Power Consumption Attacks in Wireless Sensor Networks

Micah Thornton Ryan Sligh Bobby Santoski

Computer Science & Engineering, Southern Methodist University, USA,
mathornton@smu.edu
rsligh@smu.edu
rsantoski@smu.edu

CSE 4344: Networks and Distributed Systems
Dallas, Texas
April 29, 2014

Outline of today's talk

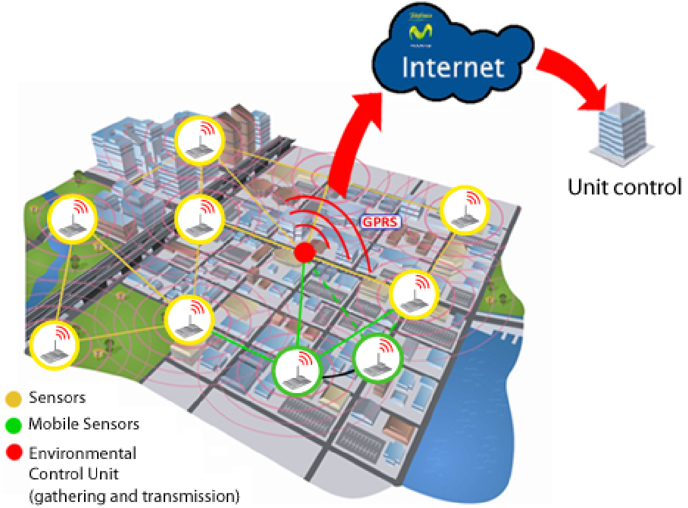
Outline

1. Introduction
   - Topics
   - Motivation
2. Methodology
   - Overview
   - Battery Behavior
   - Attack Simulations
3. Results and Analysis
   - Simulation Results
   - Mitigation Strategies
4. Conclusion
   - Future Work

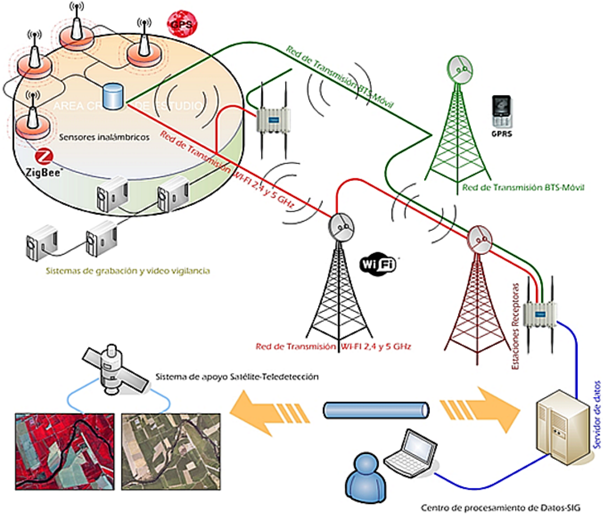
Wireless Sensor Networks(WSNs)

- A **Wireless Sensor Network(WSN)** is a network of **Sensor Nodes**
- **Sensor Nodes** monitor certain environmental variables
- **Sensor Nodes** generally operate in one of two states:
  - **Sleep Mode** - less power draw, but can't receive and transmit
  - **Active Mode** - more power draw, and can receive and transmit

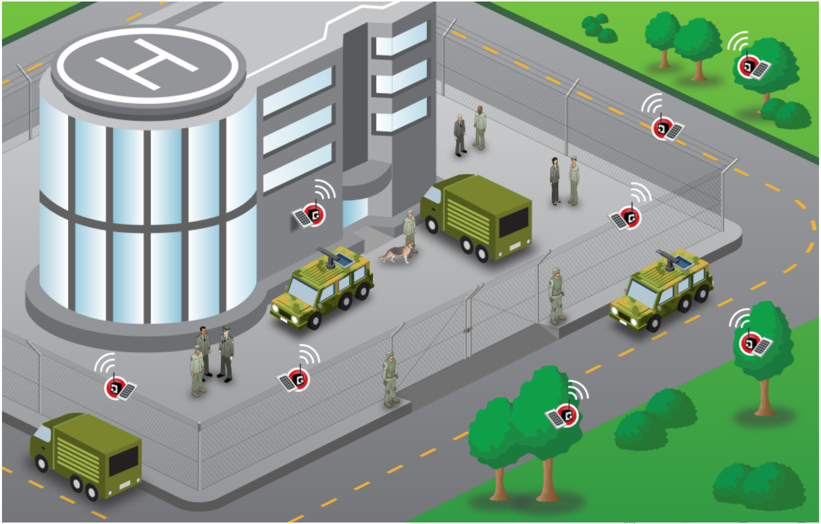
WSN examples (1) - p.H. and flow



WSN examples (2) - Fire detection and prevention



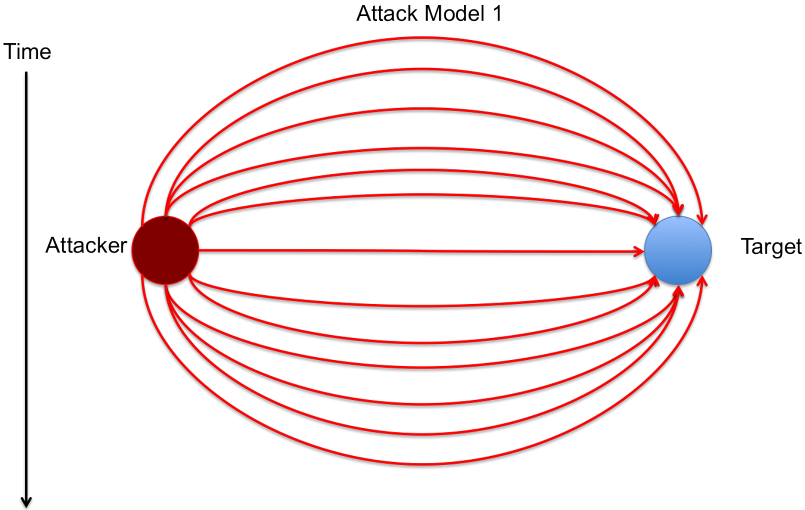
WSN examples (3) - Security systems



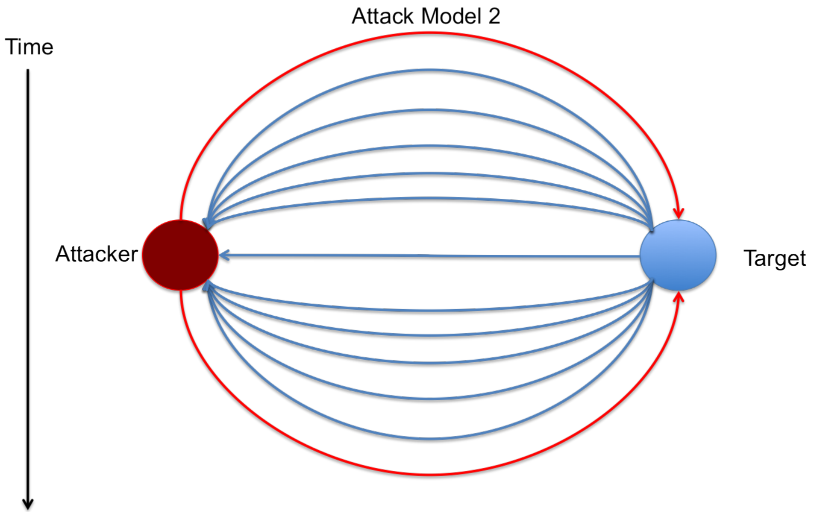
Attacks on WSN power supplies

- **Sensor Nodes** are developed in bulk for mass deployment
- Bulk production has robbed WSNs of more robust **battery lives**
- Limited battery lives make sensor nodes easy targets for **Power Consumption Attacks**
- A **Power Consumption Attack** drains the battery power of sensor nodes by forcing **meaningless active mode time**
- Attackers hope to gain something by compromising nodes:
  - Protocol information for other attacks
  - Temporary system downing
  - Permanent system downing
  - Competitive advantage

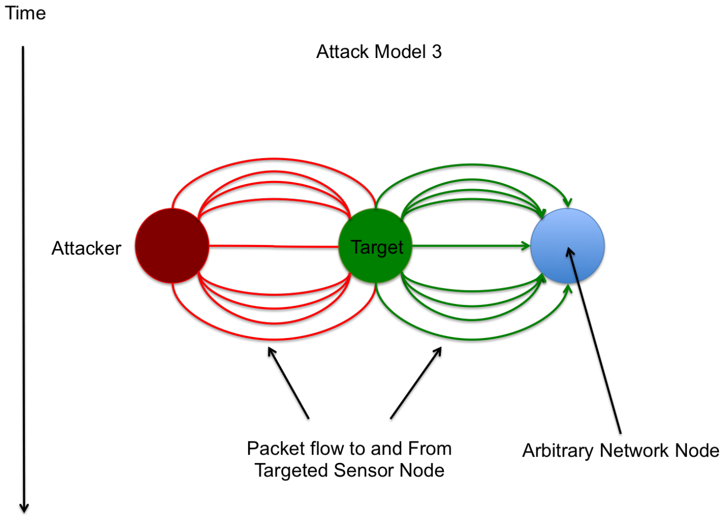
Attack Models (1) - Standard denial of sleep



Attack Models (2) - Inverse denial of sleep



Attack Models (3) - Routing power draw



Problem

How do we defend against Power Consumption Attacks?

Outline

Overview

- Simulated **standard denial of sleep attacks** and **routing power draw attacks** on WSNs
- First examined different **batteries**
- Next the **time to compromise** a node under various assumptions

Battery Tests

- The batteries tested were:
  - Lead-Acid Batteries
  - Alkaline Long-Life Batteries
  - Carbon-Zinc Batteries
  - NiMH Batteries
  - NiCad Batteries
  - Lithium Ion Batteries
- With weights varying from **0.1 mg** to **1 mg**
- And Packet sizes varying from **2 bits** to **1 kb**
- We got approximately **700** simulation results from NS3
- Packets were sent every **10 ms** in this simulation

Attack Simulation

- The attacks were simulated in an environment that allowed user defined:
  - Packet Size (bits)
  - Initial Node Energy (joules)
  - Power To Transmit Messages (Watts)
  - Power To Receive Messages (Watts)
  - Speed of Transmission radios (bps)
- Each of these were variate for **55,000** simulations

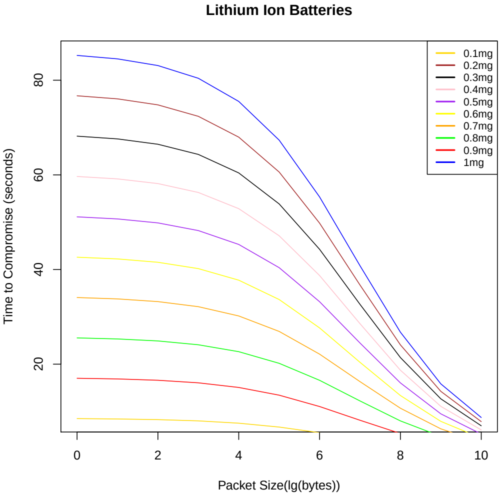
Outline

Battery Analysis(1) - Compromise Statistics

B-Type	TTC(Min)	MTTC	TTC(Max)
Lead Acid	0.2789 s	9.8798 s	27.0307 s
Alkaline Long Life	0.7589 s	27.1017 s	74.1107 s
Carbon-Zinc	0.2489 s	8.7950 s	24.0700 s
NiMH	0.6489 s	23.0336 s	62.9907 s
Nickle-Cadmium	0.2689 s	9.4734 s	25.9207 s
Lithium-Ion	0.8689 s	31.1701 s	85.2400 s

- **B-Type** = Battery Acid Type
- **TTC(Min)** = Minimum Time to Compromise w/ std attack
- **MTTC** = Mean Time to Compromise w/ std attack
- **TTC(Max)** = Maximum Time to Compromise w/ std attack
- As expected the Lithium Ion Battery is most effective

Battery Analysis(2) - Varied Weights

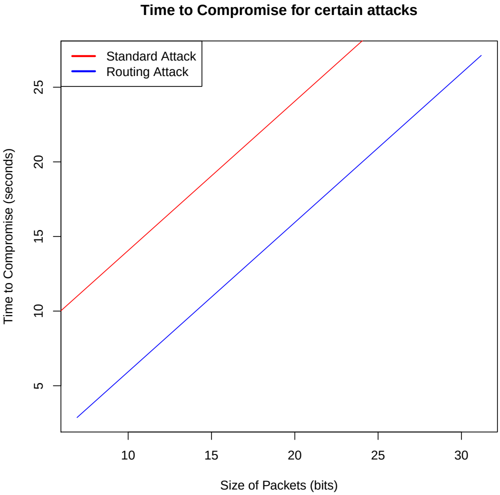


Comparing Attacks(1) - Compromise Statistics

A-Type	TTC(Min)	MTTC	TTC(Max)
Denial of Sleep	0.02558 s	14.49850 s	208.50587 s
Routing Power Draw	0.02558 s	3.16868 s	104.55439 s

- So a WSN distributor would be wise to fear the routing attack more so than a standard denial of sleep

Comparing Attacks(2) - Linear Regressions



Previous Strategies

- Some **risk mitigation strategies** have already been adopted for use in WSNs:
  - **Predefined Transfer Windows**
  - **Node Reception Memory**
  - **Jamming Detection Protocols**
  - **Low Power Wake-up Radio**
  - **Defined Maximum Path Length**
- Many strategies are developed with specific attacks in mind
- Even our proposed strategies have already been deployed

Proposed Strategies

- One logical way to mitigate the risks of **Power Consumption Attacks** is to use more powerful **batteries**
- Because the Routing attack we examined is much more potent examination of routing procedures should be carfully examined
- the possibility of placing nodes so they do not have to route should be considered for small crucial WSNs
- Targeted the root problem of all Power Consumption attacks: **pre-defined battery life**
- Installation of solar panels and other similar power regeneration devices.
- Attacks can still be mounted on the network, but would have to fight a endlessly renewing power source
- This addition could be costly, and distributors would need to shrink the size of their network
- But it is up to the distributor to examine there expected net

Outline

Future Work

- Model and test additional attack types
- Do a cost benefit analysis of different types of **batteries** and **alternative power sources**
- compare cost benefits of other mitigation strategies

Thanks

Thanks for Listening! Questions?