On the Security of Wireless Sensor Networks

Rodrigo Roman, Jianying Zhou, Javier Lopez

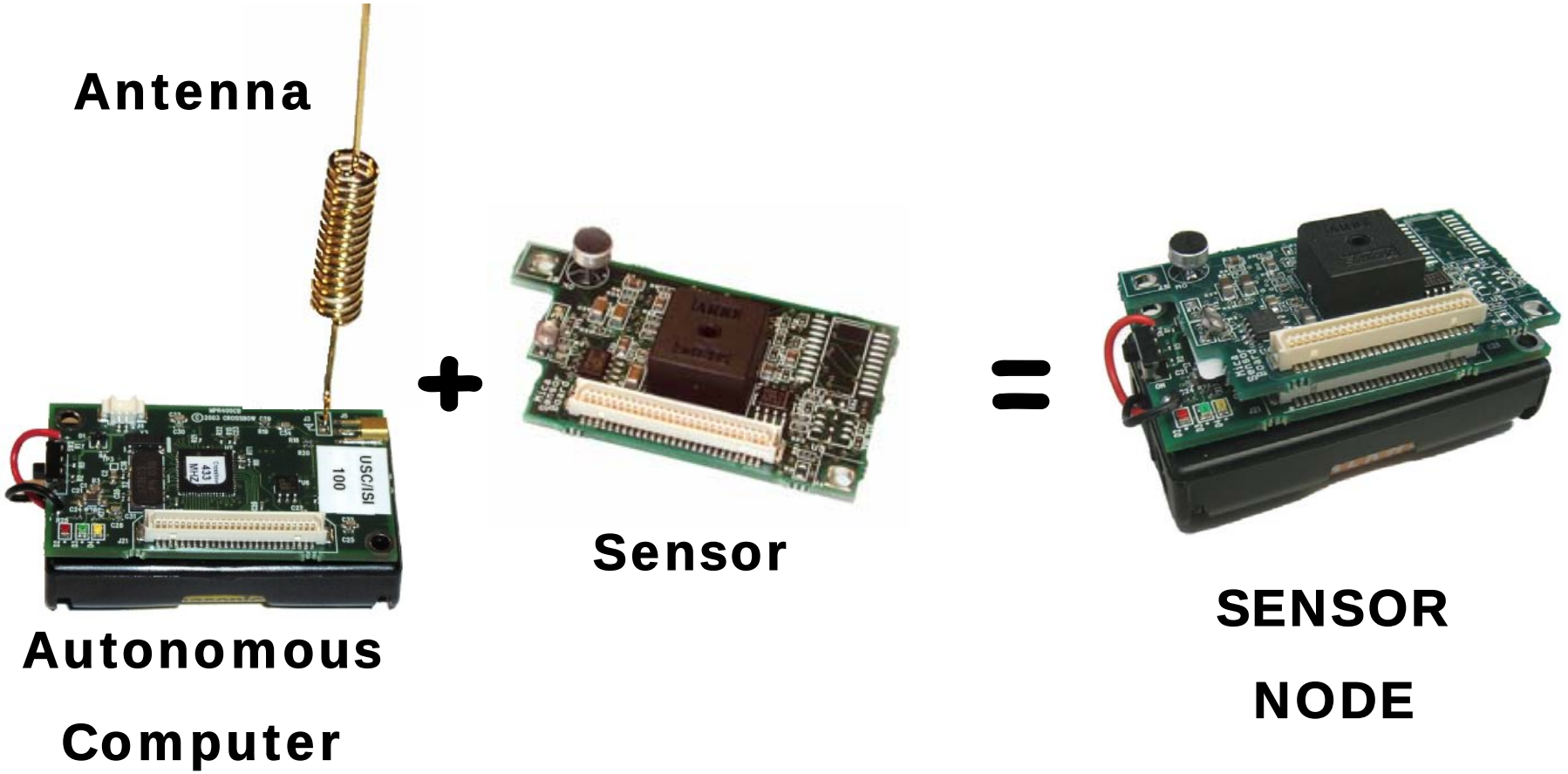
May 10, 2005

Outline

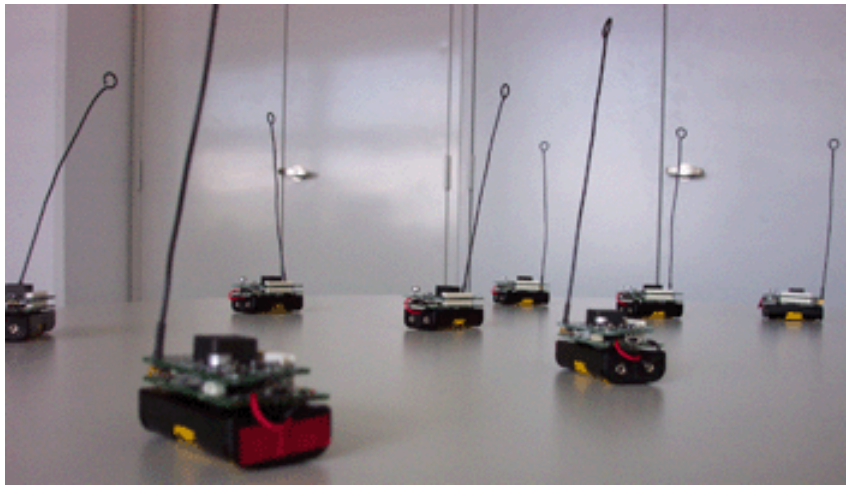
- An Introduction to Wireless Sensor Networks
- Sensor Network Architecture
- Security Issues
- State of the Art & Challenges
- Conclusions

An Introduction to Wireless Sensor Networks

From Sensors to Sensor Nodes



From Sensor Nodes to Sensor Networks



(Collaboration, Event-driven processing,...) =

Distributed Applications

WSN – Benefits & Applications

- Benefits
  - Low Cost
  - Easy to Deploy / Maintain
  - Access and Measure unreachable events
- Applications
  - Health applications
  - Environmental
  - Military
  - Home Applications, Smart environments, others…

Sensor Network Architecture

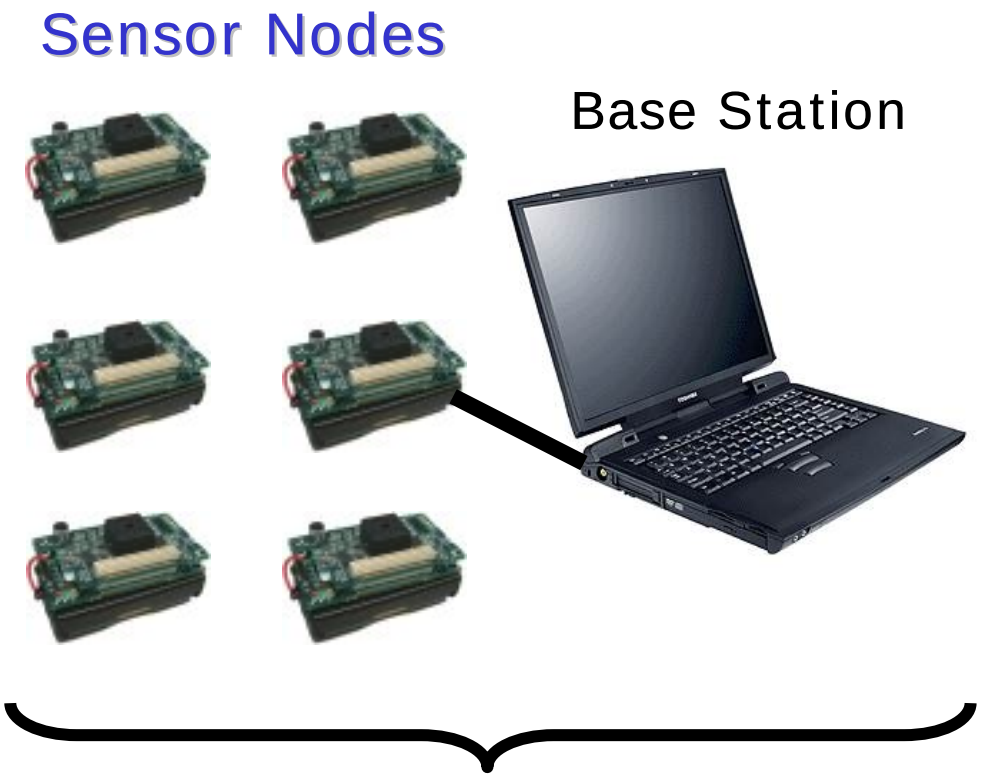
WSN – Main Infrastructure

Sensor Nodes Features:

- 8 Mhz, 128Kb I's Memory
- Batteries: 1 year (sleeping)
- Radio Links (19.2 Kbps)

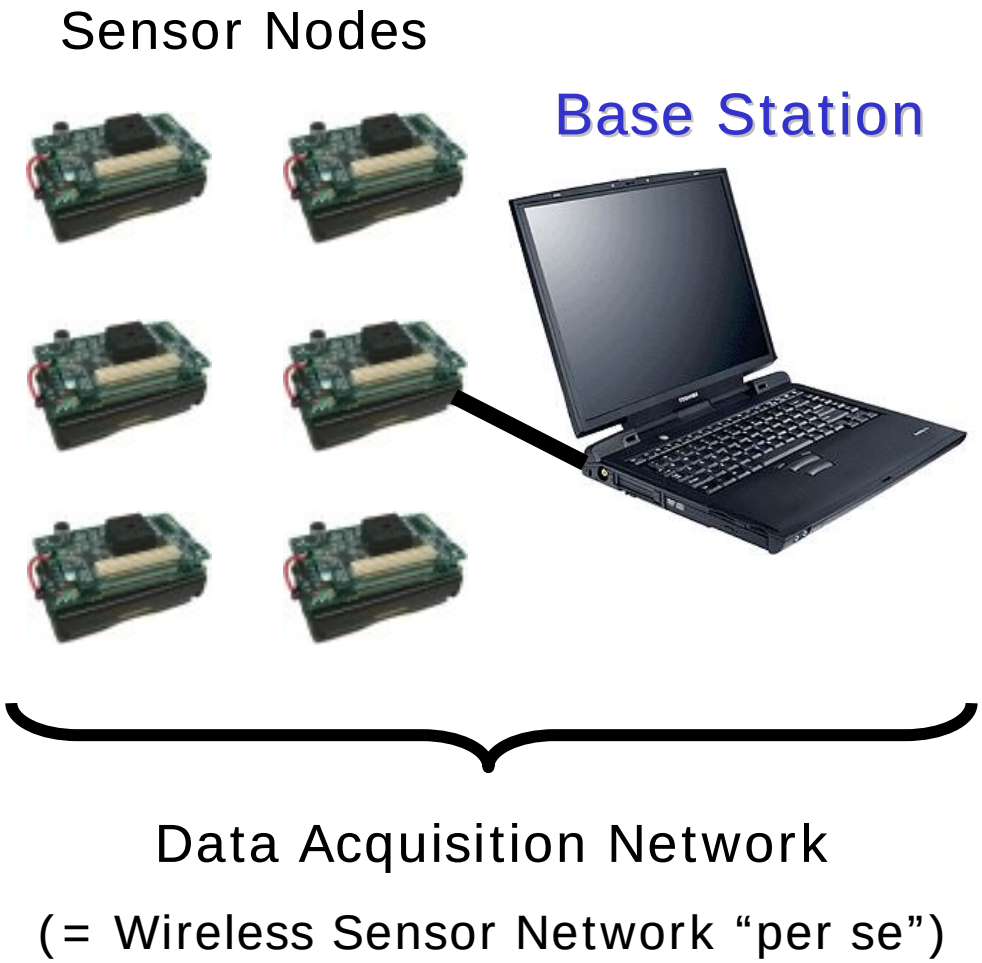
Sensor Nodes Roles:

- Harvesters
- Routers
- Distributed platform



WSN – Main Infrastructure

- Base Station: Less constrained
- Base Station Roles:
  - Manager
  - Interface



Security Issues

Security Context

Easy to attack…

Physical
- Node Integrity
- Channel Integrity
- Environment Integrity
- Energy Integrity

Logical
- Information Integrity
- Protocol Integrity
- Configuration Integrity

Security Context - Physical

- A sensor is physically vulnerable:
  - Destroyed, stolen nodes – no network/inaccessible!
  - Subverted nodes – disclose info, became malicious
  - Public wireless channel: jamming
  - Measurement vulnerabilities
  - Battery exhaustion attacks (sleep deprivation torture)

Security Context - Logical

- A sensor is logically vulnerable:
  - Public wireless channel: eavesdropping, injection
  - Attacks to protocols: external, internal nodes
    - Change network behaviour, unusable network
    - Even non-malicious nodes can harm!
  - Identity and Instruction Integrity – Easy to bypass

Security Issues

- Protect communication channels
  - Create security primitives and protocols
  - Distribute keys over the network
- “Bullet-proof” information management protocols
  - E.g. Routing, Data Aggregation
- Audit WSN events
- Privacy issues (Network privacy, Social privacy)
- Mobile systems, Delegation of privileges
- Others (HW Security, react against attacks)

State of the Art & Challenges

SotA – Security Primitives

- Sensor nodes are highly constrained. HW? SW?
  - Budget!
- SKE
  - Software (TinySEC, Block Ciphers [RC5, AES…], 10% overhead)
  - Hardware (IEEE 802.15.4, AES in CBC mode)
- MAC: Reuses algorithms used in SKE
- PKC
  - First rejected as “not possible”. Tests with ECC.
  - Usable Software PKC: EccM 2.0
    - 34 sec. Generation shared key, ±54.000 PKC operations.

SotA – Key Infrastructure

- Main Problem: Sensor Networks are huge!
  - Many nodes, few memory. Not all are reachable directly.
- Design of Key Infrastructure:
  - Key Distribution (issuing of keys)
  - Key Storage (n. of keys inside a node)
  - Key Maintenance (inclusion/exclusion of nodes, refresh)

SotA – Key Infrastructure

- Key Distribution
  - Before Deployment (preloaded), After Deployment (negotiation).
  - After Deployment: Apply PKC?
- Key Storage
  - Extreme Cases: Global Keying, Pairwise Keying
  - How to balance? (e.g. Key Pools)
- Key Maintenance
  - Almost no background. PKC?
- Local (Dynamic) Groups?
  - Few solutions, new properties (“Forward security”,“Secure tunnel”)

SotA – Routing

- Wide range of attacks against routing
  - Spoofed information, Selective forwarding, Wormholes, Sybil,…
  - Key Infrastructure not enough to protect routing!
- Secure Routing protocols?
  - (Almost) No protocols with security in mind from scratch!
    - µTESLA – Authenticated Broadcast
  - Enhanced protocols: LKHW – Directed Diffusion
  - New Techniques: Redundant routing, hole mapping
- Need to design secure routing protocols

SotA – Aggregation

- Aggregation? (Summarize) data
  - (Data, Data, … , Data) → Report
  - Who? Aggregators (Cluster heads, Special nodes,…)
  - Vulnerable! False Data, False Reports, Data on transit…
- Solutions:
  - Strong reports against false/wrong data (truncation, trimming,…)
  - Aggregator Tests:
    - Query the aggregator itself, Nodes as witnesses.
    - Based on proof creation using SKE, MACs, Bloom filters.
  - Transit Reports Tests
- Need new optimised solutions

SotA – Auditing and IDS

- Impossible to know state of the nodes (User in Base Station)
  - Solution: Auditing subsystem (simple, energy/space efficient)
- Intrusion Detection Systems – based on audit information
  - Multiple points of attack (decentralized)
  - Calculations should be done on Sensor Nodes – constraints!
  - User/Admin is far from the source of the problem
- Almost no research in this area!
  - Independent solutions: Health monitoring, HMM, code attestation

SotA – Privacy

- Two types of privacy
  - Network Privacy
    - Privacy of the network itself (nodes, information)
      - Content Privacy Threat (Meaning)
      - Identity Privacy Threat (Node Identities)
      - Location Privacy Threat (Node Locations)
  - Social Privacy
    - Privacy of the subjects under surveillance
    - Doubled-Edged sword!

SotA – Others

- Mobile Agents
  - Could be useful on a Sensor Network context
  - Constrained environment, no protection
- Mobile Sensor Nodes and Base Station (Delegation)
  - All previous cases: static environments
- Automatic reaction against external/internal problems
  - Denial of Services attacks

Conclusions

Open Areas

- Application of PKC over sensor networks
- More Routing Algorithms with secure foundations
- Optimize Secure Data Management Algorithms (Aggregation)
- Social and Network privacy – discuss
- Mobile nodes, Mobile Base Stations
- Delegation of privileges
- Tolerate the lack of physical security
- Intrusion Detection techniques, integrated IDS
- Optimize, Optimize, Optimize! (memory constraints, energy usage…)

Thanks for your Attention!