# SEGURIDAD EN REDES AD-HOC (Estado Del Arte)

Carlos Felipe Téllez Castaño

# AGENDA

- Introducción
- Requisitos de Seguridad MANET
- Aspectos Claves en la seguridad MANET
- Detección de Intrusos (IDS)
- Seguridad en el Enrutamiento
- Gestión de Claves

# INTRODUCCIÓN (I)

**Definición:**

- **Una red móvil Ad-Hoc, también conocida como MANET (Mobile Ad-Hoc Network) consiste en un conjunto autónomo y espontáneo de Routers o Nodos móviles que se comunican entre sí a través de conexiones wireless, dónde no existe una infraestructura de red fija y la gestión se realiza de forma distribuida.**

# INTRODUCCIÓN (II)

**Características:**

- **Topología dinámica.**
- **Enlaces de ancho de banda limitado.**
- **Enlaces de capacidad variable.**
- **Limitaciones de energía.**
- **Limitaciones de capacidad de procesamiento en los nodos.**
- **Seguridad física limitada.**

# INTRODUCCIÓN (III)

**Enrutamiento:**

- **Protocolos proactivos: Siempre mantienen una ruta hacia todos los nodos.**
- **Reactivos: Actúan según necesidad de transferencia.**
- **Basados en cluster: Según la densidad de nodos por área.**

# Requisitos en la seguridad

- Confidencialidad
- Integridad
- Autenticación
- No repudiación
- Disponibilidad

# Aspectos Claves en la seguridad MANET

- Sistemas de detección de intrusiones (IDS)
- Seguridad de los protocolos de Enrutamiento
- Servicios de gestión de claves

# Sistemas de Detección de Intrusos IDS

- **Arquitectura distribuida y cooperativa: Cada nodo de la red ejecuta un agente IDS (**Y. Zhang, W. Lee. "Intrusion detection in wireless ad-hoc networks". Mobile Computing and Networking**)**
- **IDS distribuido basado en tecnología de agentes móviles: Entidades software autónomas (**O. Kachirski, R. Guha. "Intrusion detection using mobile agents in wireless ad hoc networks" **)**

# Seguridad en Enrutamiento

- **Problema: Manipulación de la información de enrutamiento por parte de agentes externos o internos a la red.**
- **Ataques: Activos y Pasivos**
- **Activos: Inyección de información errónea de encaminamiento, reenvío de información de encaminamiento antigua y distorsión de la información de encaminamiento intercambiada entre los nodos de la red.**

# Soluciones de Seguridad

- **TIARA.**
- **SRP: Proporciona información de conectividad correcta, actualizada y autenticada a cada par de nodos que desean establecer una comunicación segura.**
- **SEAD, basado en parte en el protocolo de encaminamiento ad-hoc *Destination-Sequenced Distance-Vector* (DSDV).**

# Gestión de Claves

- ***Autoridad de certificación*** **(AC): Ente que define los sistemas criptográficos de clave pública.**
- **Criptografía simétrica: Clave secreta entre grupo de nodos.**