Security Management in Wireless Sensor Networks

Sarmistha Neogy

Dept. of Computer Science & Engineering
Jadavpur University, Kolkata, India

Agenda

Introduction

Challenges in WSN

Attacks in WSN

Managing Security and Integrity in WSN

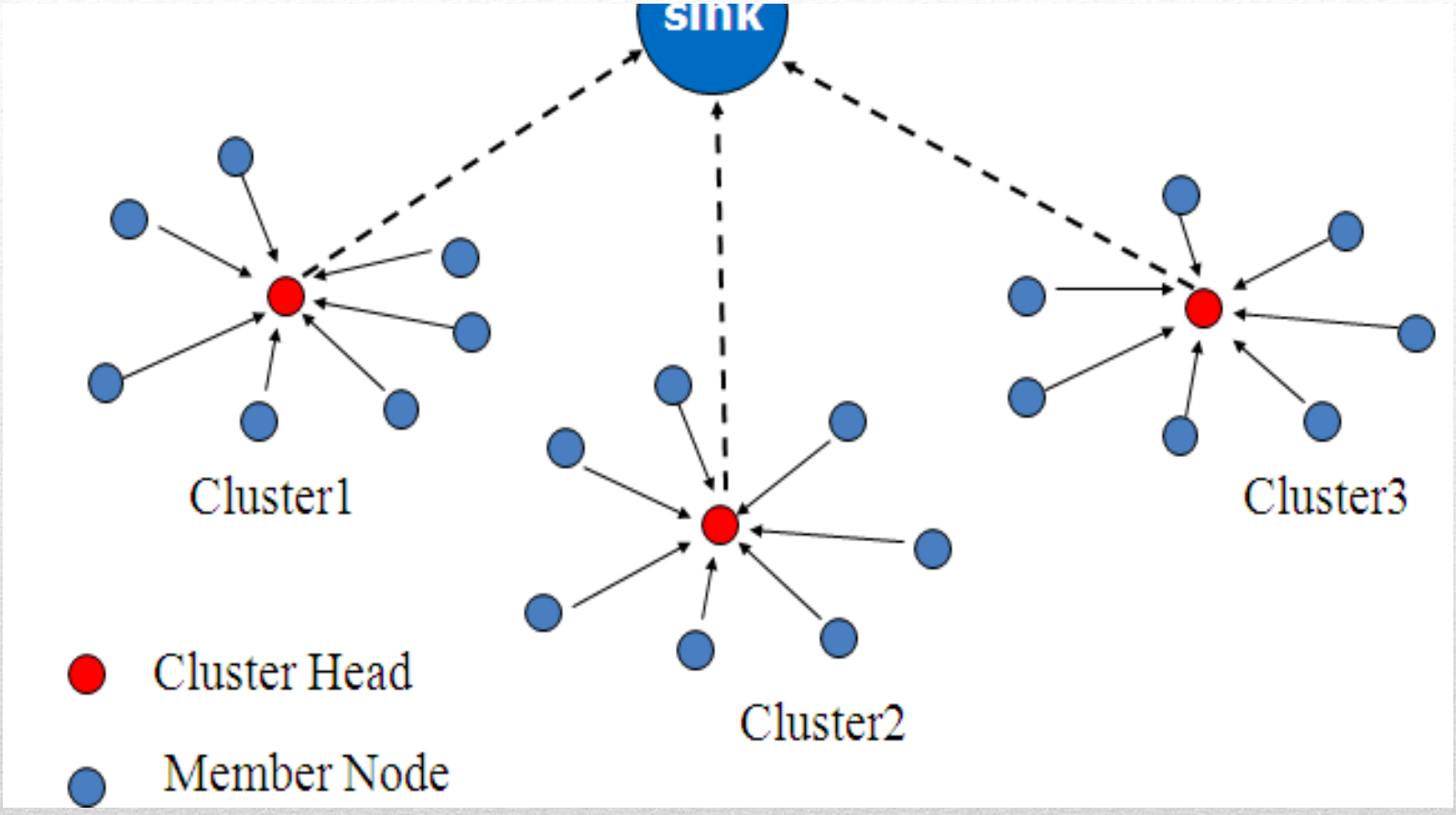
Secure Routing Protocols

Security Issues in Heterogeneous Networks

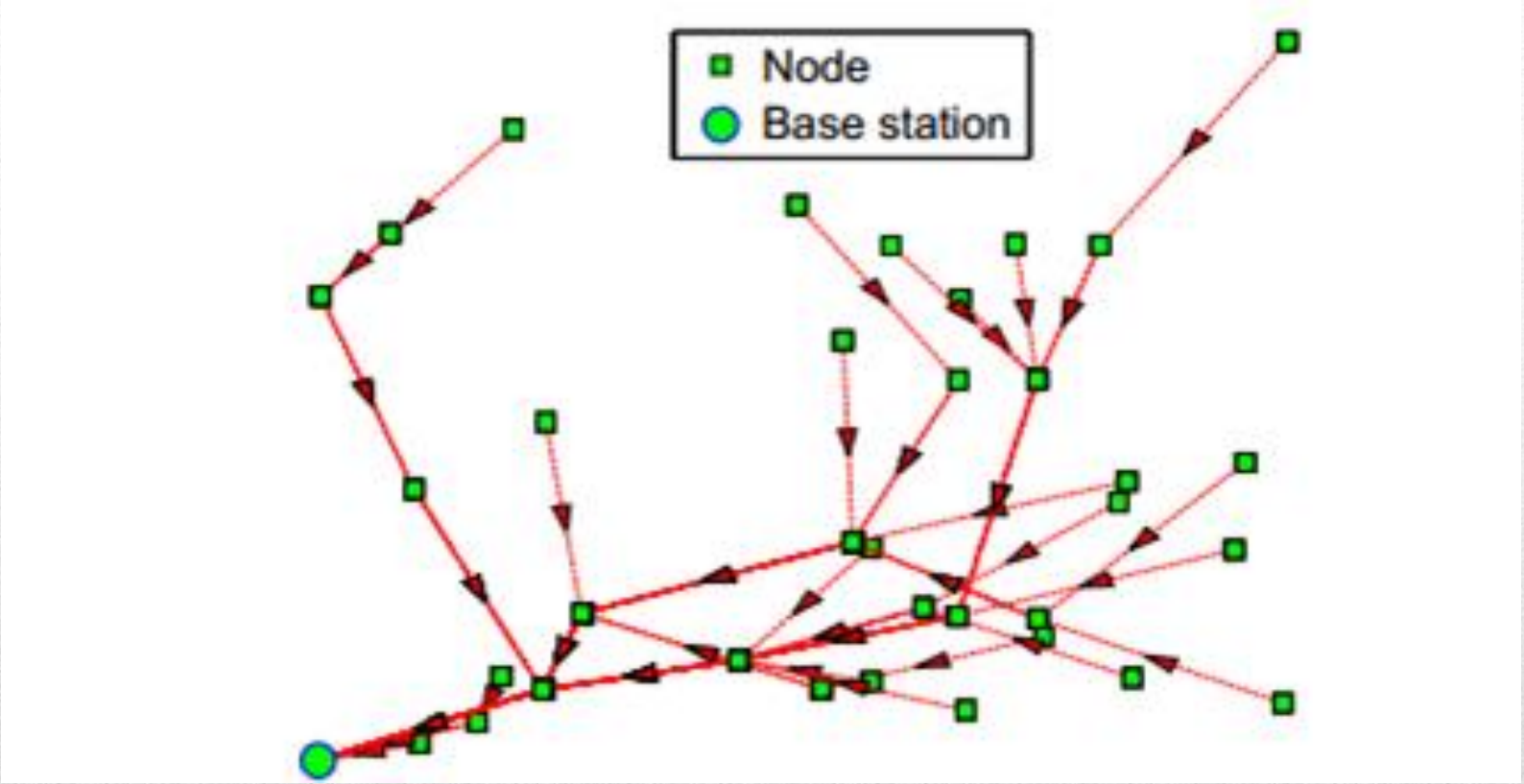
Concluding Remarks

Introduction

- A WSN consists of a large number of sensor nodes. These are generally densely (and randomly!) deployed within an area of interest.
- Hence, WSN protocols should support cooperative processing / self-organizing capabilities / low power requirements, etc.

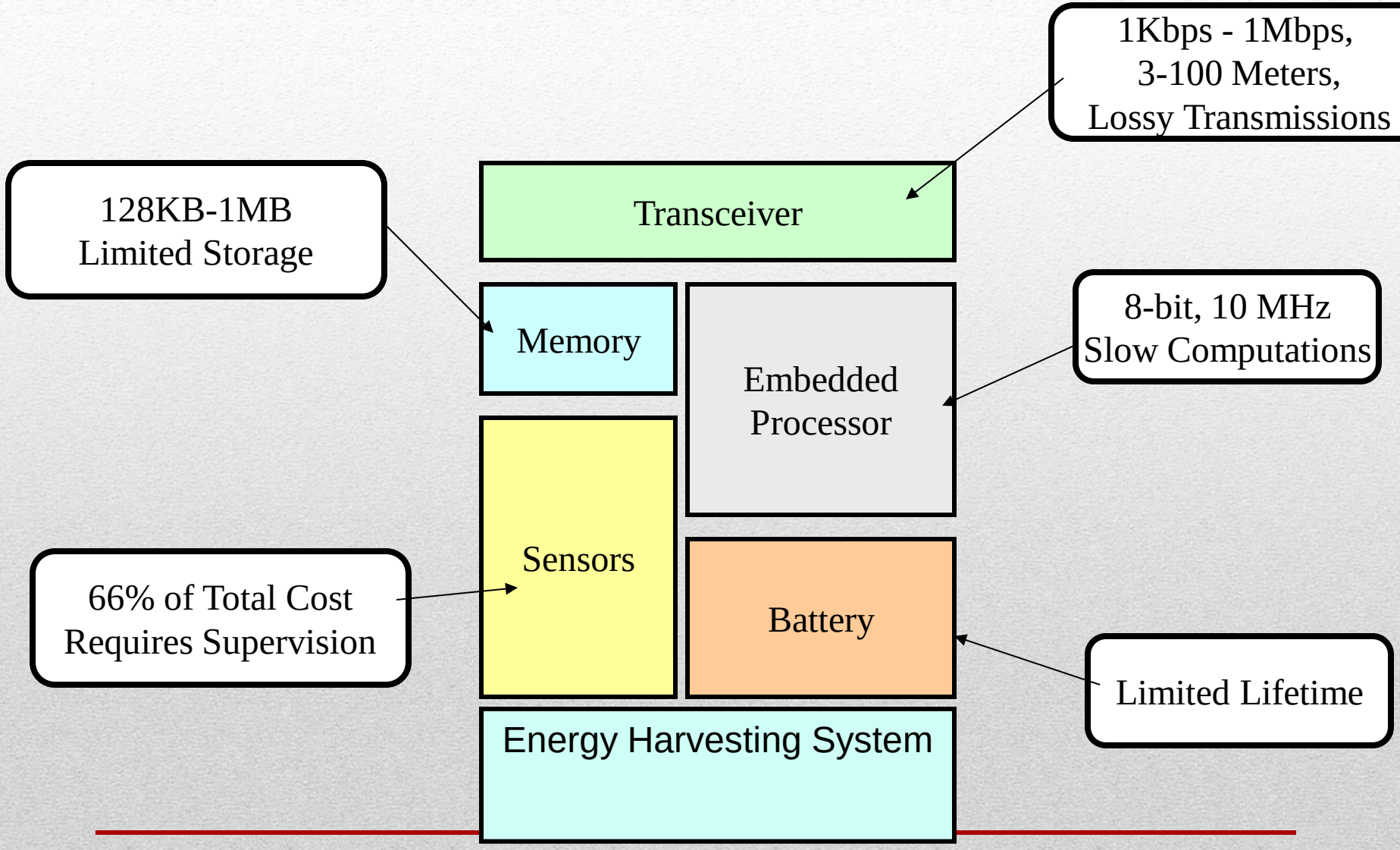


Types of WSNs (1)

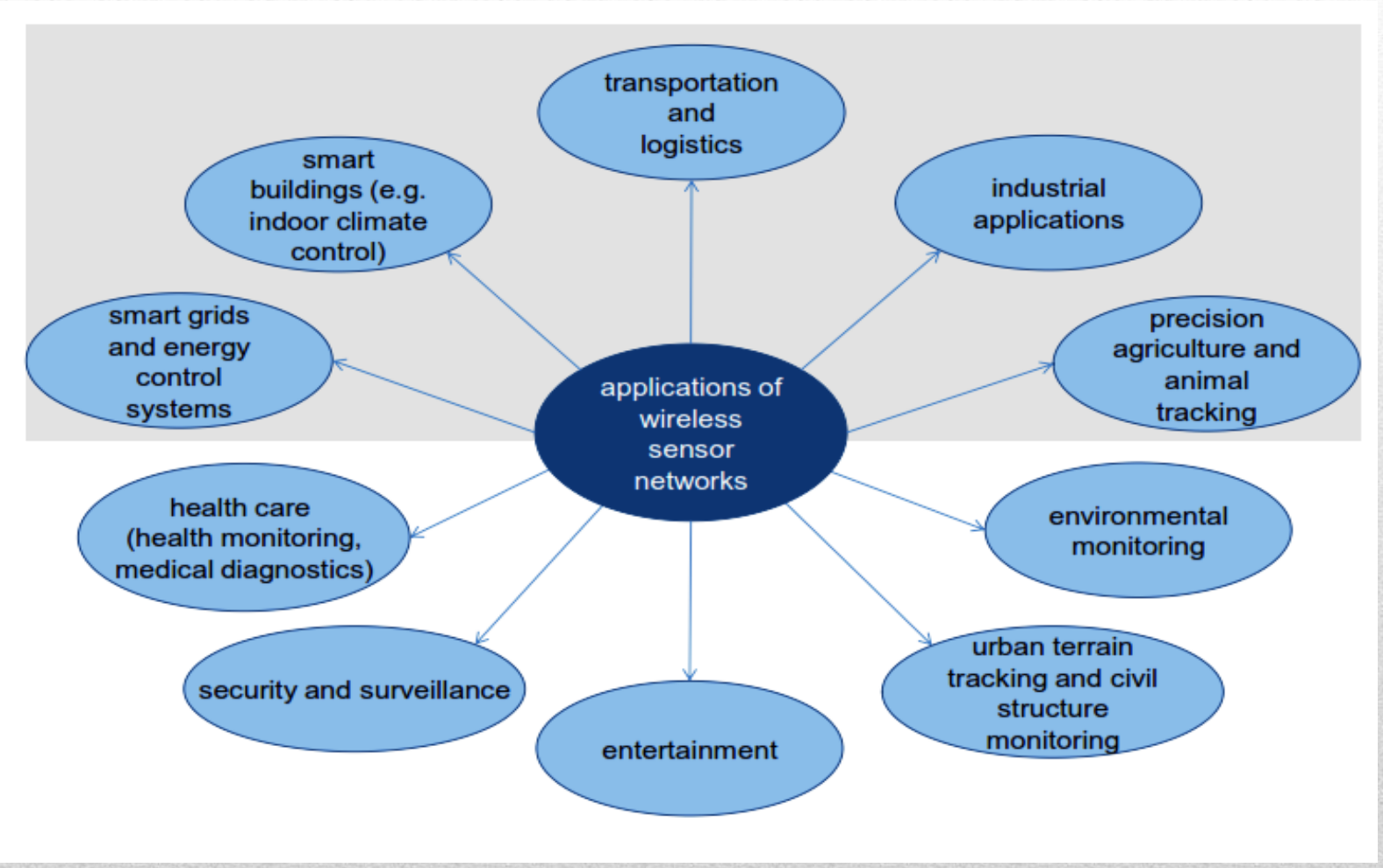


Types of WSNs (2)

Node Hardware

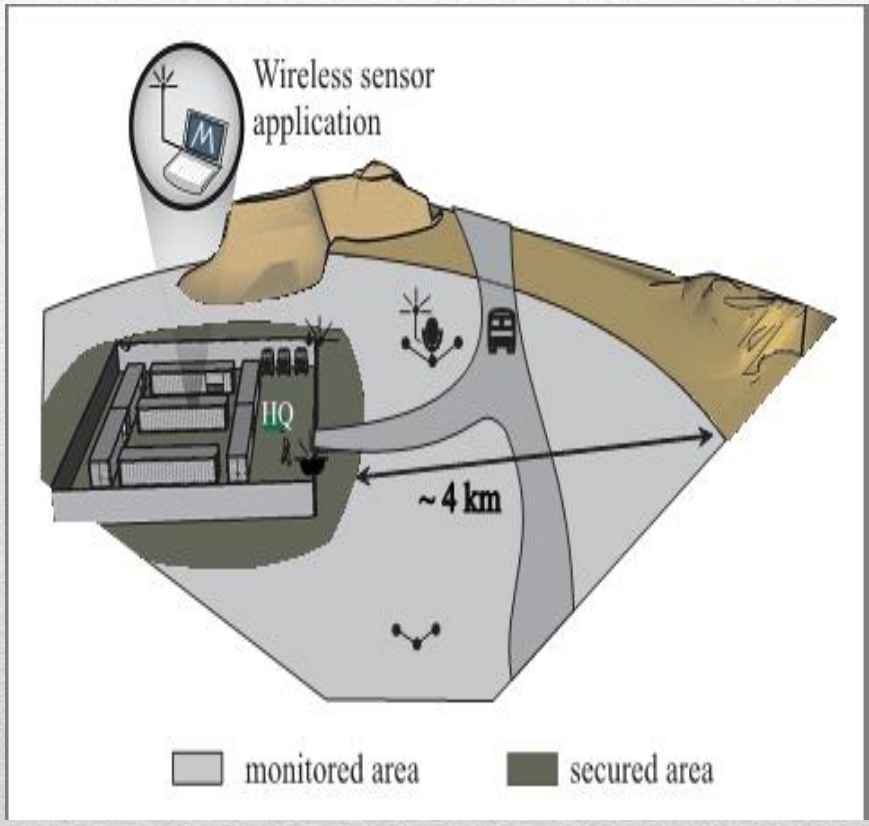


Application areas



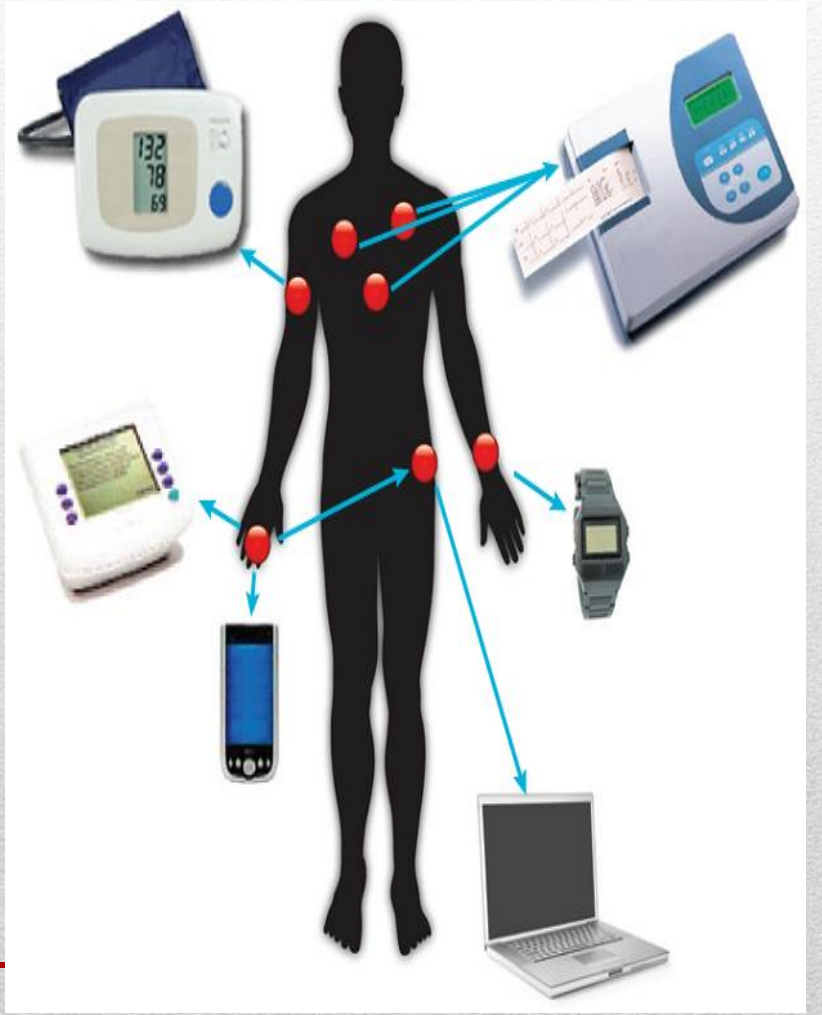
Military applications

- Monitoring forces, equipment, ammunition etc
- Exploring terrain
- Battlefield surveillance
- Battle damage assessment
- Nuclear, biological and chemical attack detection



Health applications

- Tele-monitoring of human physiological data
- Tracking and monitoring patients and doctors inside a hospital
- Drug administration in hospitals



Types of sensors

- Available sensors are generally:
  - generic (multi-purpose) nodes and
  - gateway (bridge) nodes
  - A generic sensor node takes measurements from the monitored environment. It may be equipped with a variety of devices which can measure physical attributes, viz. light, temperature, humidity, barometric pressure, velocity, acceleration, acoustics, magnetic field, etc.

Sensors…

- Gateway (bridge) nodes gather data from generic sensors and relay them to the base station. Gateway nodes have higher processing capability, battery power, and transmission (radio) range.
- Both these types are usually deployed to form WSN.

Challenges in WSN

- Services – developed to enhance the application and to improve system performance and network efficiency
- Self-organizing capacity – necessary in WSN
- Energy conservation – required in WSN
- Reliable communication – services such as congestion control, active buffer monitoring, acknowledgements, and packet-loss recovery are necessary
- Security – system is open, hence required
- Coverage – number of sensors and their placement determines coverage

Attacks in WSN

- Passive – attackers may observe from a distance
- Active - may lead to modification of existing data and so on..
- Physical layer - Jamming or radio interference
- Data link layer - collisions
- Network layer - sinkhole attack, blackhole attack, wormhole attack, Sybil attack
- Transport layer - flooding and desynchronization
- Application layer - application itself may generate large number of messages
- Denial of Service (DoS)

Managing security and integrity

- Public key cryptography – Mathematically related key pair (public key, private key)
  - Eg.: RSA, ElGamal, ECC
- Symmetric key cryptography – Same (symmetric) key for sender-receiver pair
  - Eg.: RC4, RC5, SHA-1
- Integrity – Origin integrity and Data integrity – by *signature*, by *message digest*
- Combining confidentiality and integrity

Key management

For flat topology WSN:

- Key pre-distribution schemes –
  - Pair-wise key pre-distribution, Master key based key pre-distribution, Random key-chain based key pre-distribution, Combinatorial design-based key pre-distribution

For hierarchical WSN:

- Pair-wise key distribution schemes
- Group-wise key distribution schemes
- Network-wise key distribution

Common attacks in Routing protocols

- In Directed Diffusion adversary may send strong reinforcements to the node to which interest is sent, so that data is diverted through itself.
- Hello flood attack is one of the attacks to LEACH routing protocol.
- A common attack in Rumour routing may be denying forwarding of information or performing selective forwarding.
- And others…

Secure Multipath Routing

- Multiversion Multipath (MVMP) protocol is effective against Eavesdropping and Modification attacks.
- INSENS address the DoS flooding attacks.
- SAODV-MAP, though originally proposed for mobile adhoc networks, can fight against Eavesdropping, Modification, Rushing, Sybil, Hello attacks

Energy-efficient secure routing

- It is obvious that security measures in routing protocols will drain the energy of nodes. Hence a number of energy-efficient and secure routing protocols find mention in the literature.
- Examples: SEER, energy-efficient single-path routing

Trust-based secure routing

- *TARF: A Trust-Aware Routing Framework for WSNs*, authors consider trustworthiness and energy efficiency of nodes
- Trust-based network management for hierarchical WSNs: two-level trust based on intimacy, honesty, energy and unselfishness

Location-based secure routing

- Secure Implicit Geographic Forwarding (SIGF)
- SIGF-0, a stateless and non-deterministic protocol,
- SIGF-1, remembers local state and
- SIGF-2, a stateful protocol.
- Together they provide resistance to Wormhole, Sybil, Replay DoS attacks, among others

Heterogeneous Networks: Security Issues

- Interoperability of devices - ability of systems (in general) to provide services to and accept services from other systems
- Interoperability addresses: *physical level*, *network level*, *application level* and *management level* aspects

Concluding remarks

- The work identifies the issues of security at various levels of a WSN and provides an overview to the different technical aspects regarding security schemes.
- Each WSN application has its own requirements, and hence one security solution that suits an application may not be suitable for another WSN application.

References:

- Akyldiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002). Wireless Sensor Networks: A Survey. Computer Networks 38 (pp. 393–422)
- Camtepe, S. & Yener, B. (2005). Key Distribution Mechanisms for Wire- less Sensor Networks: A Survey. Rensselaer Polytechnic Institute, Troy, New York, Technical Report: 05-07.
- Datema, S., (2005). Case study of wireless sensor network attacks. Masters thesis, Delft University of Technology.
- Dutta, S., Mukherjee, N., Neogy, S. & Roy, S. (2010). A Comparison of the Efficiencies of Different Wireless Sensor Network Algorithms with respect to Energy. In Proceedings of Fourth International Conference on Information Processing (pp. 271-280) , Bangalore, India.

References:

- Stallings, W. (2007). *Network Security Essentials:Applications and Standards*. Pearson press.
- Yick, J., Mukherjee, B., Ghosal, D. (2008). Wireless sensor network survey. Computer Networks 52 (pp. 2292–2330).
- Kundu, K., Chowdhury, C., Neogy, S. & Chattopadhyay, S. (2014). Trust Aware Directed Diffusion Scheme for Wireless Sensor Networks. In the Proceedings (IEEE) of Fourth International Conference on Emerging Applications of Information Technology, (pp. 385-391) India

Thank you