

**Modelo de Detección, Supervisión
y Prevención de Ataques basado
en una arquitectura *Honeynet*
para la correlación semántica
basada en ontologías sobre la
Red RADAR**

Gustavo Isaza E., Ph.D.
[Grupo de Investigación GITIR]
U. de Caldas
gustavo.isaza@ucaldas.edu.co

Índice

- Situación Actual**
- Solución propuesta**
- Resultados**
- Aplicaciones**

Áreas de Investigación

- Seguridad Informática**
- Web Semántica y Ontologías**
- Gestión Inteligente**
- Computación Distribuida**

Problemática Actual

- Problemas de Representación Homogénea (Modelos sintácticos)**
- Gestión de la Seguridad Informática No Autónoma, centralizada y dependiente**
- Recursos Ociosos**
- Seguridad en Redes *Correctiva y No Preventiva***

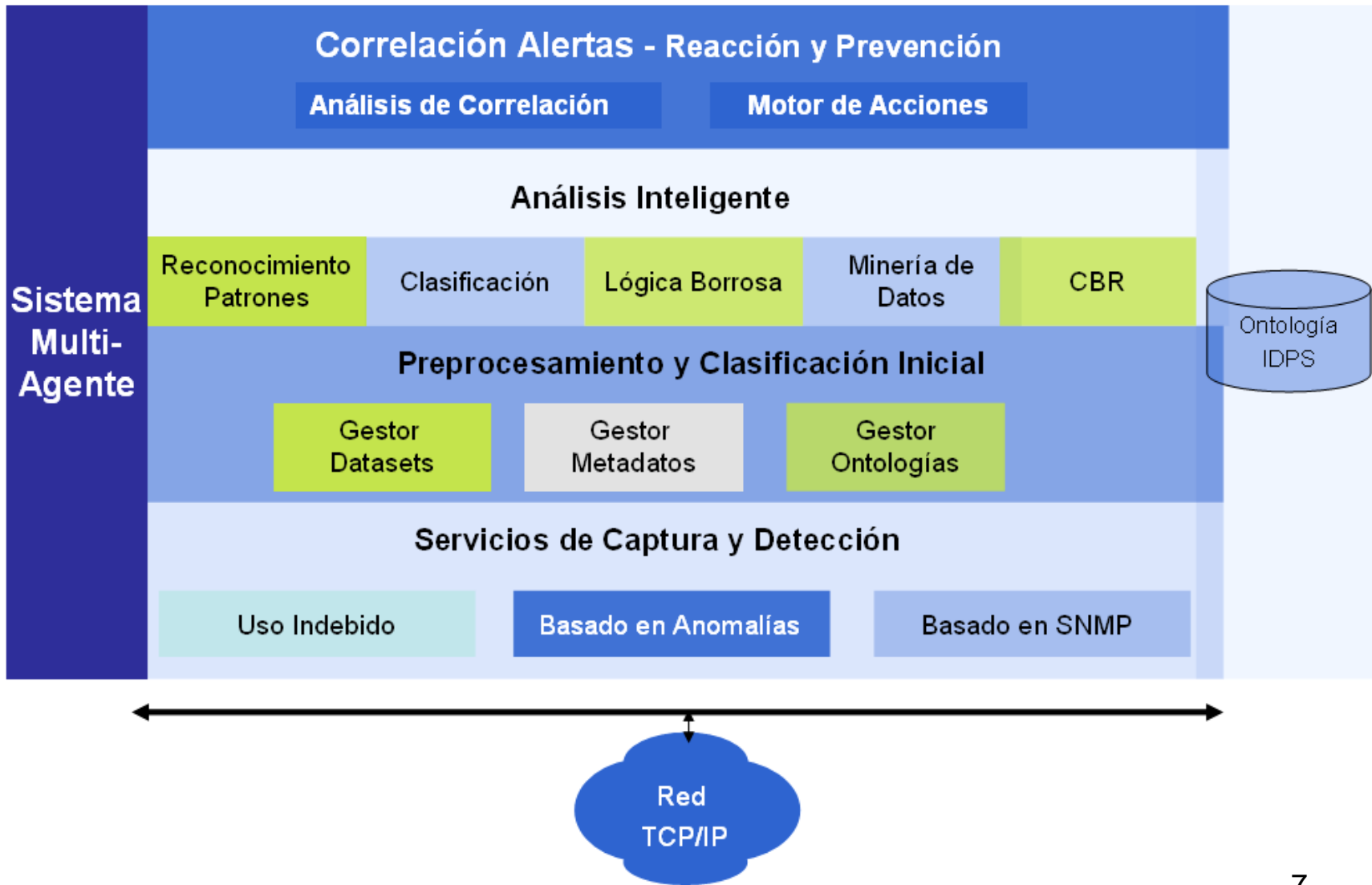
Objetivo

Desarrollar un Sistema de Detección y Prevención de Intrusiones basado en arquitecturas de Redes Señuelo usando inteligencia computacional híbrida y distribuida, con procesamiento Ontosemántico.

Motivaciones y Justificación

- Ventajas en el uso de Agentes**
- Ventajas en la representación homogénea**
- Aportes desde la Web Semántica/Ontologías**
- Aportes de la Inteligencia Computacional Distribuida**

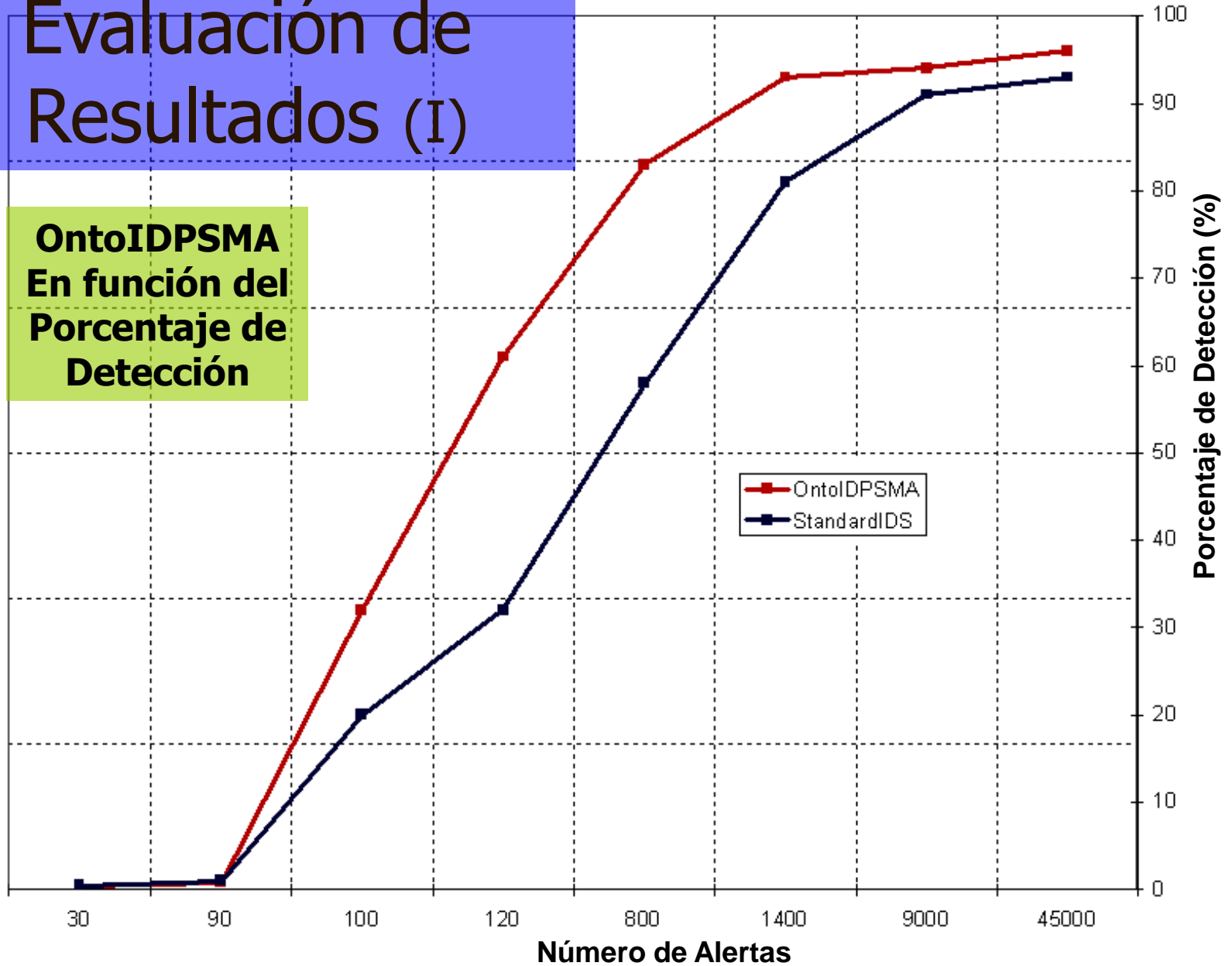
Integración OntoIDPSMA



M
o
d
e
l
o

Evaluación de Resultados (I)

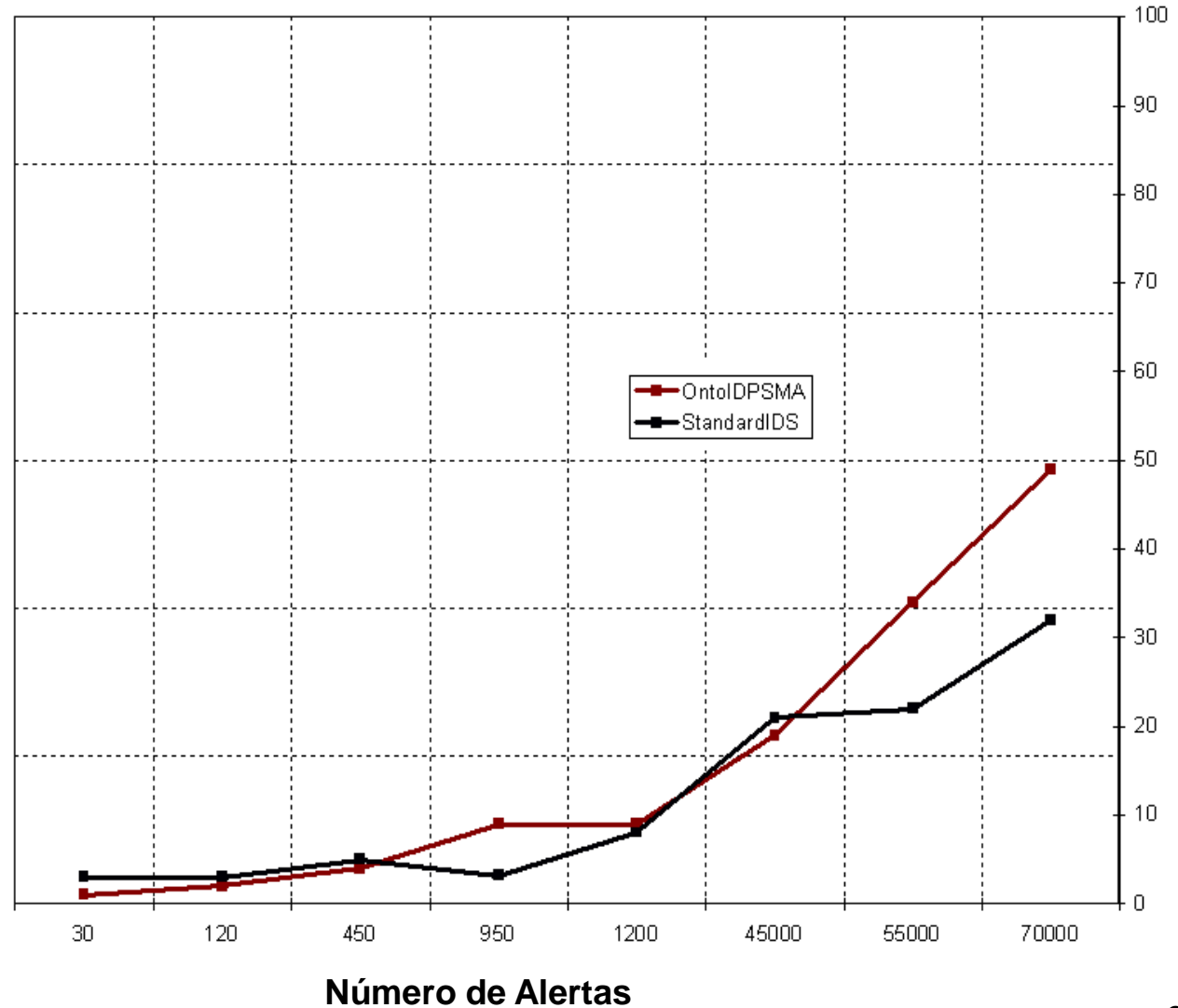
OntoIDPSMA
En función del
Porcentaje de
Detección



Evaluación de Resultados Parcial

OntoIDPSMA en función del % de CPU (IA + R)

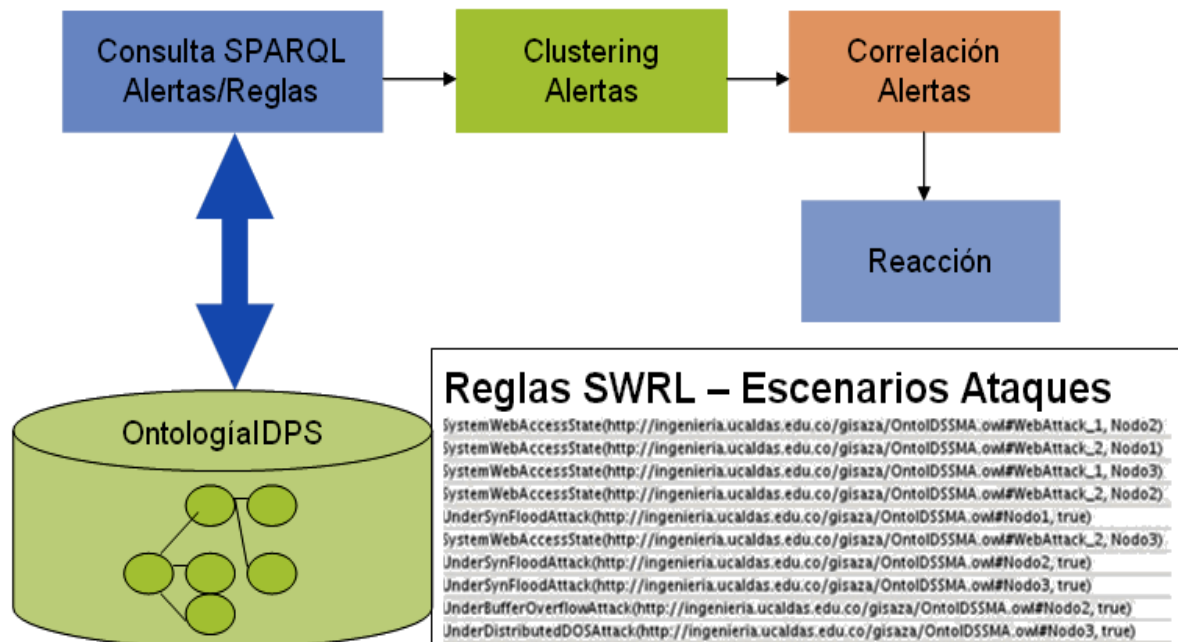
USO CPU(%)
Con IA,
Ontología
OWL y
Razonamiento



Trabajo Actual

- ❑ Gestión de Agentes en Tiempo Real
- ❑ Modelo de Sensores basado en Redes Señuelo

- ❑ **Correlación Semántica Distribuida de Intrusiones basada en Agentes y Ontologías (RADAR)**



Producto y Aplicación

- ❑ Optimización de Sistemas de Detección de Intrusiones (*Parámetros de Detección Satisfactoria, Falsos Positivos, Falsos Negativos, Tasa de Sensibilidad, Curvas ROC, Precisión ..*)
- ❑ Ontología de Detección y Prevención de Intrusiones (Razonamiento, Inferencia, Correlación Semántica)
- ❑ IDS Distribuidos Inteligentes