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 26, 2014

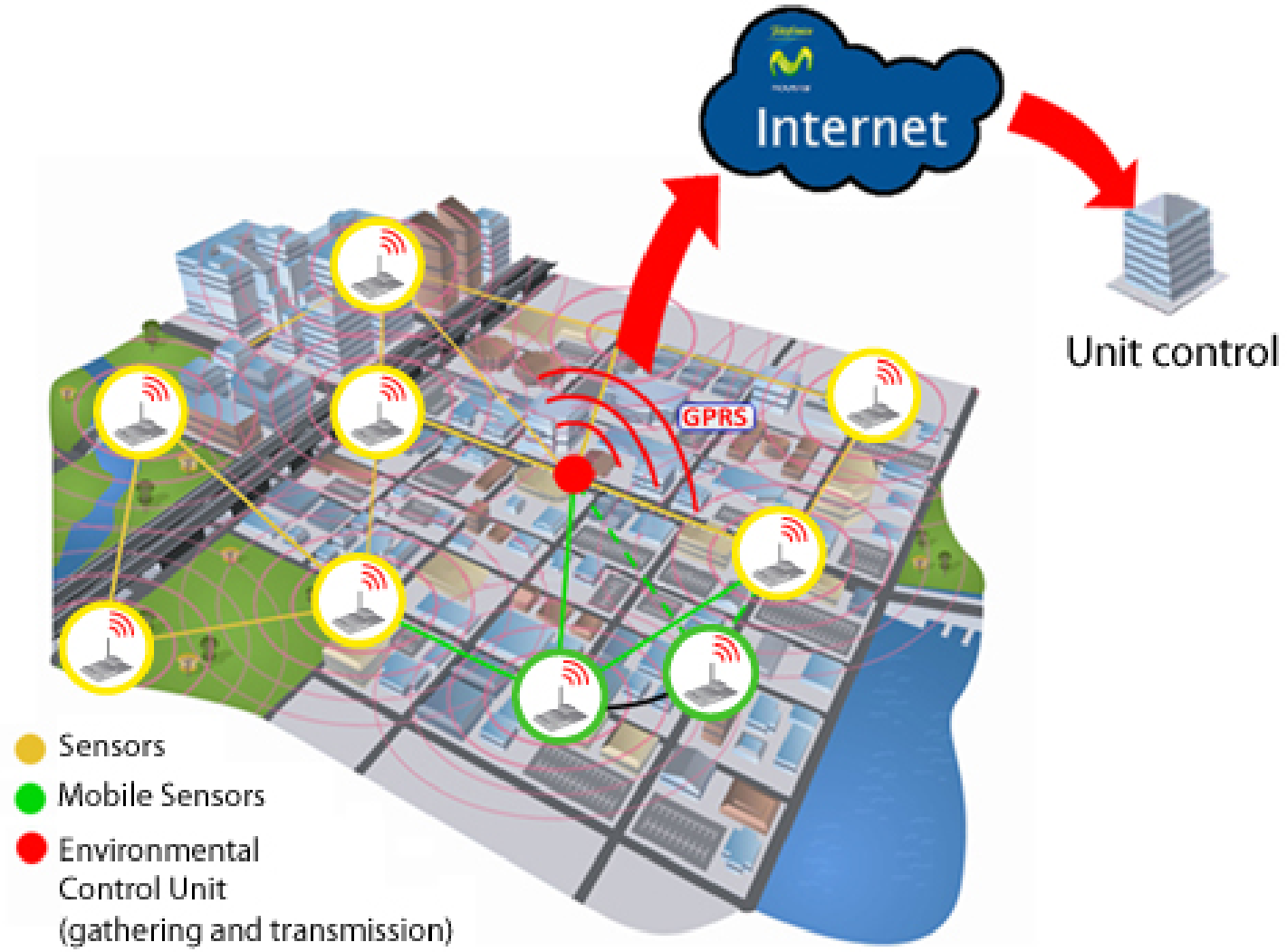
Outline of today's talk

Outline

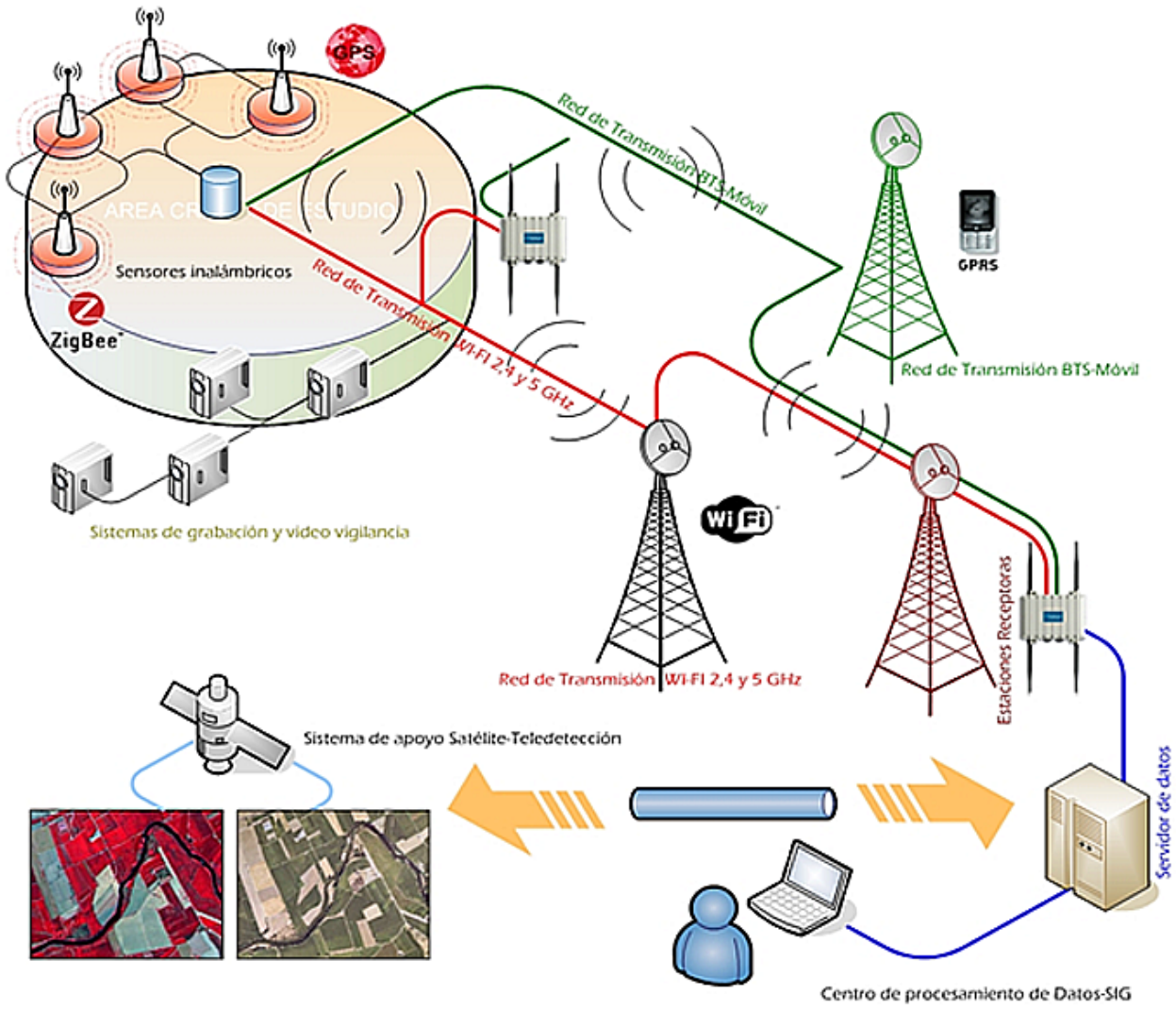
Wireless Sensor Networks(WSNs)

- A **wireless sensor network(WSN)** is a network of **Sensor Nodes**
- **Sensor Nodes** send and receive wide varieties of data.
- **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

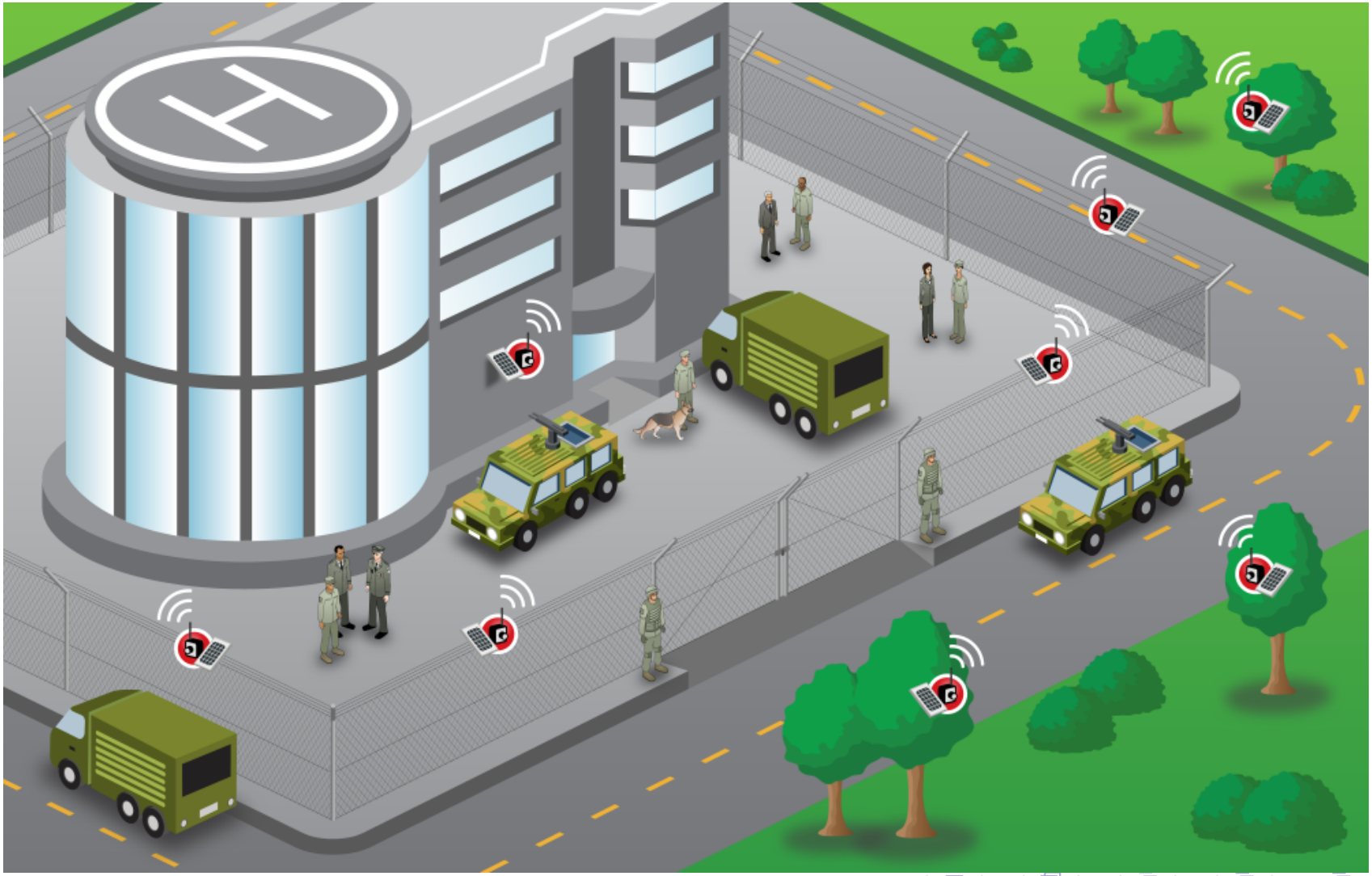
WSN examples (1) - p.H. and flow



WSN examples (2) - fire detection and prevention



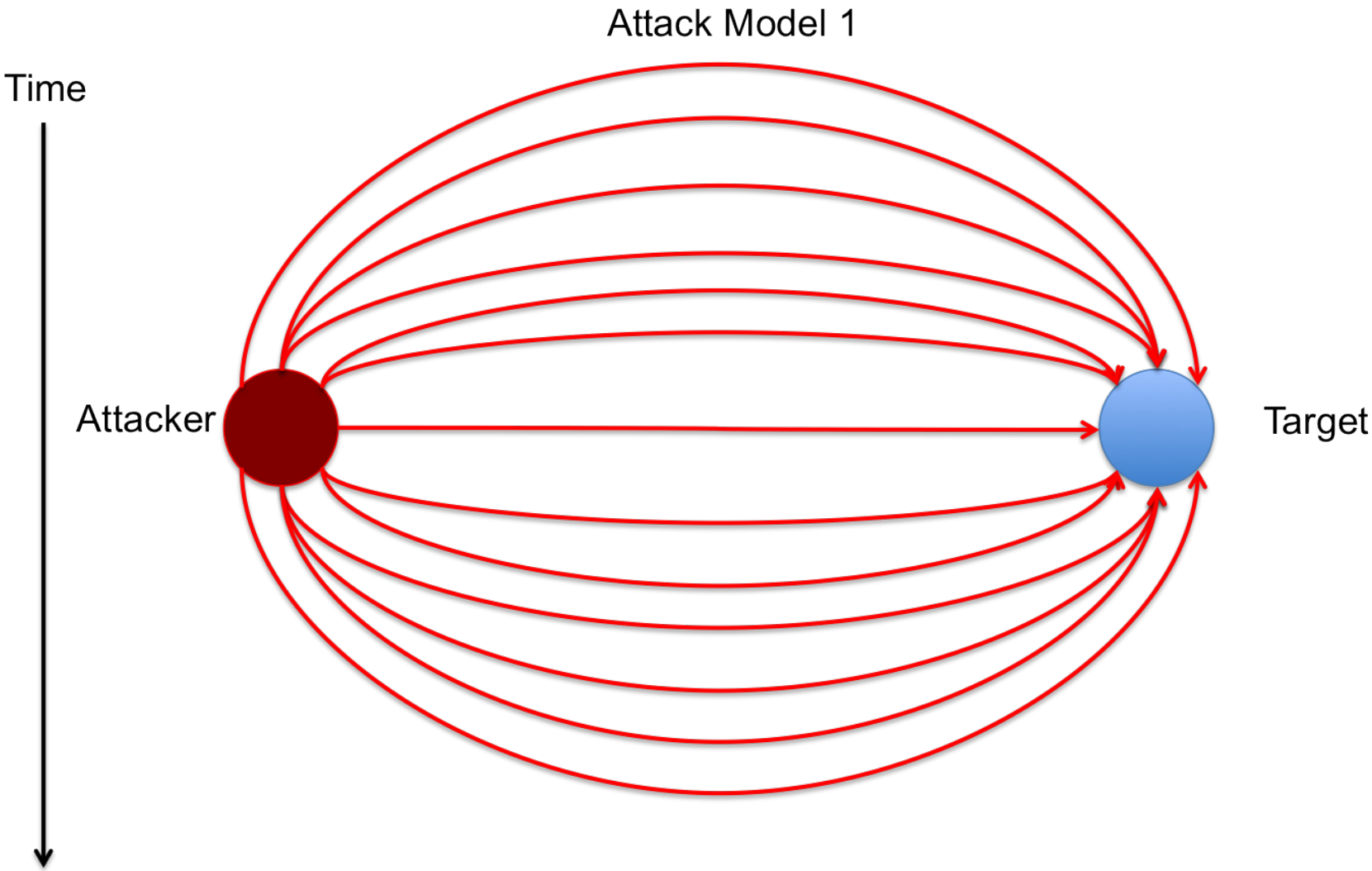
WSN examples (3) - security systems



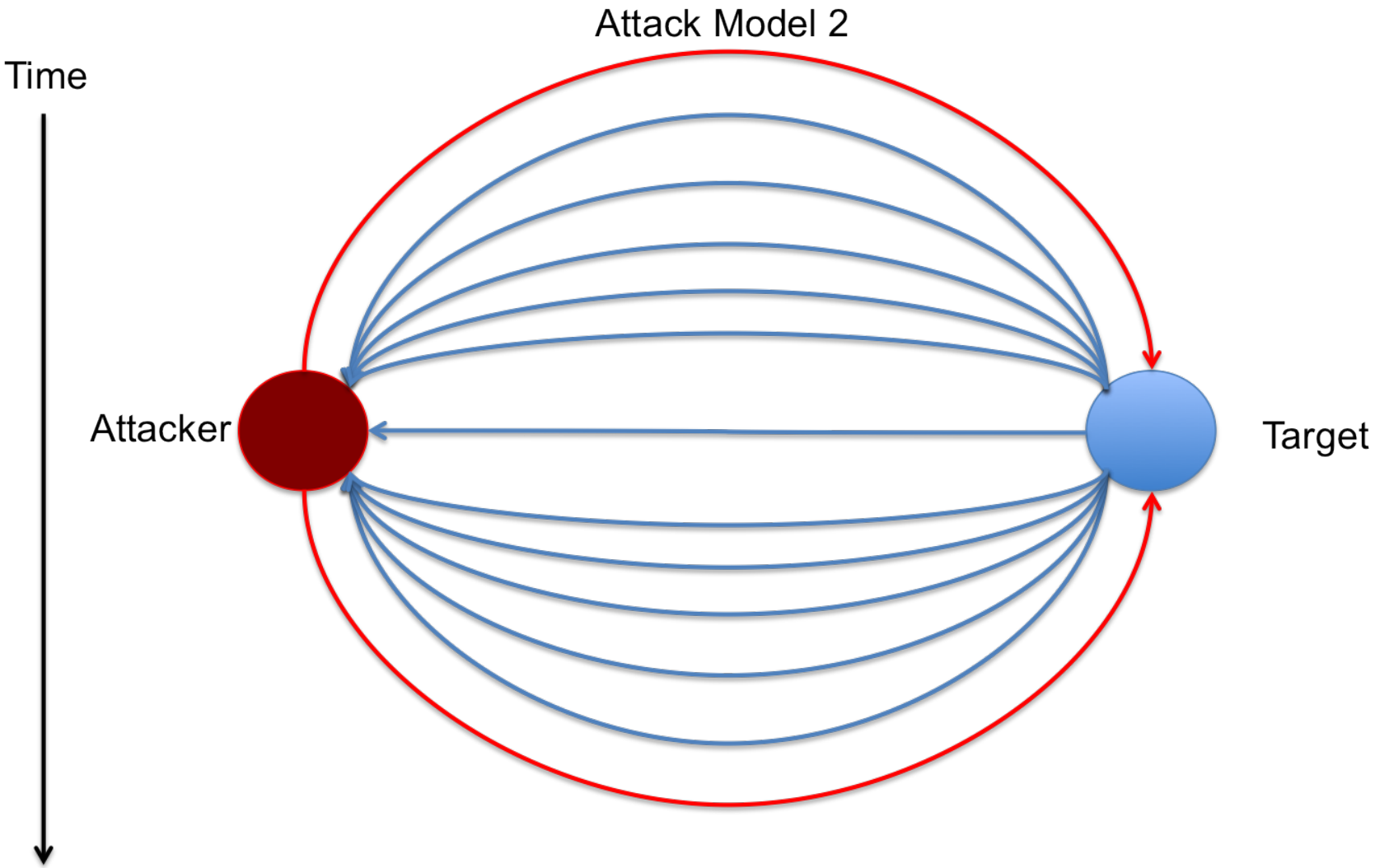
Attacks on WSN power supplies

- **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
- Here we show some of our attack models

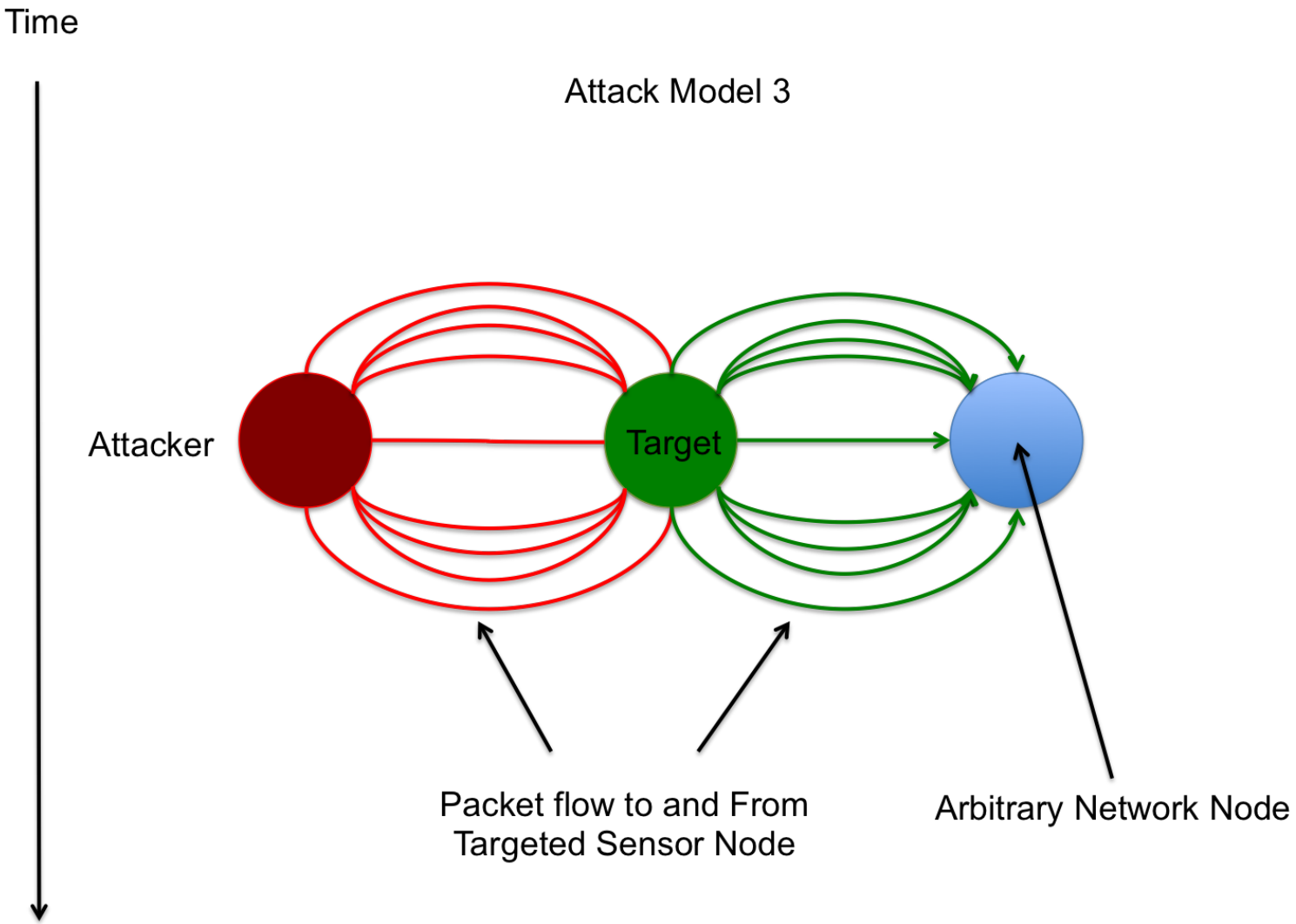
Attack Models (1) - standard denial of sleep



Attack Models (2) - inverse denial of sleep



Attack Models (3) - routing power draw



Problem

- **How do we defend against a wide range of Power Consumption Attacks?**

Outline

Overview

- we simulated **standard denial of sleep attacks** and **routing power draw attacks** on WSNs
- we first examined different **batteries**
- we then simply examined the **time to compromise** a node under various different assumptions

Battery Tests

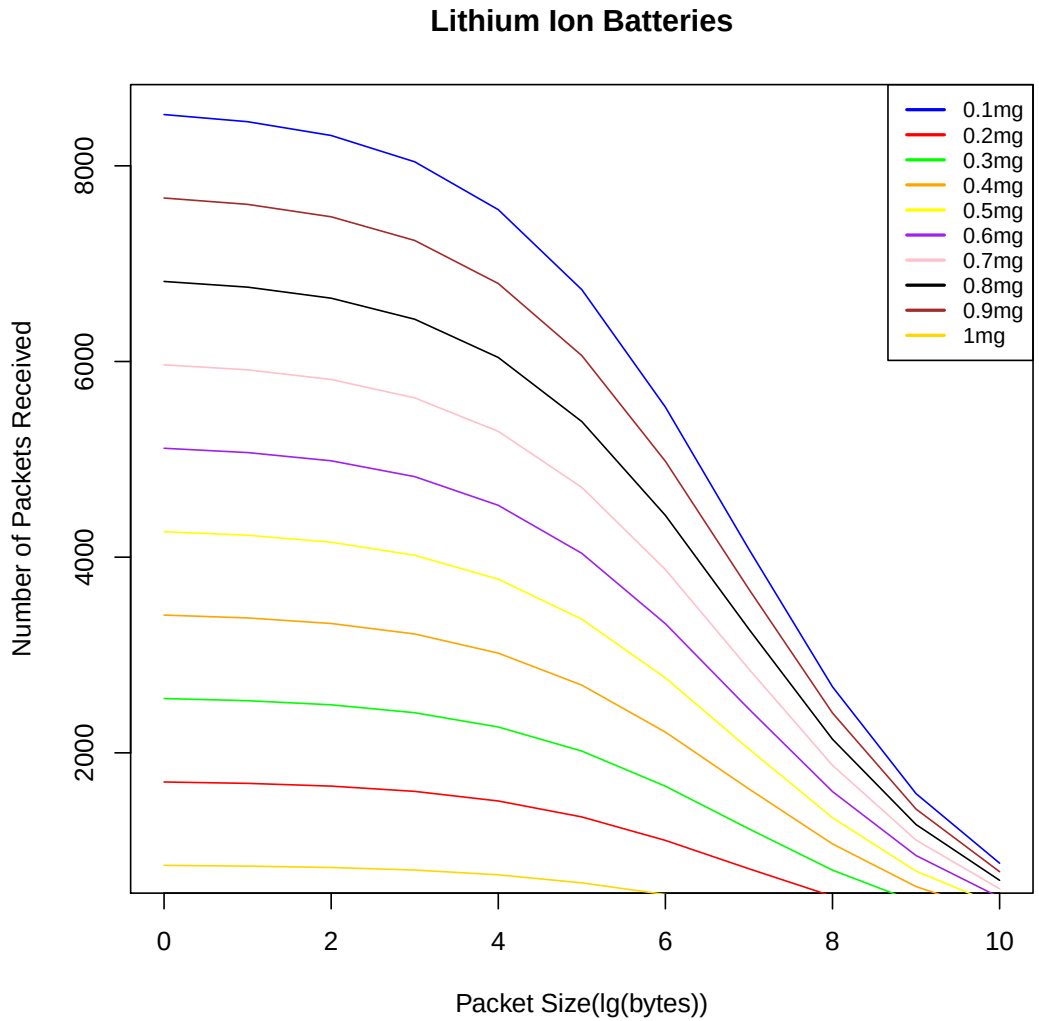
- The logical conclusion to mitigate risks of **Power Consumption Attacks** is to use more powerful **batteries**
- Another simulation we ran tested various types of batteries
- The batteries tested were:
  - Lead-Acid Batteries
  - Alkaline Long-Life Batteries
  - Carbon-Zinc Batteries
  - NiMH Batteries
  - 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

Attack Simulation

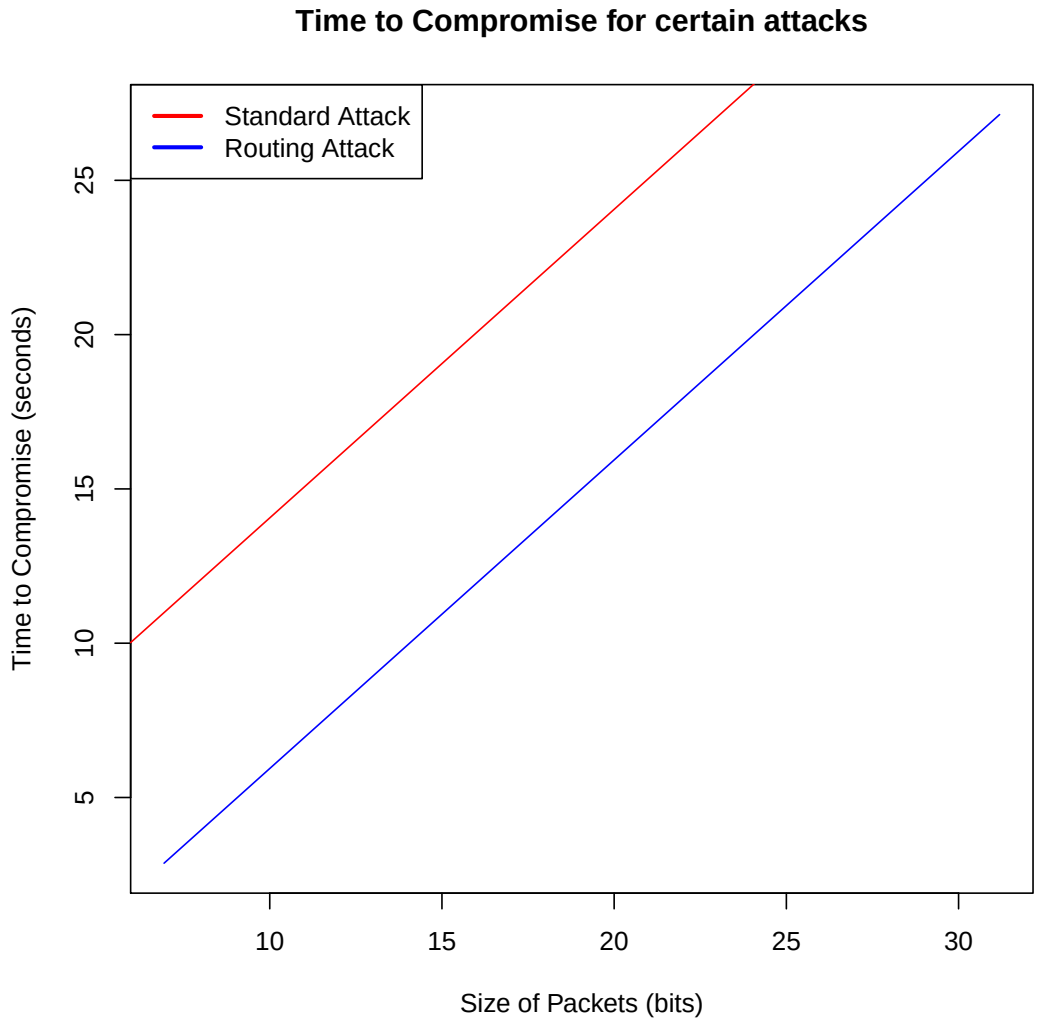
- The attacks were simulated in an environment that allowed user defined:
  - Packet Size (bits)
  - Initial Node Energy (joules)
  - Power To Transmit Messages (Watts)
  - Power To Receive Messages (Watts)
  - speed of Transmission radios (bps)
- Each of these were variate for **55,000** simulations

Outline

Lithium Ion Results



Comparing Attacks



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

- 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 benefit

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