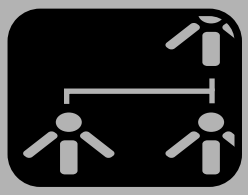
Gerenc.tecnol.inform. Vol 6|No 16|53-62,2007

TÉCNICAS INTELIGENTES, AGENTES ADAPTATIVOS Y REPRESENTACIONES ONTOLÓGICAS EN SISTEMAS DE DETECCIÓN DE INTRUSOS



AUTOR
Gustavo A. Isaza Echeverry
Doctorado(Estudiante) Ingeniería de Software
Docente Universidad de Caldas
gustavo.isaza@ucaldas.edu.co
COLOMBIA

AUTOR
Andrés G. Castillo Sanz
Doctorado Ingeniería de Software
Docente Universidad Pontificia de Salamanca
andres.castillo@upsam.net
ESPAÑA

AUTOR
Néstor D. Duque Méndez
Doctorado (C) Ingeniería de Sistemas
Ms.C. en Ingeniería de Sistemas
Profesor Asociado Universidad Nacional Sede Manizales
ndduqueme@unal.edu.co
COLOMBIA

Fecha de Recepción: Octubre 3 de 2007 ***Fecha de Aceptación : 5 de Noviembre de 2007***

Articulo Tipo 3

RESUMEN.

La seguridad Informática requiere una optimización permanente de los mecanismos de protección y estrategias que permitan prevenir ataques en las redes y sistemas de información. El proceso de monitoreo de eventos que ocurren en un sistema o en una red a partir de patrones y firmas de posibles ataques se conoce como Sistema de Detección de Intrusos (IDS). Los IDS han escalado significativamente al punto de focalizarse en modelos basados en prevención más que en corrección, estos sistemas monitorean tráfico utilizando un conjunto de firmas para detectar actividades malignas, reportar incidentes o tomar acciones correctivas; pero cualquier cambio insertado en el patrón de un ataque, puede comprometer el sistema y evitar que la tecnología subyacente de detección o prevención sea insuficiente. En los últimos años se han planteado diferentes modelos basados en técnicas de Inteligencia Artificial que pueden ayudar a la generación automática de nuevas firmas y detectar nuevos patrones de ataque sin la intervención humana. Algunas investigaciones presentan técnicas como Redes Neuronales, Algoritmos Genéticos, Razonamiento Basado en Casos, árboles de decisión, Lógica Difusa entre otras, aplicadas a la Detección de Intrusos, además de arquitecturas basadas en Agentes Inteligentes sobre IDS Distribuidos incorporando así capacidades de autonomía, reactividad, pro actividad, movilidad y racionalidad. Este artículo es el resultado de un estudio del estado del arte de las diferentes estrategias inteligentes en IDS. Además la introducción de modelos de cooperación a partir de Agentes adaptativos y de representaciones ontológicas en los Sistemas de Detección de Intrusos Distribuidos, adicionalmente se plantean los elementos de una investigación en curso donde se incorporan estos métodos.

PALABRAS CLAVE

Sistemas de Detección de Intrusos
Detección de Intrusos Inteligente
Agentes Inteligentes
Seguridad en Redes
Representaciones Ontológicas y Semánticas
Conglomerados

ABSTRACT

Security Computing requires a permanent optimization in protection mechanisms and strategies that allow preventing attacks in the networks and information systems. The event monitoring process that happens in a system or a network using patterns or signs is known like Intrusion Detection System (IDS). The IDS have been focused more in prevention models than correction models; these systems tests traffic using a set of signs to detect malicious activities, report incidents o take correction actions; but, any change inserted in the attack pattern can compromise the system and avoid the underlying technology and make insufficient the Intrusion Detection. Over the years different models based in Artificial Intelligence techniques have been considered to help the automatic signs and patterns generation without human intervention. Some researching projects present Neuronal Networks, Genetic Algorithms, Case Based Reasoning, decision trees, Fuzzy logic applied to the Intrusion Detection; additionally using Intelligent and Mobile Agents architectures over Distributed IDS incorporating autonomy, reactivity, pro activity, mobility and rationality capabilities. This paper is result of studying state of art of multiples intelligent strategies in IDS and cooperation models using Agents and ontology representation in Intrusion Detection. This paper complements elements in a course research considering integrating these methods.

KEYWORDS

Intrusion Detection Systems
Intelligent Intrusion Detection
Intelligent Agents
Network Security
Ontology and Semantic representations

INTRODUCCIÓN

La Detección de Intrusos ha sido definida como el problema de identificar posibles ataques por parte de entidades que no tienen autorización para tal efecto o que tienen legítimo acceso pero que están abusando de sus privilegios [18]. Los Sistemas de Detección de Intrusos (IDS) son modelos y técnicas que han sido diseñados para mejorar la seguridad en recursos computacionales individuales y conectados. Los estudios hechos en este campo iniciaron con análisis del flujo de información y con base en un conocimiento de expertos se estructuraron firmas y patrones que podían ser posibles incidentes de seguridad. Estas técnicas han ido evolucionando hasta convertirse en lo que hoy conocemos como Sistemas de Detección de Intrusos basados en reglas y se han posicionado como el estándar de facto. [1] [2] [5]. Estas reglas (firmas) deben ser actualizadas constantemente debido al creciente número de ataques; las modificaciones y alteraciones a los patrones hace que el incidente de inseguridad sea indetectable por los IDS. [11] [19]

En este artículo se presenta una investigación del estado del arte en el marco de un proyecto de diseño e implementación de arquitecturas basadas en técnicas inteligentes híbridas, agentes adaptativos y representaciones ontológicas en Sistemas de detección de Intrusos. El primer capítulo se centra en la descripción general de conceptos como Detección de Intrusos, Técnicas Inteligentes, Agentes y Ontologías, posteriormente se hará una breve descripción de las estrategias utilizadas para optimizar el monitoreo de ataques usando estas técnicas, en los apartados siguientes se relatarán los elementos tratados hasta el momento en la investigación en curso y los componentes en proceso de análisis y diseño.

1. CONTEXTO EN LA DETECCIÓN DE INTRUSOS

La IETF Intrusion Detection Working Group (IDWG)[1] define que un IDS está compuesto de tres elementos principales: [2] [3] uno o más sensores cuyo rol es obtener datos de un sistema monitoreado, darle estructura, formatear los datos y construir eventos, un analizador que chequea los eventos disparados por los sensores y genera alertas si se requieren y un administrador que obtiene la información (eventos, alertas) del analizador para darle un tratamiento (presentación, Correlación y reacción) [6] [8] [16]. Sin embargo algunos de los problemas que se presentan son los falsos positivos (Alarmas de ataques que No lo son en realidad) y falsos negativos (el sistema falla en detectar un fragmento que es seguro cuando está realmente infectado). [11][13][14]. Los IDS deben cumplir propiedades como ejecutarse continuamente con el mínimo de supervisión humana, deben ser tolerantes a fallos y recuperarse de posibles salidas abruptas, deben ser capaces de monitorearse a si mismos y autoprotegerse, deben generar el mínimo de sobrecarga en la red y deben ser escalables. [7][36]

Los IDS se clasifican en sistemas basados en Hosts (HIDS) se ejecutan y monitorean eventos en una sola estación, Red (NIDS) monitorean eventos en una red o segmento [35], IDS Distribuidos (DIDS) basado en arquitecturas distribuidas compuesto por NIDS (IDS de redes) que se comportan como sensores donde se centraliza la información de ataques. [7][40][41]

(1). http://www.ietf.org/html.charters/OLD/idwg-charter.html

De acuerdo a su modelo de detección se catalogan

como basados en firmas, anomalías y uso erróneo. [39] La Detección de Intrusos basada en anomalías (anomaly detection) crea una definición de "normalidad" y reporta cualquier actividad que constituya un evento irregular diferente a estos patrones como posiblemente intrusa [5] [20] [22]. Esta técnica crea un perfil de comportamientos observando actividades normales de los usuarios y aplicaciones, una vez se construyen estos perfiles a través de entrenamientos, cualquier suceso que sea divergente será considerado una posible intrusión. [31][47]. Este tipo de detección también se conoce como de "conocimiento positivo"

La detección de usos indebidos del sistema (Misuse Detection) propone un modelo donde se puedan establecer patrones de ataques reconocidos y posibles variaciones. Se conoce como de "conocimiento negativo" [50] [52]. Estos patrones se pueden estructurar a partir de firmas de ataques que capturan la esencia de una intrusión y que pueda ser usada para identificar futuros intentos de vulnerar el sistema [34]

2. ESTADO DEL ARTE EN EL USO TÉCNICAS INTELIGENTES EN DETECCIÓN DE INTRUSOS

En los siguientes apartados se describirán algunas de las estrategias usadas en los IDS a partir de modelos matemáticos, estadísticos y de la aplicación de técnicas inteligentes. [39]

2.1 Modelos Probabilísticos

Estos modelos pueden ser usados definiendo un conjunto de variables de medida, donde cada una puede tomar 2 posibles valores 0 o 1. 1 indica que la medida es anómala y 0 lo contrario. Aplicando matemática probabilística se puede determinar la sensibilidad de un sistema ante posibles ataques combinando sus probabilidades. [47]

2.2 Redes Bayesianas

Estos modelos toman la estructura básica de una detección probabilística en el cual una variable de medida puede afectar a otras. Esta información es usada para crear redes de credibilidad y representar gráficamente dependencias casuales entre variables. [12] Estas redes son grafos acíclicos y están en capacidad de calcular las distribuciones probabilísticas entre nodos adyacentes. Las Redes Bayesianas usan un conjunto de Tablas de Condiciones Probabilísticas (CPT) que almacenan los valores de probabilidad correspondientes a ciertas variables aleatorias dadas en una precondición. Estas probabilidades son tomadas usualmente de la experiencia pasada de eventos y contribuyen a tomar acciones eficientes de predecir una variable deseada. La intrusión es determinada por la probabilidad dada de la presencia o ausencia de evidencia. [12][51][52]

2.3 Sistemas Expertos

Estos sistemas han sido usados a partir de la construcción de conocimiento de un experto en pro de identificar acciones y datos irregulares. Estos métodos están directamente relacionados con dos factores principales: la idoneidad de uno o más expertos en seguridad que alimenta la entrada como mecanismo de detección y la implementación efectiva y coherente de la estructura de datos dada por el experto (humano) en un sistema computacional. Los Sistemas expertos han sido usados para interpretar medidas de prevención. [29][30][40]

2.4 Redes Neuronales

Los métodos de aprendizaje supervisado han sido usados en diferentes investigaciones en la detección de intrusos. [49] Estos métodos desarrollan clasificadores que predicen la salida de posibles valores basados en un conjunto de atributos de entrada. Las redes Neuronales pueden ser usadas para lograr una técnica efectiva de aprendizaje que permita clasificar los diferentes tipos de datos (a través de soluciones heurísticas) y optimizar la búsqueda de patrones a partir de valores y firmas ya existentes. Una Red Neuronal contiene un conjunto de nodos organizados en capas, las capas de entrada y de salida están interconectadas a través de capas intermedias. El aprendizaje se realiza actualizando los pesos y adaptando los parámetros de las funciones presentes en cada nodo. Un modelo de detección de intrusos neuronal puede ser usado para predecir el siguiente evento en un sistema. Por ejemplo, la secuencia de comandos en un aplicativo es una entrada útil para entrenar la red y calcular posibles secuencias futuras o valores esperados. [49] Por supuesto, uno de los grandes problemas de estos modelos es el tiempo de entrenamiento, suele ser alto, aunque depende explícitamente de depurar las funciones, los pesos y la capacidad de procesamiento con que se ejecute.

2.5 Redes de Petri

Las Redes de Petri están formadas por espacios, transiciones y arcos dirigidos que conectan un lugar (espacio) a una transición o viceversa. Las transiciones funcionan a través de disparadores a partir de fichas de una posición de inicio y generan fichas en una posición de llegada. Estas técnicas en el ambiente de los IDS pertenecen al grupo de detección de usos indebidos. Las transiciones de un estado inicial a un estado final describen la evolución de un ataque. Estas técnicas han sido usadas para modelar eventos de seguridad como comandos de usuario y llamadas del sistema. [30][40].

Las Redes de Petri permiten describir y hacer coincidir parcialmente secuencias ordenadas para visualizar los escenarios de posibles ataques. A partir de estas representaciones se pueden construir múltiples eventos de intrusión, y es evidente la simplificación del modelo. [29][30]

2.6 Programación Genética

La programación genética es un método basado en máquinas de aprendizaje derivado de los algoritmos genéticos[2] donde se toma una población de programas y puntos de muestra para resolver un problema. Las posibles soluciones son representadas a través de árboles analíticos cuyos componentes (nodos) son manipulados a través de operaciones, tales como mutaciones y recombinaciones genéticas [18] [39]. Posteriormente se aplican funciones de refinamiento en la identificación de los mejores individuos (programas). En la detección de Intrusos las actividades normales y anormales se presentan a los programas en orden para ser evaluadas y ser distinguidas según su categoría. [40][41]

2.7 Sensores Embebidos

Esta técnica propone el uso de segmentos de código que son insertados en los programas durante la fase de desarrollo. Estas instrucciones automáticamente buscan condiciones anormales en tiempo de ejecución incluyendo errores conocidos o incluso sobrecargas de pila y tipos de datos erróneos. [8][18][55]

2.8 Minería de Datos

La minería es una técnica de exploración y predicción para análisis de datos, estos métodos permiten optimizar la gestión de los mismos conducente a un proceso de gestión de conocimiento completamente relevante en los sistemas de detección de Intrusos. Esta disciplina emplea máquinas de aprendizaje y métodos de análisis estadístico para identificar patrones ocultos e información que un usuario no detecta de manera eficiente en grandes bases de datos (Bodegas de Datos). [4] Los patrones inferidos permiten la predicción de futuros resultados y para el caso de la detección de intrusos puede ayudar a detectar futuros intentos a partir de nuevas reglas generadas. [19][37]. La Detección de Intrusos ha generado problemas como el tratamiento y análisis de un gran número de alarma, la Minería de Datos puede ser usada para soportar parcialmente (y automáticamente) la gestión de este proceso.

(2).Es un método de búsqueda dirigida basado en técnicas probabilísticas. Mitchell, Melanie. An Introduction to Genetic Algorithms. MIT Press, 1996.

Con esta técnica se pueden usar combinaciones informativas para transformar conocimiento de tácito-explícito-tácito, modelos predictivos que permiten a un analista generar nuevas interpretaciones de los datos existentes. [19][20]

2.9 Lógica Difusa

La integración de la lógica difusa con minería de datos ayuda a crear patrones más abstractos en un nivel superior, así como a describir rangos de medida para eventos normales, anormales, o incidentes de seguridad como “altos”, “medios” o “bajos”, que pueden ser interpretados de manera más sencilla por los usuarios.[9][40]. A partir de la Lógica Difusa, las falsas alarmas pueden ser reducidas determinando cuales actividades de intrusión se pueden depurar, y usando un conjunto de reglas difusas se puede definir un comportamiento como “normal” o “anormal” a partir de un motor de inferencia difuso.

2.10 Máquinas de Soporte Vectorial (SVM)

Son máquinas de aprendizaje que usan algoritmos basados en clasificadores lineales e inducen hiperplanos en espacios de alta dimensionalidad con un modelo inductivo particular. Una SVM aprende la superficie decisión de dos clases diferentes en sus puntos de entrada. La descripción de los datos de los vectores forma un modelo de decisión sobre el dominio de aprendizaje con poco conocimiento de los datos fuera de sus límites. Los datos se mapean a través de un modelo de kernel en un espacio dimensional superior. En los sistemas de detección de intrusos, SVM clasifica los datos determinando un conjunto de vectores de soporte, que son parte de un conjunto de entradas entrenadas y cuya salida es un hiperplano en el espacio característico, permitiendo optimizar la velocidad de aprendizaje. [49]

2.11 Razonamiento Basado en Casos (CBR)

Esta técnica consiste en resolver nuevos problemas con base en soluciones anteriores de problemas similares. Los pasos para implementar un modelo de detección de intrusos utilizando razonamiento basado en casos propuestos por [54] son identificar posibles técnicas que caractericen un conjunto de firmas, desarrollar una técnica similar que caracterice firmas similares conocidas, incorporar los nuevos hilos de firmas de intrusión e introducir los resultados positivos de firmas similares.

2.12 Consideraciones sobre el uso de Técnicas Híbridas

Si bien el uso de estas técnicas han demostrado la eficiencia (“aceptable”) en el reconocimiento de patrones de ataques e incluso la minimización de falsos

positivos y negativos; la tendencia en investigación apunta a combinar diferentes métodos inteligentes para lograr mejores resultados, la posibilidad de combinación podría ser muy amplia teniendo en cuenta las variaciones de cada estrategia (tipos de redes neuronales, sistemas combinados de aprendizaje, sistemas difusos y genéticos, tipos de redes de petri, modelos de razonamiento de casos, entre otros). En consecuencia, se puede afirmar que se pueden lograr nuevos aportes en el problema de detección de intrusiones fusionando modelos de inteligencia artificial que puedan ser complementarios.

Durante la investigación que se plantea (enunciada en el capítulo 5) se definirán qué métodos serán utilizados para buscar un modelo híbrido inteligente y posteriormente incorporado en una arquitectura basada en agentes y representaciones ontológicas.

3. AGENTES ADAPTATIVOS EN IDS

Son muchas las definiciones que se han dado sobre el significado de Agentes. Podría entenderse como: "una entidad cuyo estado es visto como un conjunto de componentes mentales, tales como creencias, intenciones, deseos, capacidades, elecciones y acuerdos"[3] con características de autonomía, movilidad, reactividad, pro actividad, movilidad, veracidad, benevolencia, racionalidad. De acuerdo a estas características la incorporación de agentes a los IDS puede ayudar a resolver problemas como: [24] [25]

- Reducir la carga de la Red: Los agentes permitirían incorporar capacidades de autonomía en los nodos y solo despachar información crucial cuando sea estrictamente requerido en el IDS Distribuido.
- Superar la latencia de la red: Los agentes móviles permiten enviar información de operaciones directamente a puntos remotos, evitando cargar nodos centrales y disminuyendo la latencia.
- Ejecución asíncrona y autónoma: Los agentes pueden iniciar y terminar su operación sin comprometer otros recursos del IDS. Los agentes móviles pueden seguir trabajando de manera autónoma aun teniendo algunos recursos desconectados, incluso con un nodo central fuera de línea. [25][32][38]
- Adaptación Dinámica: Los agentes pueden ser construidos, clonados, despachados, dormidos y terminados de acuerdo a eventos de configuración en la red, cambios en la topología o situaciones de tráfico. Esto permite que nuevos agentes se generen y se envíen a estos nodos. [6]
- Robustez: Los agentes tienen la habilidad de reaccionar dinámicamente a condiciones de seguridad facilitando la construcción de sistemas distribuidos robustos.
- Escalabilidad: Los IDS basados en agentes móviles optimizan la gestión de los recursos a partir de monitoreo de tareas y responsabilidades para distribuir trabajos en los diferentes nodos, balanceando cargas, mejorando la disponibilidad y tolerancia a fallos del sistema. [21][32]

Investigaciones relacionadas [3] [6] [7] [9] [10] [11] [13] [18] [20] [24] [25] [26] [27] [28] [32] [33] han aplicado el uso de agentes de software a la detección de intrusos, algunos a partir de agentes estáticos otras utilizando agentes móviles. Muchos de estos modelos han sido iniciativas de continuidad de proyectos antecesores, cambiando algunas características o incorporando nuevos comportamientos a los agentes, e incluso llegando a términos de prototipos e implementación.

Una de las investigaciones que ha tenido más relevancia en este campo ha sido la desarrollada por el Centro de Investigación en Seguridad de la Información de la Universidad de Purdue donde se desarrolló un modelo basado en agentes inteligentes para sistemas de detección de intrusos distribuidos conocida como AAFID (Autonomous Agents for Intrusion Detection) [56]. En esta arquitectura los nodos IDS son organizados en una estructura jerárquica en árbol; el modelo se compone de Agentes, Transmisores y Supervisores. Sobre esta arquitectura se han propuesto otros modelos [32] [33] que han generado resultados y aportes importantes en la aplicación de Agentes en IDS.

4. ONTOLOGIAS EN IDS

Las ontologías representan formalmente especificaciones de conceptos que ofrecen un conocimiento compartido en un dominio definido sobre un lenguaje semántico. Una ontología está compuesta por conceptos (elementos básicos de los dominios, que se organizan en taxonomías), instancias (específicas de los conceptos), relaciones (entre los conceptos del dominio), funciones, axiomas. Las ontologías se han convertido en elementos fundamentales de los sistemas multi-Agentes, ya que permiten la comunicación entre agentes heterogéneos y hace posible la creación, la transmisión y el almacenamiento del conocimiento. Algunas investigaciones han evidenciado el uso de ontologías en modelos de seguridad, algoritmos criptográficos y en sistemas de detección de intrusos [21] [23] [40]. La utilización de estas representaciones permite estandarizar y unificar un lenguaje de comunicación homogéneo en la definición de firmas y eventos de los IDS. La evolución de una taxonomía tradicional a ontologías en el dominio de los ataques informáticos y de las intrusiones optimiza la gestión en un ambiente de IDS distribuido, ya que permite

(5). El multiplicador de las exportaciones desarrollado por Keynes,

disminuir las dificultades de representaciones y comunicaciones heterogéneas.

5.PROPUESTA PARA UNA ARQUITECTURA DE IDS BASADO EN AGENTES INTELIGENTES Y EN REPRESENTACIONES ONTOLOGICAS

Hecha una revisión del estado del arte de las técnicas inteligentes, modelos de agentes aplicados a los sistemas de detección de intrusos y representaciones ontológicas, actualmente nos encontramos trabajando en un proyecto de investigación doctoral, que consiste en diseñar e implementar una arquitectura de sistema de detección de intrusos distribuida utilizando agentes inteligentes móviles y representaciones ontológicas-semánticas, aplicando Técnicas Híbridas Inteligentes. Hasta el momento se han hecho algunas simulaciones con algoritmos de redes neuronales en IDS, sin embargo, el componente de inteligencia que aquí se plantea pretende mejorar resultados sobre la combinación de algunos métodos (computación blanda), y demostrar factores diferenciadores y características reales de optimización en la detección de nuevos eventos. El modelo de agentes en IDS distribuidos se hará tomando como referencia las arquitecturas planteadas en otras investigaciones [6] [40] [43] [46].

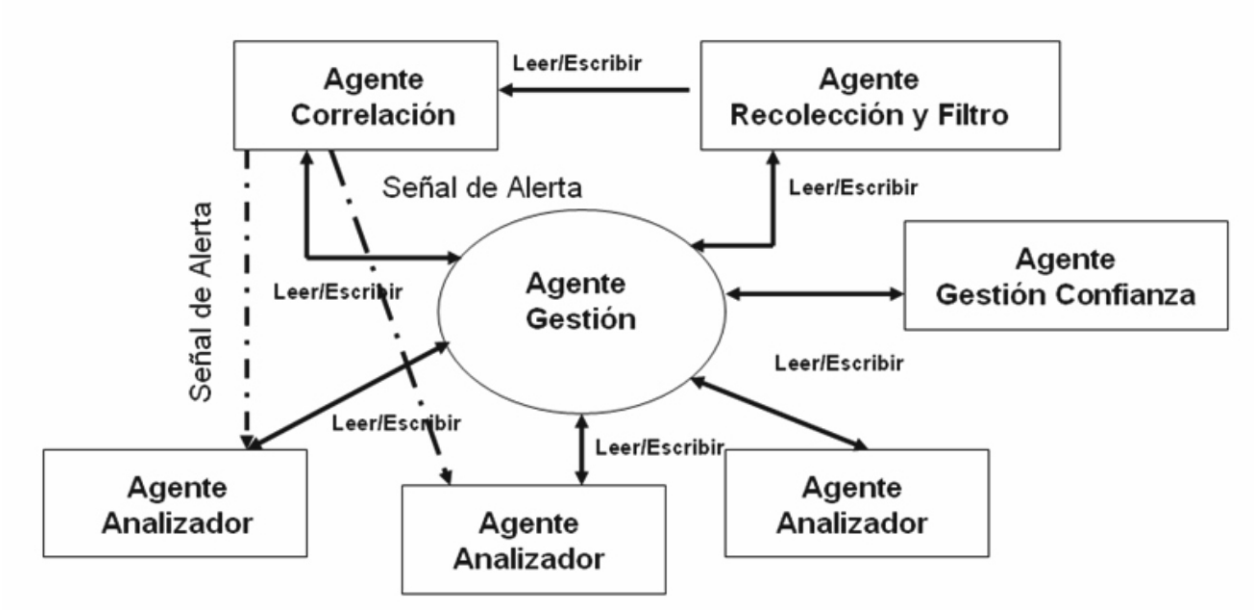
El principal aporte científico esperado con esta investigación es:

Un modelo integrado de sistemas multiagente con una arquitectura basada en técnicas híbridas de inteligencia artificial en sistemas de detección de intruso distribuido y la definición de una base de conocimiento de ataques, firmas y patrones basada en representaciones ontológicas y semánticas. Teniendo como referencia los proyectos explorados, se puede afirmar que no hay una propuesta que integre en un mismo modelo técnicas hibridas de inteligencia artificial, representaciones de ataques semánticas sobre una arquitectura basada en Agentes, adicionalmente se están probando las técnicas inteligentes a usar que serán diferentes a las ya utilizadas[4], esto se validará en el prototipo y en las simulaciones pertinentes.

Tomando como referencia la arquitectura la Figura 1, se propone una nueva arquitectura planteada en la Figura 2 con los siguientes roles:

- Agente Sensor: Captura datos de la red y filtrar la

Figura 1. Propuesta de Arquitectura IDS basado en Agentes



(4). Actualmente se encuentra en proceso de análisis un híbrido entre Redes Neuronales Artificiales y SVM (Support Vector Machines), pero esto no garantiza que sea el método a utilizar en el rol de un agente de correlación.

información pertinente. Este agente será clonado y distribuido a través del sistema de comunicación recolectando eventos, adicionalmente disminuye los falsos positivos y falsos negativos.

- Agente Analizador: Es el motor de la arquitectura. Procesa análisis de firmas, detección de anomalías y análisis de nuevos protocolos de seguridad basados en las interpretaciones del experto.
- Agente Gestor: Toma la información recolectada y la distribuye entre los agentes analizadores.

Como aporte a las arquitecturas referenciadas en esta investigación se integrarán:

Agentes onto-semánticos: Encargados de construir la base de conocimiento sobre un modelo ontológico basado en OWL.

Agentes de correlación inteligente: Su rol principal es comparar los patrones detectados contra la ontología de firmas de ataque sobre un modelo semántico que permita definir de manera autónoma nuevas reglas, y principalmente establecer nuevas reglas (a partir de técnicas híbridas Inteligentes) en una misma arquitectura.

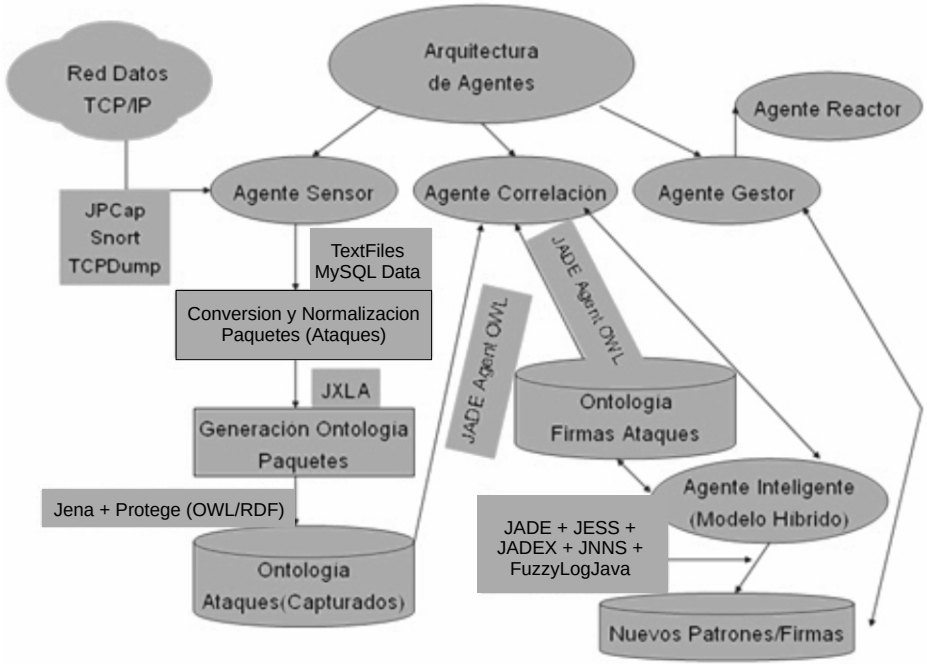
Agente de Reacción (Reactor): Recoge la información de los agentes distribuidos y con base en el modelo de alarmas toma decisiones informativas, preventivas o correctivas.

Aplicación Metodológica

Por el momento se están analizando y diseñando los modelos de representación de roles, tareas, conocimiento, interacción, sistema, recursos, arquitectura, agentes y entorno utilizando una metodología de Ingeniería de Software de Agentes[5] propuesta por uno de los autores, donde se espera validar la aplicación de una nueva metodología en el contexto del problema aquí descrito, es importante aclarar que en las investigaciones relacionadas no se evidencia la utilización de un ciclo metodológico basado en la ingeniería de Software de agentes que permita demostrar un proceso evolutivo en la construcción de sistemas inteligentes en detección de intrusos.

La metodología orientada a agentes seleccionada (UPSAM) está basadas en responsabilidades servicios, metas y facilita el diseño y comprensión de sistemas complejos como son los casos basados en arquitecturas

Figura 2. Modelo del Sistema basado en Agentes, Ontologías y técnicas hibridas Inteligentes en Detección de Intrusos



(5).Castillo, Andrés. Modelos y Plataformas de Agentes Software Móviles e Inteligentes para Gestión del Conocimiento en el Contexto de las Tecnologías de la Información. Capítulos 9. PP 1-40. 2004.

distribuidas inteligentes; ofreciendo la posibilidad de describir e integrar funcionalidades, características, aprendizaje, comunicación e interacción.

El uso de AUML (Agent UML) como lenguaje extendido para refinar y complementar los modelos propuestos por las metodologías facilitará la transición hacia el desarrollo de prototipos que validen la propuesta en mención.

En la investigación hecha por uno de los autores de este artículo[6] se planteó un modelo de IDS Neuronal, demostrando la optimización que se logra en la detección de nuevos patrones. A partir de esta iniciativa y combinando otras técnicas se lanza una hipótesis para mejorar la capacidad de inteligencia de los agentes en los nodos IDS, durante la fase de diseño, simulación y desarrollo del prototipo (del IDS usando agentes y técnicas híbridas inteligentes) se publicarán los resultados y análisis estadísticos. El modelo que se está trabajando utiliza los siguientes recursos computacionales:

- **Librería JPCAP:** Librería de Java para enviar y recibir paquetes en una red, pueden ser capturados en diferentes formatos para ser procesados.
- **JADE (Java Agent Development Framework):** Es un entorno de código abierto basado en Java para construir sistemas basados en agentes, sigue el estándar FIPA que contiene librerías para la caracterización de comportamiento, comunicación y control de los agentes. JADE soporta mensajes ACL (Agent Communication Language) para intercambiar mensajes. En el sistema propuesto se utilizará para diseñar los agentes y la comunicación entre los mismos.
- **JENA:** Es un framework para desarrollar aplicaciones semánticas, provee un API basado en lenguajes RDF (DAML+OIL y OWL) para manipular datos ontológicos. Para este proyecto se usará como aplicativo de representación semántica y ontológica de los agentes.
- **Protégé:** Es un editor de ontologías y conocimientos. Provee una interfaz amigable para definir clases, relaciones, instancias, propiedades y eventos de razonamiento. En esta investigación se utilizará como herramienta de definición ontológica de firmas y eventos.
- **Herramientas de Inteligencia, Algoritmos de Entrenamiento y Razonamiento:** Se utilizarán algoritmos de código abierto, APIS existentes en utilidades como Neuronal Networks y Fuzzy Logic ToolBox for MatLab Neuro-Solutions, Neuronal-Expert, JESS (API de Java para Sistemas Expertos), JNN (API de Java para redes neuronales), JOONE (Framework de Java para entrenar redes neuronales), JSVM (API Multi-de Java que permite definir modelos basados en SVM) y otras herramientas para el proceso de inteligencia en los componentes donde sea relevante aplicar estás técnicas.

(6). Brito J, Pérez C, Isaza Gustavo. Aplicación De Redes Neuronales Para La Detección De Intrusos En Redes Y Sistemas De Información. Scientia Et Technica Año Xi, No 27, Abril 2005. Utp. Issn 0122-1701. 2005

6. CONCLUSIONES

- En los últimos años se han evidenciado un buen número de investigaciones relacionadas con la aplicación de agentes (móviles, adaptativos, autónomos, inteligentes) en la Detección de Intrusos generando resultados de optimización importantes en los procesos de cooperación, delegación, distribución, reacción y autonomía en estos sistemas.
- El desempeño de estos modelos puede mejorar significativamente combinando técnicas probabilísticas e inteligentes en el proceso de análisis y de optimización de firmas.
- El uso de representaciones ontológicas en IDS facilita la interoperabilidad y comunicación en los IDS distribuidos donde la existencia de lenguajes heterogéneos se ha convertido en una restricción.
- Se presenta una iniciativa que se está desarrollando como investigación doctoral donde se propone integrar una arquitectura de IDS distribuidos utilizando Agentes móviles inteligentes (técnicas híbridas) y representaciones semánticas-ontológicas en su base de conocimiento.

7. REFERENCIAS

[1]Abad C., J. Taylor, C. Sengul, and W. Yurcik. “Log correlation for intrusion detection: A proof of concept”. In 19th Annual Computer Security Applications Conference, Las Vegas, NV. PP 2-10. December 2003.

[2]Allen J., A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. State of the practice of intrusion detection technologies, PP 4-6 2000.

[3]Balasubramaniyam J.S., J. O. Garcia-Fernandez, D. Isacoff, E. Spafford, and D. Zamboni. An Architecture for intrusion detection using autonomous agents. In Proceedings of the 14th Annual Computer Security Applications Conference, PP 14-16. 1998.

[4]Barbara, D., Couto, J., Jajodia, S., & Wu, N. (2001). ADAM: A testbed for exploring the use of data mining in intrusion detection. ACM SIGMOD Record, 30 (4). PP

15-24. 2001
[5]Barbara, D., Couto, J., Jajodia, S., & Wu, N. (2002). An architecture for anomaly detection. In D. Barbara & S. Jajodia (Eds.). PP 6-7. 2002
[6]Barika F., Kadhi N.. Intelligent and Mobile Agent for Intrusion Detection System: IMA-IDS Laboratoire SOIIE. Voltaire Le Kremlin Bicetre France. PP 9-14 September 30, 2003
[7]Barnett B., and Dai N. Vu. Vulnerability assessment and intrusion detection with dynamic software agents. In Proceedings of the Software Technology Conference, PP 162-167. April 1997.
[8]Bass T. Multisensor data fusion for next generation distributed intrusion detection systems. In Proceedings of the IRIS National Symposium on Sensor and Data Fusion, May 1999.
[9]Benattou M., and K. Tamine. Intelligent Agents for Distributed Intrusion Detection System. Transactions On Engineering, Computing And Technology V6. PP 4-5 June 2005
[10]Bernardes M., and E. Dos Santos Moreira. Implementation of an intrusion detection system based on mobile agents. In International Symposium on Software Engineering for Parallel and Distributed Systems, PP 8-10. 2000.
[11]Boudaoud K., N. Foukia, Z. Guessoum An Intelligent Agent Approach for Security Management, Proceeding of the 7th HP OpenView University Association Plenary Workshop, Greece. PP 12-14 June 2000.
[12]Burroughs D., L. Wilson, and George V. Cybenko. Analysis of Distributed Intrusion Detection Systems Using Bayesian Methods, PP 7. 2002.
[13]Christopher K. Applying Mobile Agent Technology to Intrusion Detection Technical University Viena, 2001
[14]Crosbie, M., and Spafford, E. H. Defending a Computer System using Autonomous Agents. 18th National Information Systems Security Conference, pp. 549558, October 1995.
[15]Curry D and H. Debar. "Intrusion detection message exchange format data model and extensible markup language (xml) document type definition." PP 2-12. January 2003.
[16]De Boer R. A Generic Architecture for Fusion-Based Intrusion Detection Systems. 2002
[17]Eckmann S, G. Vigna, and R. Kemmerer. "STATL: An Attack Language for State-based Intrusion Detection". Journal of Computer Security, PP. 71 . 104, 2002.
[18]Eid M., "A New Mobile Agent-Based Intrusion detection System Using distributed Sensors", In proceeding of FEASC, 2004.
[19]Feiertag, R., Rho, S., Benzinger, L., Wu, S., Redmond, T., Zhang, C., Levitt, K., Peticolas, D., Heckman, M., Staniford, S., & McAlerney, J. Applications of Data Mining in Computer Security (pp. 63-76). Boston: Intrusion detection inter-component adaptive negotiation. Computer Networks, 34, 605-621. 2000
[20]Fenet S. and S. Hassas, "A Distributed Intrusion Response System Based on Mobile Autonomous Agents Using Social Insects Communication Paradigm". Published by Elsevier Science B. V., pages 21-29, 2001.
[21]Gorodetski V, L. J. Popyack, I. V. Kotenko, and V. A. Skormin. "Ontology-based multi-agent model of an information security system". In 7th International Workshop, RSFDGrC, Springer, volume 1711 of Lecture Notes in Computer Science, Yamaguchi, Japan, 1999
[22]Gómez J, and Dasgupta D. Evolving Fuzzy Classifiers for Intrusion Detection. Proceedings of the 2002 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY. PP. 1-7 June 2001.
[23]Hendler J. "DARPA Agent Markup Language+Ontology Interface Layer" http://www.daml.org/2001/03/daml+oil-index, 2001.
[24]Hulmer G., J. S.K. Wong, V. Honavar, L. Miller, Y. Wang, "Lightweight Agents for Intrusion Detection", Journal of Systems and Software 67 (03), pages 109-122, 2003.
[25]Jansen W, P. Mell, T. Karygiannis, and D. Marks. "applying mobile agents to intrusion detection and response". Technical report, NIST Interim Report - 6416, October 1999.
[26] Jansen W., "Intrusion detection with mobile agents", Computer communication (15): PP: 1392-1401, 2002.
[27]Jansen W., P. Mell, Karygiannis, and D. Marks, "Applying mobile agents to intrusion detection and response," Interim Report (IR) 6416, NIST, October 1999.
[28]Kannadiga P.; Zulkernine, M.; "DIDMA: a distributed intrusion detection system using mobile agents", Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. PP. 238 245. May 2005.
[29]Kumar, S. Classification and Detection of Computer Intrusions. PhD thesis, Department of Computer Sciences, Purdue University. West Lafayette, IN, 1995.
[30]Kumar, S., and Spafford, E. H. An Application of Pattern Matching in Intrusion Detection. Tech. Rep. CSDTR94013, Department of Comptuter Sciences, Purdue University, West Lafayette, IN, June 1994.
[31]Kuregel W., T. Toth, and E. Kirda. Service Specific. "Anomaly Detection for Network Intrusion Detection". In Symposium on Applied Computing (SAC). ACM Scientific Press, PP 9,22. March 2002.
[32]Krügel C., T. Toth, and E. Kirda, "Sparta - a mobile agent based intrusion detection system," in IFIP Conference on Network Security, Belgium, 2001, Kluwer Academic Publishers.
[33]Krügel C., T. Toth. Flexible, Mobile Agent Based Intrusion Detection for Dynamic Networks Distributed Systems Group, Technical University Vienna A-1040 Argentinierstrasse 8, Viena 2001
[34]Kumar S,Spafford EH. A software architecture to support misuse intrusion detection. In: Proceedings of the 18th national information security conference,1995. p. 194204.
[35]Kumar S,Spafford EH. An application of pattern matching in intrusion detection. Technical Report CSD-

TR-94-013,Purdue University,1994.
[36]Kumar S. Classification and detection of computer intrusions. PhD thesis, Department of Computer Science,Purdue University,August 1995.
[37]Lee W and S. Stolfo. "Data Mining Approaches for Intrusion Detection". Proc. 1998. 7th USENIX Security Symposium, 1998.
[38]Lippmann R, D. Fried, I. Graf, J. Haines, K. Kendall, D. McClung, D. Weber, S. Webster, D. Wyschogrod, R. Cunningham, and M.Lugmayer W., "Gypsy: A component-based mobile agent system," in 8th Euromicro Workshop on Parallel and Distributed Processing (PDP 2000), Rhodos, Greece, January 2000.
[39]Mahoney M. and P. Chan. "Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks". In Proceedings of the 8th International Conference on Knowledge Discovery and Data Mining, 2003
[40]Mandujano S. Multiagent Approach to Outbound Intrusion Detection. Ph.D. thesis. Instituto Tecnológico y de Estudios Superiores de Monterrey Monterrey Campus Doctoral Program in Artificial Intelligence. PP 1-5. Diciembre 2004
[41]Mandujano S., A. Galván. Outbound Intrusion Detection. Center for Intelligent Systems Instituto Tecnológico y de Estudios Superiores de Monterrey. Monterrey, NL . 64849, Mexico. PP 2-3. 2004
[42]McHugh J.. Intrusion and intrusion detection. CERT Coordination Center, Carnegie Melon University, Springer.Verlag, July 2001.
[43]Mell P., M. McLarnon. Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems. 1999
[44]Méndez J.R., F. Fdez-Riverola, F. Díaz, J. Corchado Sistemas inteligentes para la detección y filtrado de correo spam. U Vigo, U. Valladolid, U. Salamanca. PP 8-11. 2006
[45]Mukkamala S, Sung AH, Abraham A. Modeling intrusion detection systems using linear genetic programming approach,The 17th international conference on industrial & engineering applications of artificial intelligence and expert systems, innovations in applied artificial intelligence. Germany: Springer; 2004a. PP. 63342.
[46]Nagesh A. Distributed Network Forensics using JADE Mobile Agent Framework , Graduate Student, Arizona State University, Division of Computing Studies, Sutton Hall, Suite 140, 7001 E. Williams Field Rd, Mesa, AZ 85212. 2006
[47]Ning P., Probalistic states in Network Security. North Carolina State University Sushil Jajodia, George Mason University. 2003
[48]Northcutt S., M. Cooper, M. Fearnow, and K. Frederick. Intrusion Signatures and Analysis. New Riders, SANS GIAC, Indianapolis, IN, 1st edition, January 2001.
[49]Peddabachigaria S, A. Abrahamb, C. Grosanc, J. Thomasa. "Modeling intrusion detection system using hybrid intelligent systems". Computer Science Department, Oklahoma State University, Chung-Ang University, Seoul, Republic of Korea, Department of Computer Science, Babes-Bolyai University, Cluj-Napoca 3400, Romania. 2005
[50]Pouzol J. and M. Ducasse. "Formal specification of intrusion signatures and detection rules". In Proceedings of 15th Computer Security Foundations Work-shop (CSFW'02), IEEE Computer Society Press, 2002
[51]Robertson W., G. Vigna, C. Kruegel, R. Kemmerer. "Using Generalization and Characterization Techniques in the anomaly-based Detection of Web Attacks Reliable". Software Group Department of Computer Science. University of California, Santa Barbara. (2006)
[52]Sebyala, A. A., Olukemi, T., and Sacks, L. Active Platform Security through Intrusion Detection using Naive Bayesian Networks for Anomaly Detection. London Communications Symposium, 2002.
[53]Staniford-Chen S., S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C.Wee, R. Yip, and D. Zerkle, Grids - a graph based intrusion detection system for large networks, in Proceedings of the 20th National Information Systems Security Conference, vol. 1, pp. 361370. October 1996
[54]Yoo S. Case Based Reasoning Approach to Intrusion Detection. Information Assurance Engineering Lab Electrical and Computer Engineering Dept. University of Alabama in Huntsville. PP 4-22. 2005.
[55]Zamboni D.. Doing Intrusion Detection using Embedded Sensors. PhD thesis, Purdue University, West Lafayette, IN, PP. 54-88. 2000.
[56]Zamboni D., Balasubramaniyan J., Garcia-Fernandez J., E. H. Spafford., Department of Computer Sciences, Purdue University; Coast TR 98-05. 1998