Título: MOVICAB-IDS: A MOBILE HYBRID INTRUSION DETECTICON SYSTEM (MOVICAB-IDS: SISTEMA DE DETECCIÓN DE INTRUSIONES HÍBRIDO Y MOVIL)

Nombre: Herrero Cosío, Álvaro

Universidad: Universidad de Burgos

Departamento: INGENIERIA CIVIL E INDUSTRIAL

Fecha de lectura: 24/09/2009

Programa de doctorado: INGENIERÍA CIVIL E INDUSTRIAL

Dirección:

> **Director:** EMILIO SANTIAGO CORCHADO RODRIGUEZ

Tribunal:

> **presidente:** LUIS ALONSO ROMERO

> **secretario:** JAVIER SEDANO FRANCO

> **vocal:** MANUEL GRAÑA ROMAY

> **vocal:** BODGAN GABRYS

> **vocal:** RAFAEL CORCHUELO GIL

Descriptores:

> INFORMATICA

> INTELIGENCIA ARTIFICIAL

El fichero de tesis ya ha sido incorporado al sistema

Localización: SERVICIO DE GESTIÓN ACADÉMICA

Resumen: Esta tesis doctoral expone un trabajo de investigación en el campo de la Detección de Intrusiones (DI) a nivel de red, desarrollado bajo los enfoques de visualización y sistemas inteligentes híbridos. Como resultado del mismo, se ha diseñado un Sistema de Detección de Intrusiones (SDI) denominado MOVICAB-IDS (MObile

Esta tesis doctoral expone un trabajo de investigación en el campo de la Detección de Intrusiones (DI) a nivel de red, desarrollado bajo los enfoques de visualización y sistemas inteligentes híbridos. Como resultado del mismo, se ha diseñado un Sistema de Detección de Intrusiones (SDI) denominado MOVICAB-IDS (MObile VIsualization Connectionist Agent-Based IDS), que se presenta, describe y valida en esta tesis.

El SDI propuesto combina diferentes paradigmas del campo de la Inteligencia Artificial (IA) para visualizar tráfico de red con el objetivo de llevar a cabo DI a nivel de paquete. Para ello se ha diseñado un Modelo Híbrido basado en un Sistema Multiagente que incluye Agentes Deliberativos capaces de aprender y evolucionar con su entorno. Estos agentes combinan un Modelo Neuronal Proyeccionista basado en Aprendizaje no Supervisado y el paradigma de Razonamiento Basado en Casos. Mediante la aplicación del mencionado modelo neuronal,

MOVICAB-IDS extrae proyecciones interesantes de un conjunto de datos de tráfico de red y las presenta mediante un interfaz de visualización móvil. Como resultado de visualizar cada paquete y preservar el contexto temporal, MOVICAB-IDS ofrece al administrador de red una visión sintética e intuitiva del tráfico de red y de las interacciones de los diferentes protocolos. Esta visualización permite la detección e identificación de situaciones anómalas e intrusiones de un simple vistazo. Además, ayuda a conocer la estructura interna y el comportamiento de los datos de tráfico, permitiendo la supervisión de la actividad de una red.

Para comprobar su funcionamiento, MOVICAB-IDS ha sido aplicado a ciertos dominios con diferentes ataques y situaciones anómalas. Se ha generado un conjunto real de datos propio (GICAP-IDS) que contiene ejemplos de los ataques en los que se centra MOVICAB-IDS: escaneos y ataques relacionados con SNMP. Estos tipos de ataques han sido también analizados para el conocido conjunto de datos DARPA 1998. Se ha desarrollado una novedosa técnica para la prueba de SDI orientados a visualización que ha sido aplicada al SDI propuesto. Esta técnica se basa en la mutación del tráfico relacionado con situaciones anómalas para la simulación de nuevos ataques. Además, el modelo neuronal propuesto se ha comparado con otros modelos neuronales orientados a la visualización de datos.