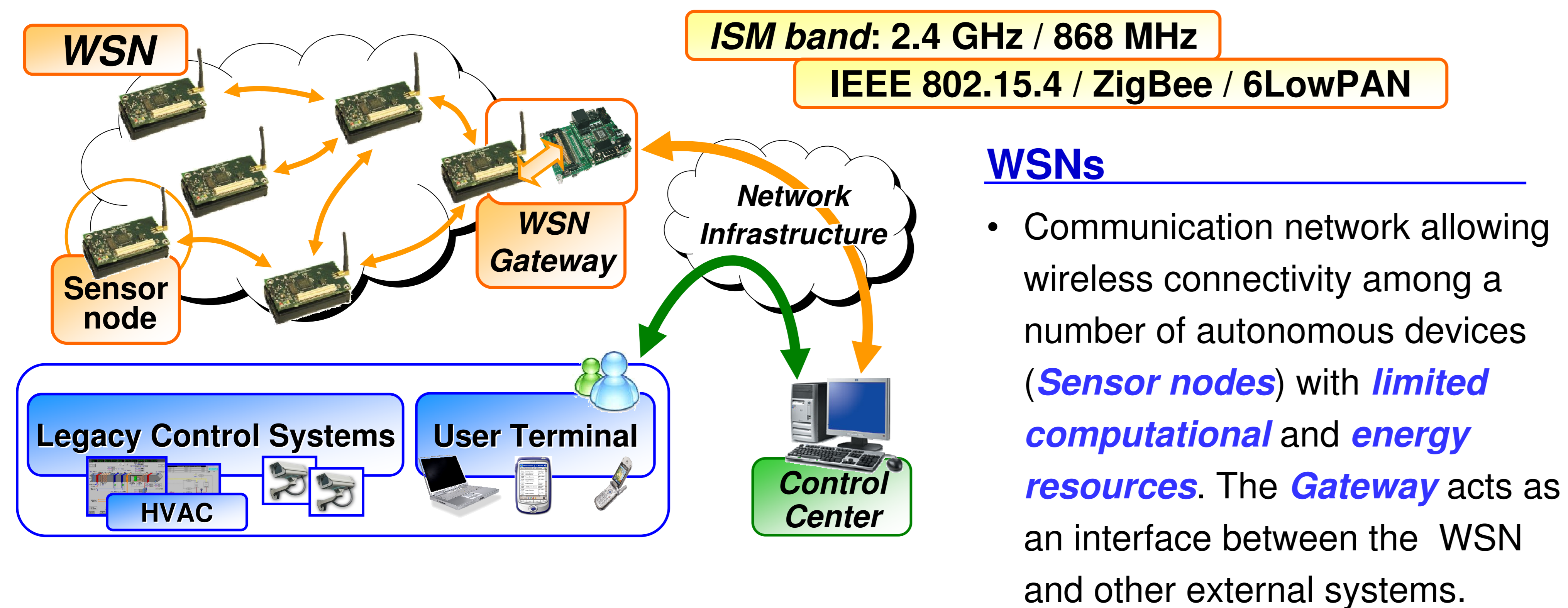


# Security in Wireless Sensor Networks

## Wireless Sensor Network (WSN) Scenario



### WSN main characteristics

- *Low data-rate* (about ten of kbps)
- *Low RF output power* (typical 0 dBm) → short range transmission
- *Self-configuration* and *self-organization* → fault tolerance, adaptability, flexibility
- *Multi-hop routing* mechanisms
- *Cooperative* approach

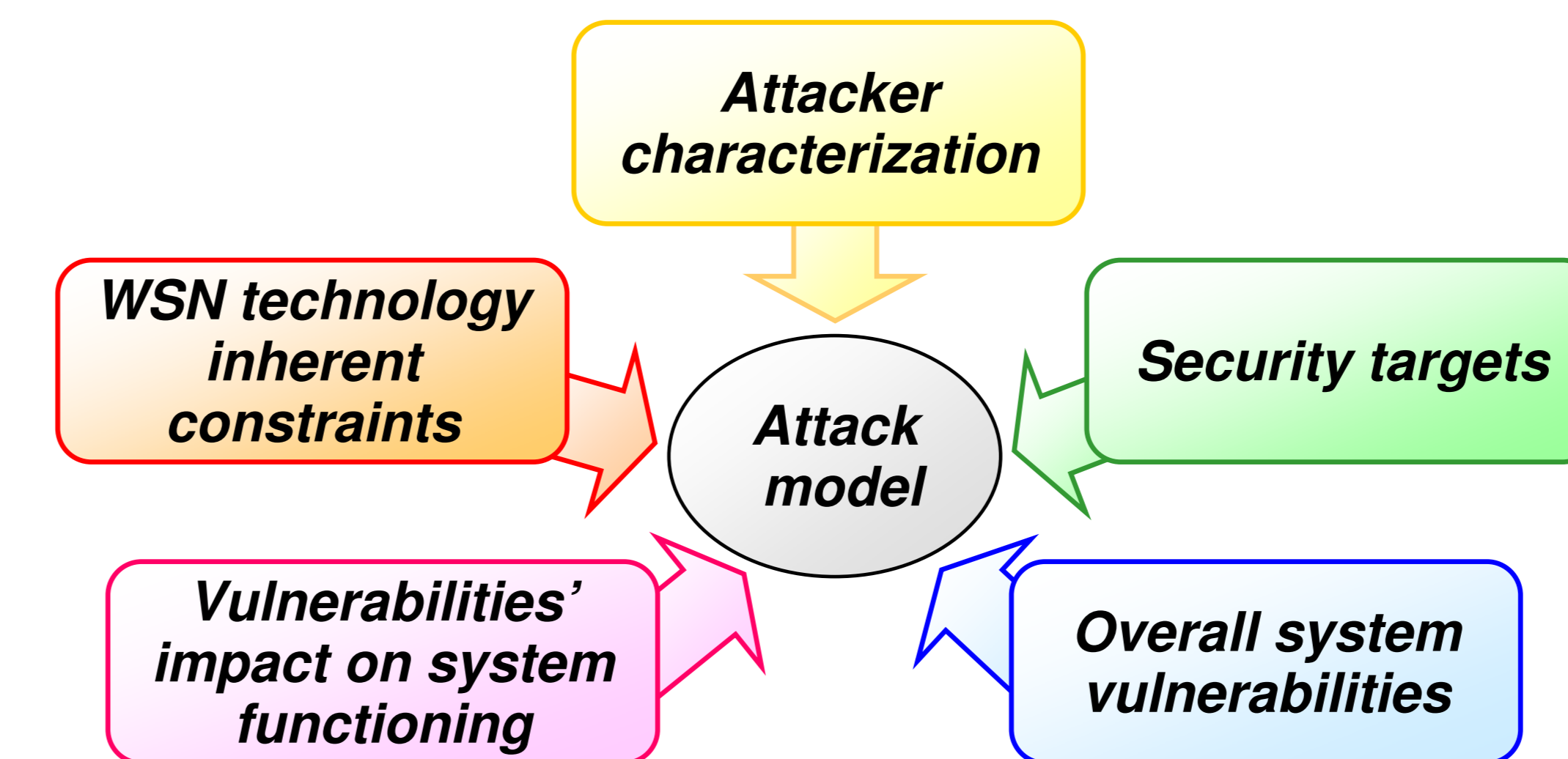
**Security Objectives.** Authentication, secrecy, availability, service integrity, privacy

**Open issues.** Group communication confidentiality, Trust modeling, impact of *mobility* on WSN security

## Attack Model

### Main goals

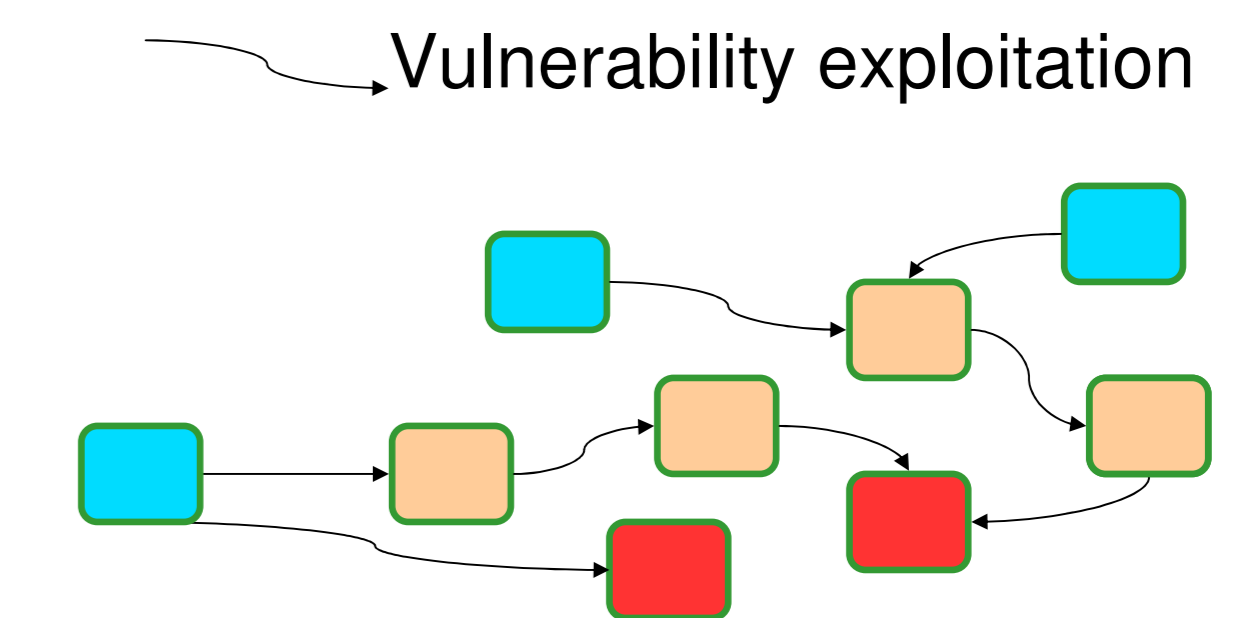
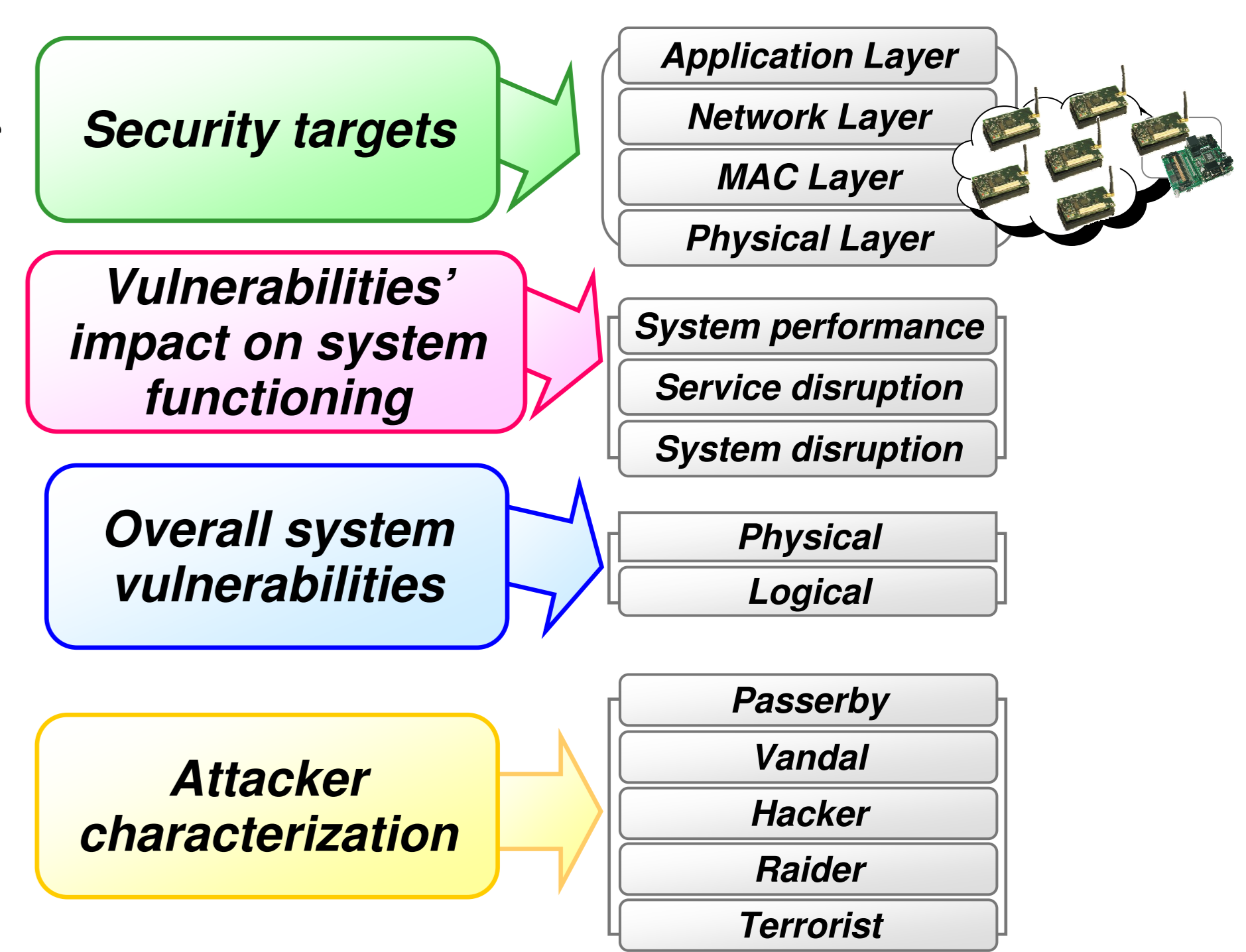
- To determine which vulnerabilities can be tolerated
- To select the most appropriate defense mechanisms to be employed in WSNs.



### Attack model analysis

- Attack graph based security analysis tool
- By input models, attack graph is created and automatically analyzed
- Achievable attacker goals are identified

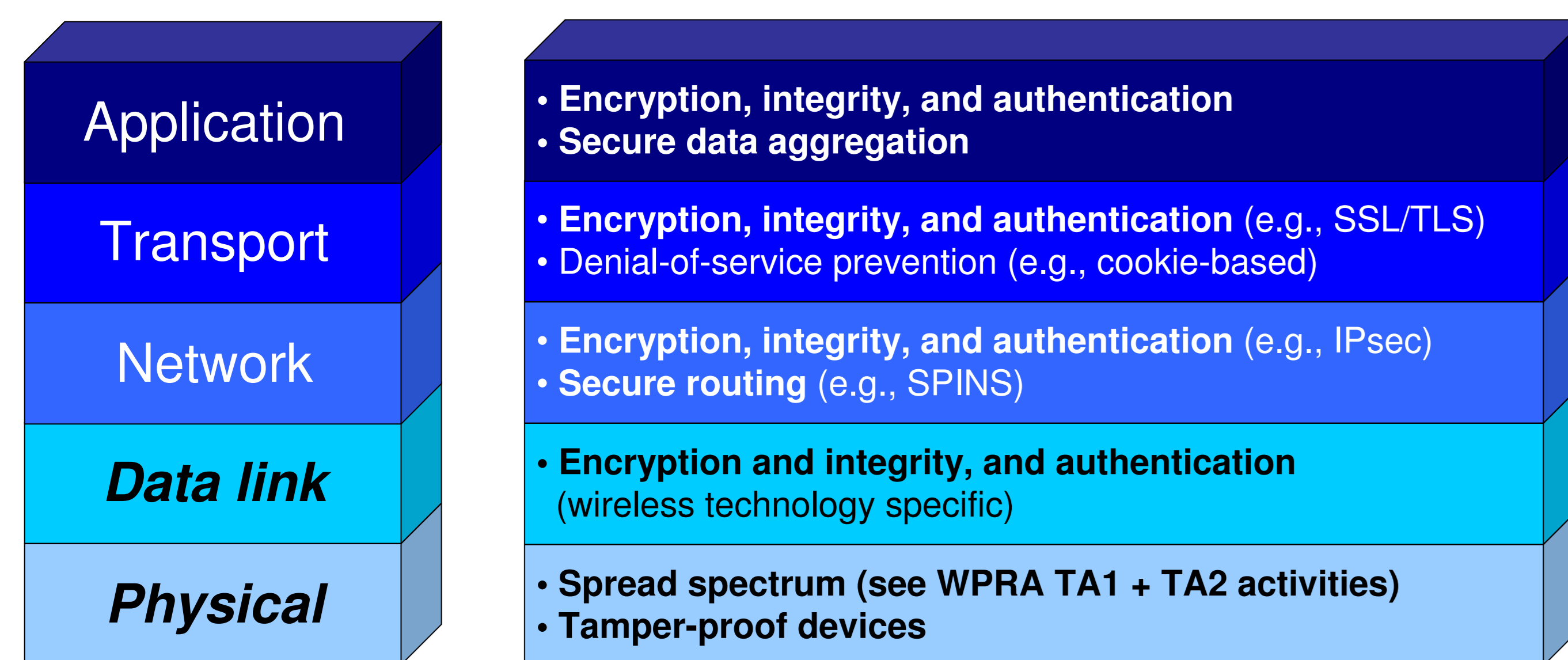
### Attack model components



## Security Countermeasures

### Communication stack

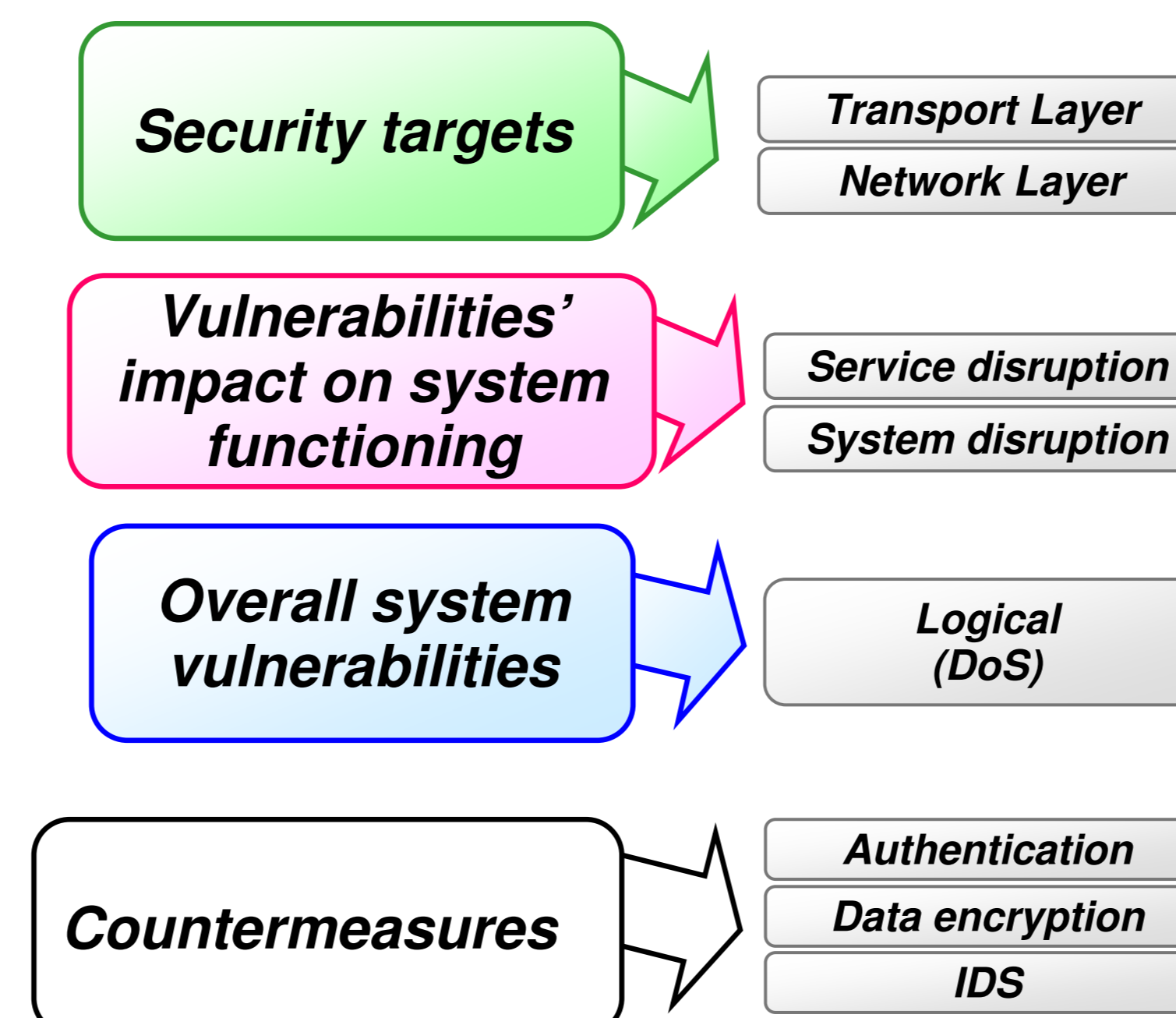
### Security countermeasures



### Selective forwarding attack

**Goal:** Insert malicious nodes in the WSN

Drop packets → Denial of Service (DoS)



## Concrete Examples

### Traffic analysis attack

**Goal:** Analyze the traffic in order to deduce the sensors' positions and to destroy them with a logical or physical attack

