Capa para tráfico IP, capa para protocolos TCP UDP, capa para tipo de servicio	SOM para cada tipo de servicio (FTP, SMTP, Telnet).	
Resultados			detección SOM 97.89%

Tabla 3a. Redes SOM orientadas a detección de anomalías.

Ref	[17]	[21]
Entradas	cabecera de protocolos (29 datos en total	cabeceras de protocolo
Salidas	anómalo, normal, sin etiquetar	anomalías y datos normales
Entrenam	niveles de vecindad con relación a la neurona ganadora	
Arquitectura	rectangular de 40 por 40	rectangular 5*5
Resultados	Detección: 99.0627%	Detección > 95%

Tabla 3b. Redes SOM orientadas a detección de anomalías.

3.7.3. Redes Recurrentes.

La literatura esboza trabajos en detección de anomalías

Ref	[22]	[23]
Entradas	protocolo http	protocolos y datos de paquetes
Salidas	Identificación y Detección	
Algoritmo Entrenam	Backpropagation	Resilient Propagation
Arquitectura	Nivel de filtrado y el nivel de detección 64-30-30-5	20-126-2
Observac		
Resultados	Detección: 94,3%, Falsos P: 4.7%,	Detecc: 97%

Tabla 4. Redes Recurrentes orientadas a detección de anomalías.

Dada esta clasificación es importante hacer notar la diferencia entre los dos tipos de orientación de los IDS: detección de anomalías y detección de usos indebidos del sistema. Los primeros proponen la creación de perfiles de uso de los sistemas durante un determinado periodo de tiempo, luego las desviaciones son reportadas para su análisis. El segundo enfoque es el más tradicional y sigue siendo el más extendido, donde se tiene conocimiento específico sobre determinados ataques y el análisis se basa en esto, buscando coincidencia con alguno de los patrones conocidos para emitir una alerta.

3.8. Sistemas de Agentes Inteligentes

Un agente inteligente es una entidad que percibe y actúa sobre un entorno de forma razonada, que puede realizar tareas especificas para un usuario y posee un grado de inteligencia suficiente para ejecutar parte de sus tareas de forma autónoma y para interactuar con su entorno de forma útil [24]. Por lo tanto, son entidades de software que ejecutan un conjunto de operaciones en nombre de un usuario u otro programa. Los Sistemas Multiagentes SMA, son sociedades de agentes que se orientan a fines comunes y mediante coordinación y colaboración distribuyen las tareas. Dentro de los diferentes trabajos se reseña el proyecto en desarrollo en la Universidad de San Buenaventura en Medellín, NET-MASS, un sistema multiagente distribuido como herramienta de protección para redes con diferentes sistemas operativos y susceptibilidad a diversos ataques. El Sistema está compuesto por un grupo de agentes autónomos heterogéneos con características particulares en cuanto a sus estrategias de detección de intrusos y protección de los sistemas primordiales de la red, estos agentes basan sus decisiones en la aplicación de diferentes técnicas de inteligencia artificial como heurística de sistemas expertos, algoritmos evolutivos y redes neuronales. Dentro del NET-MASS los agentes tienen una estructura constituida de los siguientes componentes: Componente de ejecución, componente funcional y componente de comunicación. El sistema cuenta con 6 tipos de agentes: agentes de escucha, agentes de detección de intrusos de red (NIDS), agentes de detección de virus, agentes de coordinación, agentes de reporte y agentes de alarma y auditoria. Más allá de la capacidad de operar en múltiples plataformas, el sistema espera poder generar esquemas adaptativos que representen incluso el estado actual de la red. Agente de conocimiento para seguridad en redes, VMSoar, es una implementación realizada en Pace University en Estados Unidos. VMSoar es una agente cognitivo diseñado para configuración y administración de seguridad en redes, creando copias virtuales de las maquinas y aprende como asociar patrones de actividades en la red con acciones ilegales de usuarios. Este desarrolla una evaluación automática de vulnerabilidades explorando configuraciones frágiles y buscando intrusos en la red. VMSoar hace una copia de la porción de red e intenta generar los paquetes observados en la red simulada aplicando varios exploits. Inicialmente es lento pero el aprendizaje eleva significativamente el desempeño. Estas conductas aprendidas son usadas luego durante la detección de intrusiones intentando

modelar las metas de los usuarios de la red. Posee conocimiento para separar las actividades legales de las ilegales y lo usa para probar la vulnerabilidad en la configuración de los sistemas. La evaluación de vulnerabilidades es usada para encontrar fallas en sistemas operativos y servidores. Igualmente el conocimiento sobre actividades en la red permite monitorear en tiempo real. El SIV Agent es una idea del grupo de investigación de Ambientes Inteligentes Adaptativos de la Universidad Nacional de Colombia Sede Manizales y consiste en agentes inteligentes para verificación de integridad de archivos, que permiten conocer si en algún momento la máquina fue comprometida y alguno de archivos sensibles modificado. El diseño está basado en tripwire, la primera herramienta ampliamente disponible para verificación de integridad. Se espera que el sistema realice las diferentes verificaciones en forma autónoma y presente las inconsistencias encontradas. Entre las funciones de los agentes se tienen la recuperación de información histórica, realizar las sumas de verificación y comparación, comparación de permisos en los archivos, presentación de alarmas en caso de ser necesario, entre otras.

4. CONCLUSIONES

Este artículo muestra la confluencia de estos dos campos (IA y seguridad) lo que robustece la seguridad minimizando las vulnerabilidades y aprovechando los avances en las técnicas de inteligencia artificial.

Los grandes retos están asociados con la representación del conocimiento que permitan mapear el problema en la técnica y en la calibración los parámetros que permitan lo resultados esperados.

5. BIBLIOGRAFÍA

[1]Duque Méndez, Néstor Darío. Inteligencia Artificial y Seguridad en Cómputo. En Seguridad en Cómputo e Inteligencia Artificial. Día internacional de seguridad en Cómputo. UTP 2005

[2] Garnham. Artificial Intelligence, 1987.

[3] Ramió Aguirre, J., Curso de Seguridad Informática. Universidad Politécnica de Madrid. España. 2002.

[4] Calvo, Jorge Mario. Lucha contra el SPAM: será una causa perdida? DISC. Pereira. 2004

[5] Graham, Paul. A Plan for Spam, http://www.paulgraham.com/spam.html.

[6] Valdes , Skinner Keith. Adaptive, Model-based Monitoring for Cyber Attack Detection. SRI International. 2000.

[7] Chao, D y Forrestert, S. , Information Inmune System University of New Mexico ,USA.

[8] Hofmeyr, Steven A. Computer Immune Systems, Computer Science Department, Farris Engineering Center.University of New Mexico. 1997

[9] Forrest. Computer Immune Systems, Computer Science Department.University of New Mexico. www.cs.unm.edu/ immsec/.2000

[10] Hofmeyr, S. y Forrest, S. .Architecture for an Artificial Immune System. Evolutionary Computation. Morgan-Kaufmann, San Francisco. 2000.

[11] Duque, Néstor. Zuluaga, C. González H. Sistema Inteligente de Auditoria de Sistemas para aplicaciones en funcionamiento usando Software Libre En: EITI2003. Medellín. Universidad Nacional de Colombia 2003

[12] Chittur, Adhitya. Model Generation for an Intrusion Detection System Using Genetic Algorithms, 2001

[13] Hossain, M. y Bridges, S. A Framework for an Adaptive Intrusion Detection System with Data Mining. Department of Computer Science. Mississippi State University. 2000.

[14] Ryan Jake, Lin Meng-Jang, Miikkulainen Risto. "Intrusion Detection with Neural Networks". Department of Computer Sciences. 1998.

[15] Cannady, James. "Neural Networks for Misuse Detection". Initial Results. Proceedings of the Recent Advances in Intrusion Detection '98 Conference, 1998.

[16] Pérez Rivera Carlos Alfonso, Britto Montoya Jaime Andrés, Isaza Echeverry Gustavo Adolfo. Aplicación de redes neuronales para la detección de intrusos en redes y sistemas de información. Scientia Et Technica Año XI, No 27, Abril 2005.

[17] Grediagal Ángel, Ibarra Francisco, Ledesma Bernardo, Brostons Francisco. Utilización de redes neuronales para la detección de intrusos. Primer Congreso Iberoamericano de Seguridad, Departamento de Tecnología Informática y Computación. Universidad de Alicante, España, 2002.

[18] Rhodes, B. C., Mahaffey, J. A., and Cannady, J. D. "Multiple Self-Organizing Maps for Intrusion Detection". In Proceedings of the 23rd National Information Systems Security Conference (NISSC). 2000.

[19] Nguyen B.V. Self Organizing Map (SOM) for Anomaly Detection. Ohio University School of Electrical Engineering and Computer Science CS680 Technical Report, Spring 2002

[20] Zhong, J. Lei y Ali Ghorbani. Network Intrusion Detection Using an Improved Competitive Learning Neural Network. Faculty of Computer Science, University of New Brunswick Fredericton, Canada.2004

[21] Cortada Pere, Sanromà Gerar., García Pedro, Arenas Alex y Rallo Robert. IDS basado en Mapas autoorganizados. Departamento de Ingeniería Informática y Matemáticas. Universidad Rovira y Virgili. Tarragona, Cataluña, España.2002

[22] Torres, Efraín. Sistema inmunológico para la detección de intrusos a nivel de protocolo HTTP. Propuesta de proyecto de grado. Pontificia Universidad Javeriana, Bogotá, 2002.

[23] Pinacho Davidson Pedro, Valenzuela Tito. Una propuesta de IDS, basado en Redes Neuronales Recurrentes. Grupo de Investigación en Tópicos de Seguridad (GITS), Departamento de Ingeniería Informática, Universidad de Santiago de Chile (USACH) 2005

[24] Brenner, W., Zarnekow R y Witting H., Intelligent Software Agents, Springer-Verlag. 1998.