



# **A NEW HOD BASED INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORK**

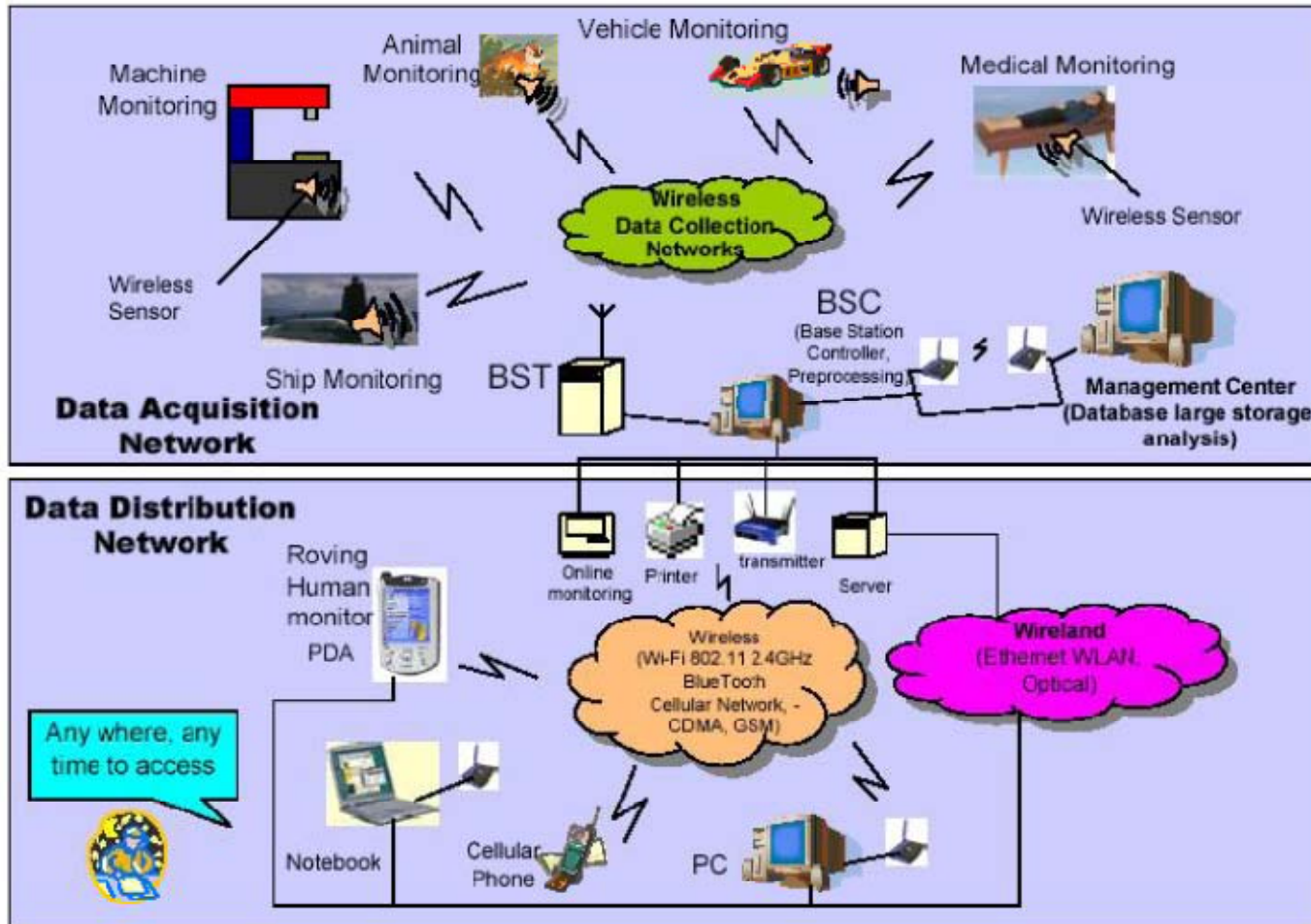
**IK2206: Internet Security and Privacy**

**Sumanta Saha  
Md. Safiqul Islam  
Md. Sakhawat Hossen**

# WIRELESS AD HOC NETWORK

- Wireless ad hoc networks are autonomous nodes that communicate with each other in a decentralized manner through multi-hop radio network
  - Mobile ad hoc networks (MANET)
  - Wireless sensor networks (WSN).

# WIRELESS SENSOR NETWORK



# COMMON SECURITY VULNERABILITIES

- Lack of infrastructure
- Shared wireless medium
- Cooperative nature between the nodes
- Easy physical accessibility
- Dynamic network topology
- Operational constraints
  - Low Battery Life
  - Small Memory
  - Limited Processing Capability

# TYPES OF ATTACKS

- Sleep Deprivation Torture
- Network Partition Attack
- Wormhole Attack
- Sybil Attack
- Sinkhole Attack
- Selective Forwarding

# INTRUSION DETECTION SYSTEM

- *“Intrusion detection and response is the task of monitoring systems for evidence of intrusions or inappropriate usage and responding to this evidence.”* - Network Security Bible
- Wireless IDS needs to face more threats than wired IDS
  - Broadcast media
- Even more special IDS required for WSN
  - Low processing power
  - Limited battery backup

# OUR PROPOSED MODEL

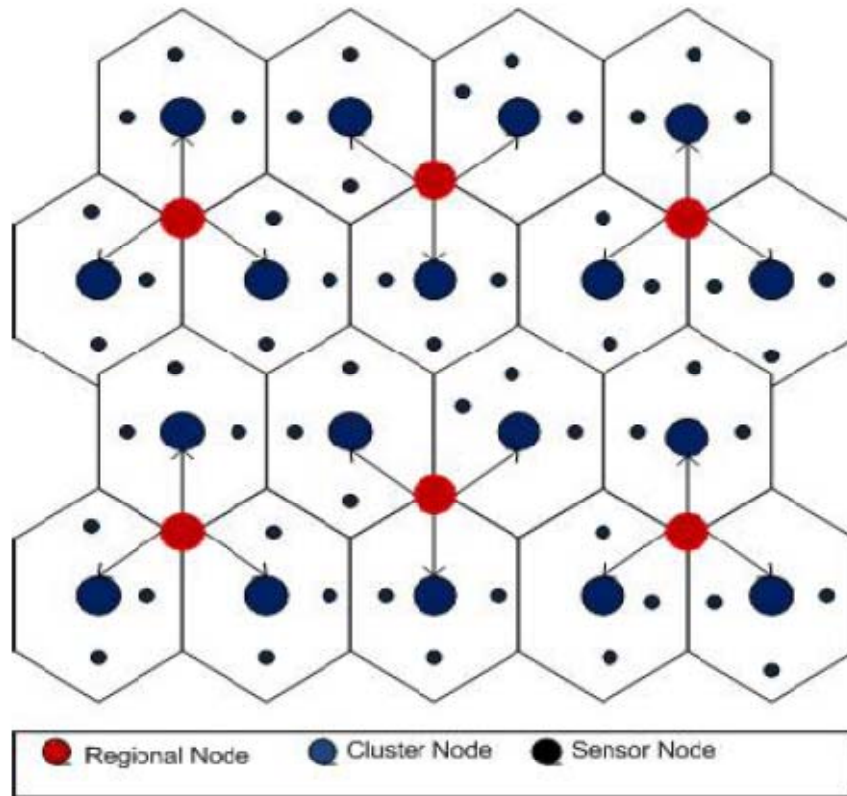


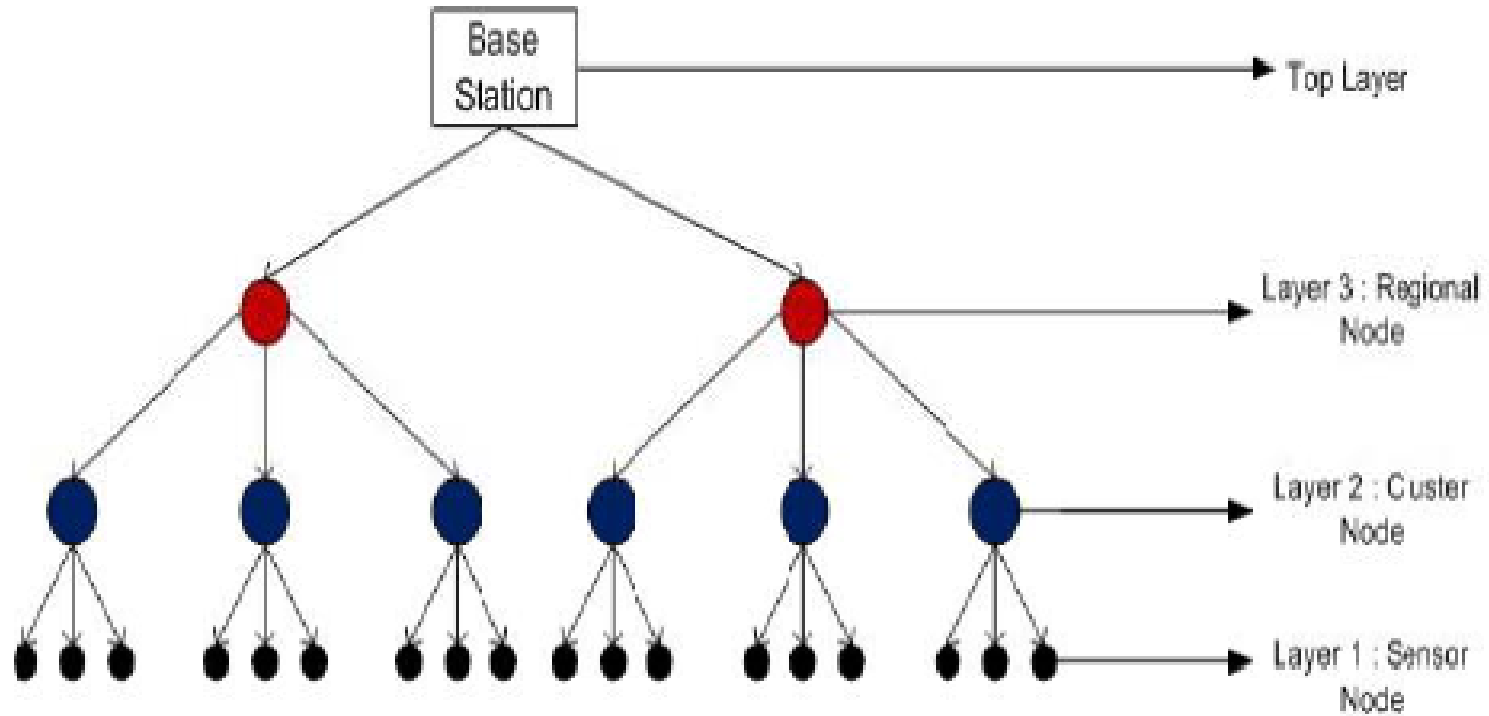
Figure 1: Hierarchical Overlay Design

## OUR PROPOSED MODEL (CONTD..)

- GSM cell based.
- Four Layer architecture
- Sensor Node - Sensing the environment
- Cluster Node - Monitoring Sensor nodes, Data collection
- Regional Node - Monitoring three neighbor cluster nodes
- Base station - Monitors Regional nodes and distributes collected data



# OUR HOD ARCHITECTURE



*Figure 2: Four Layer Architecture*

# MONITOR NODE

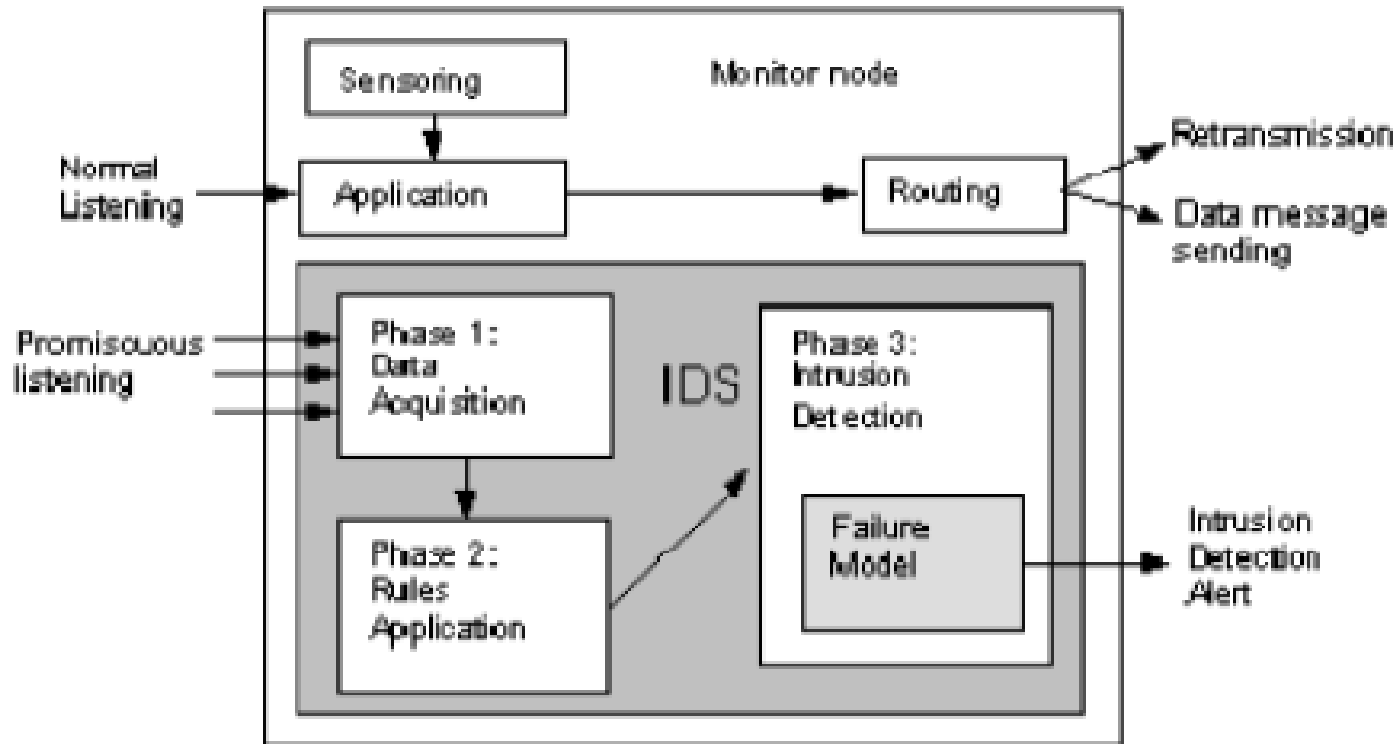


Figure 3: Monitor Node

# ID MECHANISM

- Multi Layer IDS.
- Robustness
- Physical Layer – RSSI (Received Signal Strength Indicator).
- MAC Layer- SMAC and TDMA
- Network Layer – Route tracing
- Application Layer – Three Layer Watchdog

# APPLICATION LAYER

- Three level watchdog
  - Base Station
  - Regional Node
  - Cluster Node

# IDS

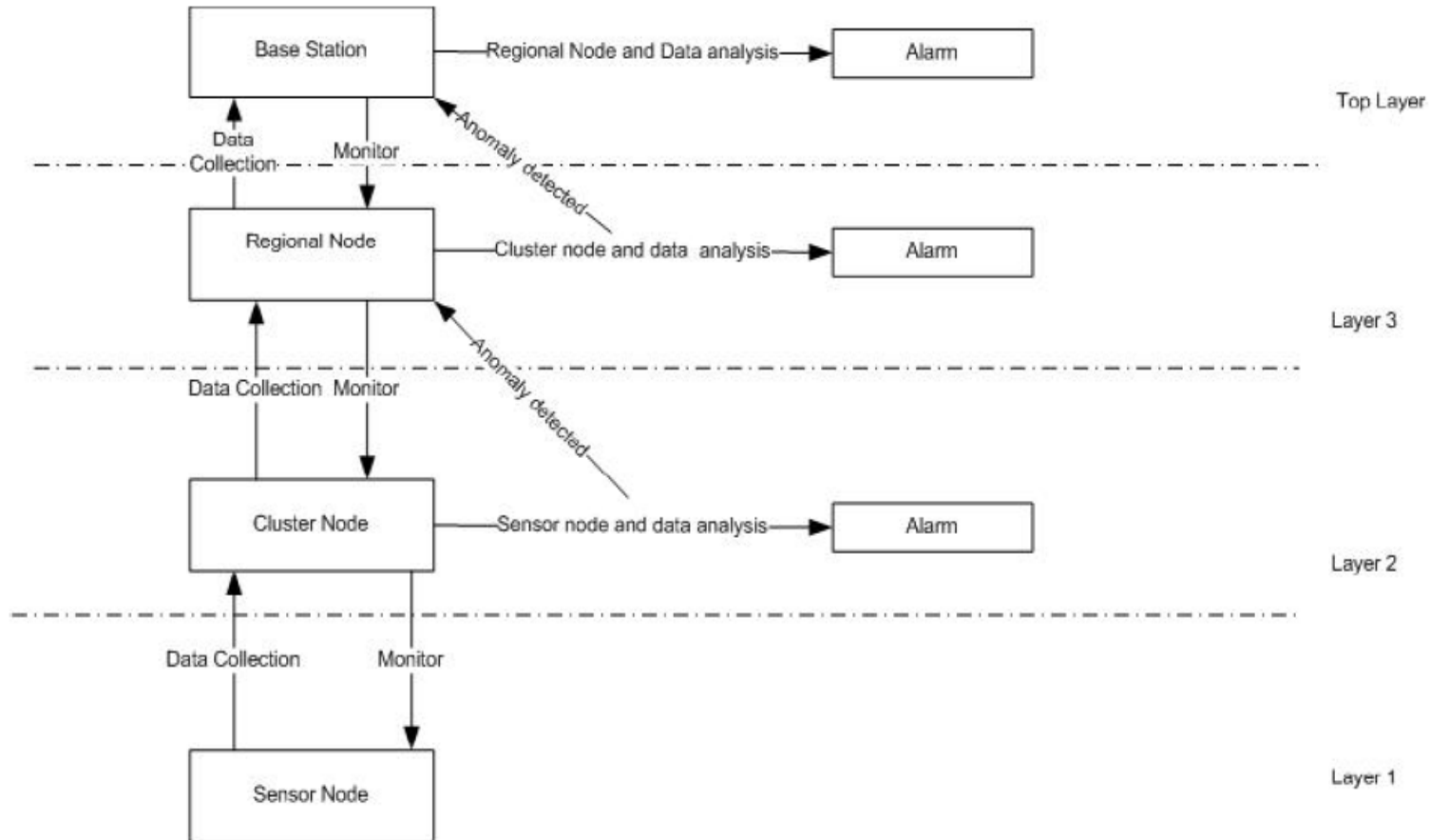


Figure 4: Intrusion Detection System

# FUTURE WORK

- *Election procedure to select cluster and regional node*
- *Building our own Simulator*

# Discussion and Questions