



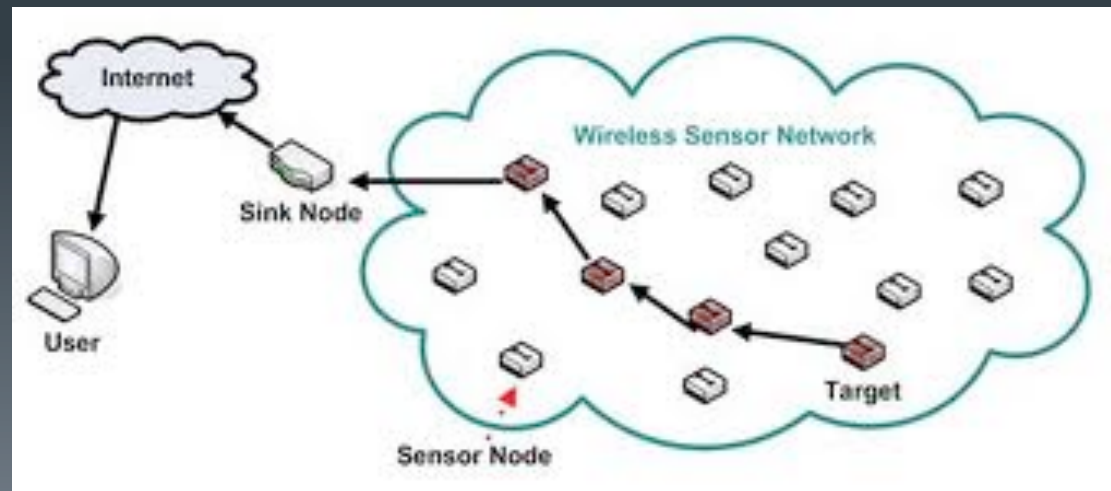
Wireless Sensor Network Security

Seth A. Hellbusch
CMPE 257

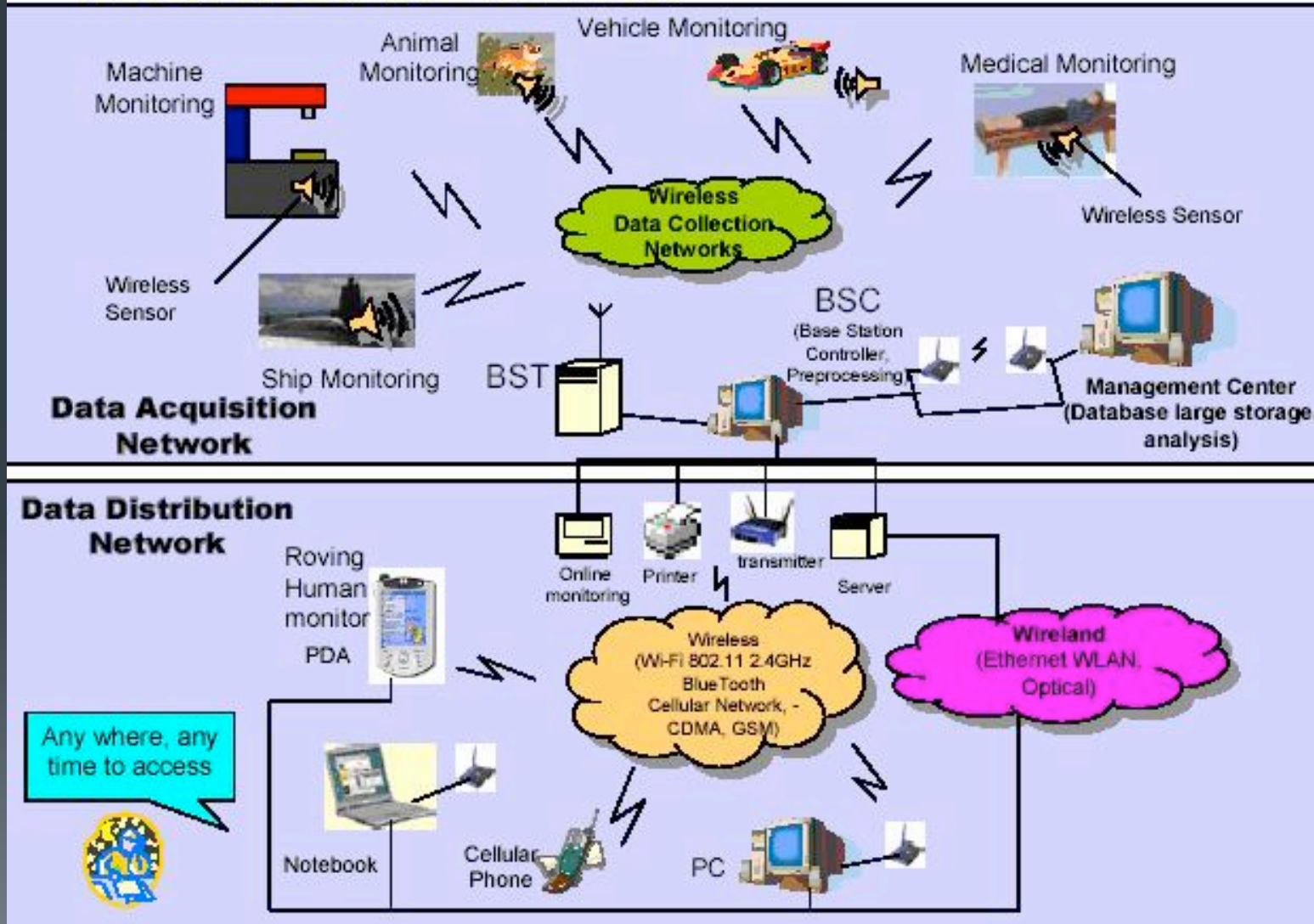
Wireless Sensor Networks (WSN) ²

The main characteristics of a WSN include:

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Easy of use
- Unattended operation.



Wireless Sensor Networks



WSN Security Papers

- Security in Wireless Sensor Networks
 - Adrian Perring, John Stankovic, & David Wagner – 06/2004
- Wireless Sensor Network Security Analysis
 - Hemanta Kumar Kalita & Avijit Kar – 12/2009
- Security in Distributed, Grid, Mobile, and Pervasive Computing, Chapter 16: Wireless Sensor Network Security: A Survey".
 - Yang Xiao – 04/2007

Paper 1 - Security in WSNs

5

- Sensor networks pose unique security challenges
 - Limited energy, computation, and communication capabilities
 - Deployed in accessible areas adding to physical attack risk
 - Interact closely with physical environment
- Existing network security techniques are inadequate
 - Traditional network security cannot be directly applied
 - Extensive new research is required

Paper Topics

- Secure Systems and Challenges
- Network Security Services
- Future Research Challenges

A Secure System

Security Challenges for a secure WSN system include:

- Key Establishment and Trust Setup
- Secrecy and Authentication
- Privacy
- Robustness to Communication Denial of Service
- Secure Routing
- Resilience to Node Capture



Key Establishment and Trust Setup⁷

Establishment of Cryptographic Keys

- Public-key primitives overhead, limited computation
- Need to be able to scale for thousands of nodes
- Key setup between individual nodes

Potential Solutions

- Network-wide shared key
- Establish link keys through initial shared key
- Preconfigured symmetric link keys
- Bootstrapping keys
- Random key predistribution pools
- Hardware support for public-key crypto



Secrecy and Authentication

WSNs must provide protection against eavesdropping, injection, and modification

- Cryptography is standard defense
 - End-to-end
 - High level of security
 - Requires key management
 - Link-layer *
 - Easier and more common to deploy
 - Still allows intermediate node threat
 - Hardware and Software based
 - HW cost vs. SW computation
- Performance and packet size challenges
 - Cryptography increases packet sizes

Privacy

- Sensor networks pose potential privacy concerns
 - Secret surveillance
 - Spying
- Smaller devices are easier to conceal
- Surveillance deployments increase as cost goes down
- Many potential (il)legitimate uses cases
 - Tracking of people and vehicles
 - Data collection, analysis, distribution
- May need new laws to address potential issues

Robustness to Com DoS

DoS can severely limit value of WSNs

- Potential Attacks
 - High energy broadcasts
 - Link layer violation (RTS/CTS)
- Counter measures
 - Spread-spectrum radios
 - Routing around

Secure Routing

- Data forwarding key service in WSNs
 - Malicious routing information can be injected
- Simple routing authentication
- Secure routing challenges
 - Replay attacks
 - Node capture
- Need more research in this area

Resilience to Node Capture

- One of the most challenging security aspects of WSNs
 - Physical security often neglected
 - Accessible deployments
- Adversaries may capture nodes
 - Extract crypto keys
 - Reprogram
 - Replace
- Counter Measures
 - Tamper resistance (*!*)
 - Replicated network state, voting, & cross checking
 - Redundancy *

Network Security Services

13

High-level Security Mechanism for WSNs

- Secure Group Management
 - Data analysis and aggregation by groups
- Intrusion Detection
 - Fully distributed & decentralized IDS
- Secure Data Aggregation
 - Common in WSNs
 - Random node sampling for threats

Research Challenges

WSN system research generally more challenging than traditionally wireless networks

What could help?

- Architect security solutions in new research
- Single administration domains to simplify threat model
- Utilize characteristics of WSNs
 - Redundancy
 - Scale
 - Collective computation

Needed solutions

- Toleration of the lack of physical security
- Individual node computation restrictions

Paper 2 – WSN Security Analysis

15

Wireless Sensor Networks & Motivations

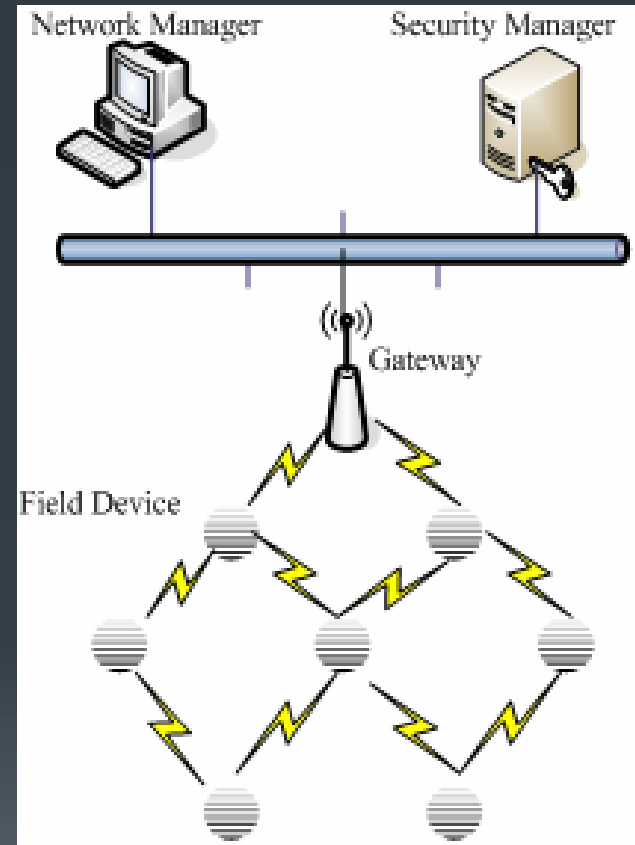
- Diverse application domains
- Dense deployments
- Perform many applications
 - Signal processing
 - Computation
 - Self configuration
- Scalable, robust, & long-living

Paper Topics

- WSN Architecture
- WSN Security Threat Analysis
- Counter Measures

WSN Architecture

- Sensor Nodes (Field Devices)
 - Sensor / Processing
 - Routing
- Gateway / Access Point
 - Access to host application
- Network Manager
 - Configuration
 - Scheduling
 - Monitoring
- Security Manager
 - Key management



WSN Security Threat Analysis

17

- Simplicity can potentially increase vulnerability
- Many potential attacks
 - Will cover the classifications next...
- Must provide various security properties:
 - Confidentiality
 - Integrity
 - Authenticity
 - Availability

This paper covers a very comprehensive potential threat matrix. Even though this paper focuses on WSNs, many of these attacks apply to other wireless networks and security.

WSN Security Threats

- 1) Denial of Service (1,2,3,4)
 - ① Jamming, Tampering
 - ② Collision, Exhaustion, Unfairness
 - ③ Neglect/Greed, Homing, Spoofing, Black Holes, Flooding
 - ④ Flooding, De-synchronization
- 2) Interrogation (2)
- 3) Sybil (1,2,3)
 - ① Multiple Identities or places at once
 - ② Data Aggregation, Voting
 - ③ Multiple Identities
- 4) Wormholes (3)
- 5) Sinkholes (3)
- 6) Manipulating Routing Info (3)
- 7) Selective Forwarding (3)
- 8) HELLO Flood (3)
- 9) Acknowledgement Spoofing
- 10) Cloning (5)
- 11) Impersonation / Replication
- 12) Eavesdropping
- 13) Traffic Analysis
- 14) Mote Class / Insider Threat
- 15) Invasive / Probing / Reversing
- 16) Non-Invasive / Side-Channel
- 17) Laptop Class
 - ① Passive Eavesdropping
 - ② Traffic Injection
- 18) Attack on Protocol
 - ① Key Management
 - ② Reputation Assignment Scheme
 - ③ Data Aggregation
 - ④ Time Synchronization
 - ⑤ Intrusion Detection Systems

WSN Counter Measures

19

Threat Counters & Methodologies

- Outsider Attacks and Link Layer Security
- Sybil
- HELLO Flood
- Wormholes & Sinkholes
- Leveraging Global Knowledge
- Selective Forwarding
- Authenticated Broadcast & Flooding
- OSI Layer Wise Threats

WSN Counter Measures - 2

20

- Outsider Attacks and Link Layer Security
 - Majority prevented by link layer encryption / shared keys
 - Still susceptible to wormholes and flood attacks
 - More sophisticated mechanisms are needed
- Sybil
 - Traditionally deterred by public-key crypto (WSNs limitations)
 - Trusted base station and unique symmetric key
 - Establish keys through base station
 - Limit key sets
- HELLO Flood
 - Verify bi directionality of link
 - Identity verification
- Wormholes & Sinkholes
 - Very difficult to verify info (hop count, topology, energy, reliability, etc.)
 - Need to design routing protocols to reduce effects

WSN Counter Measures - 3

21

- Leveraging Global Knowledge
 - Map network topology
 - Geographic location
 - Periodic updates
 - Drastic changes may indicate malicious activity
 - Probabilistic next-hop
- Selective Forwarding
 - Multipath routing
 - Braided & multiple braided paths
- Authenticated Broadcast & Flooding
 - Must not be able to spoof messages from a base station
 - Limit packet overhead
- OSI Layer Wise Threats

WSN Counter Measures - 4

- OSI Layer Wise Threats – Physical Layer

Threat	Countermeasure
Interference	Channel hopping and Blacklisting
Jamming	Channel hopping and Blacklisting
Sybil	Physical Protection of devices
Tampering	Protection and Changing of key

WSN Counter Measures - 5

- OSI Layer Wise Threats – Data Link Layer

Threat	Countermeasure
Collision	CRC and Time diversity
Exhaustion	Protection of Network ID and other information that is required to joining device
Spoofing	Use different path for re-sending the message
Sybil	Regularly changing of key
De-synchronization	Using different neighbors for time synchronization
Traffic analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network
Eavesdropping	Key protects DLPDU from Eavesdropper

WSN Counter Measures - 6

- OSI Layer Wise Threats – Network Layer

Threat	Countermeasure
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use Packet Leach techniques.
Selective forwarding	Regular network monitoring using Source Routing
DoS	Protection of network specific data like Network ID etc. Physical protection and inspection of network.
Sybil	Resetting of devices and changing of session keys.
Traffic Analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network.
Eavesdropping	Session keys protect NPDU from Eavesdroppers.

Paper 3 – WSN Security: A Survey²⁵

Paper Topics

- Obstacles to WSN Security
- Requirements of a Secure WSN
- Attacks*
- Defensive Measures*

WSN Security Obstacles

- Very Limited Resources
 - Memory & storage
 - Power
- Unreliable Communication
 - Unreliable Transfer
 - Conflicts
 - Latency
- Unattended Operation
 - Exposure to physical attack
 - Managed remotely
 - No central management point

WSN Security Requirements

27

A secure WSN will consider these concepts:

- Data Confidentiality
- Data Integrity
- Data Freshness
- Availability
- Self-Organization
- Time Synchronization
- Secure Localization
- Authentication

WSN Attacks & Defenses

- Much of this was similar to the last paper
- Went into greater detail with example research

Additional items worth mentioning:

- Disabling base stations can potentially cripple entire network
 - Traffic analysis – find which nodes send the most data
 - Skipjack was winning cipher in every category measured
 - Successful implementation of public-key crypto in WSNs
 - Tamper proof by reducing the deterministically of sensor nodes – “random randomness”
-
- Whole paper had a very “military” feel