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

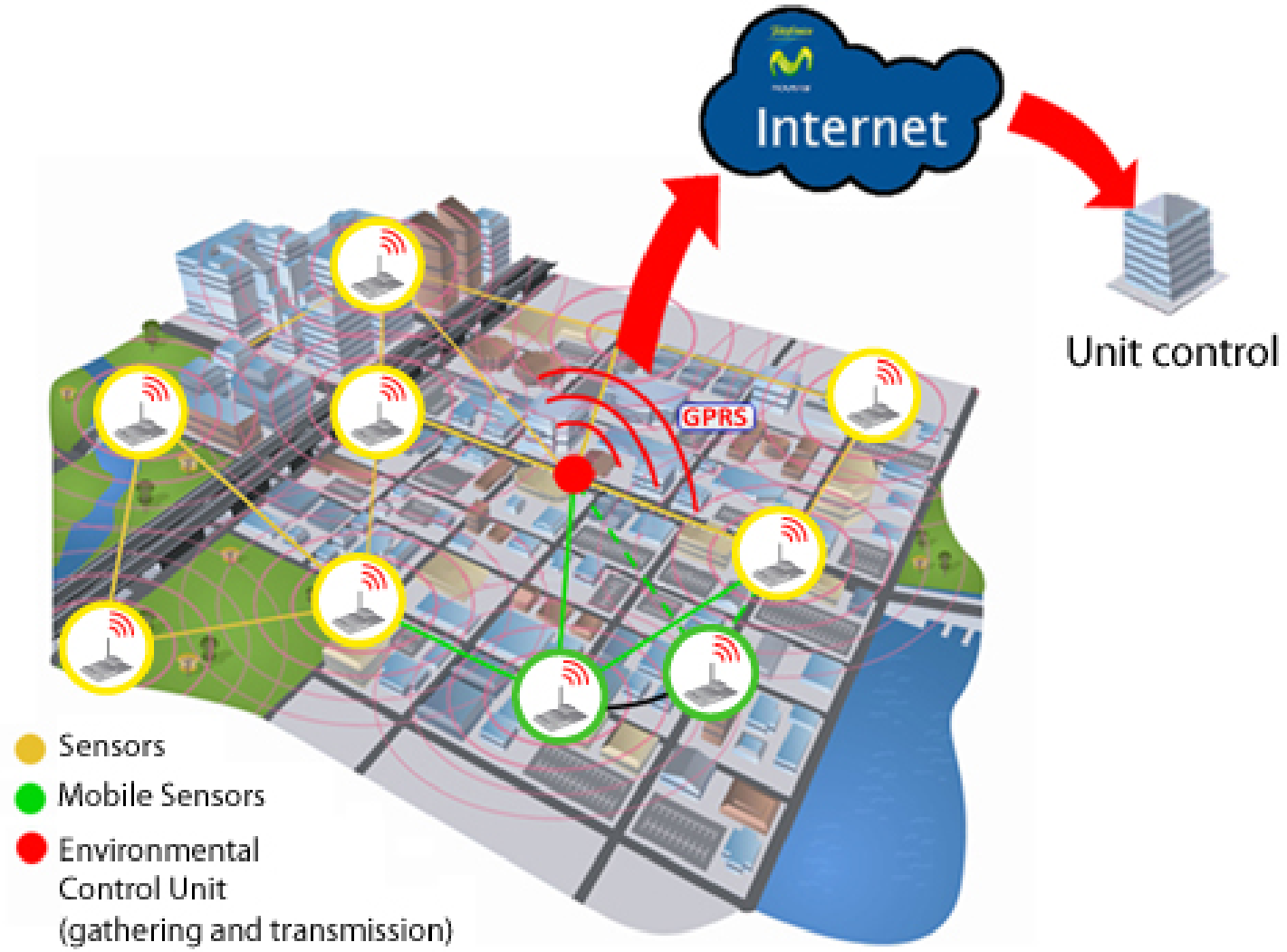
Outline of today's talk

Outline

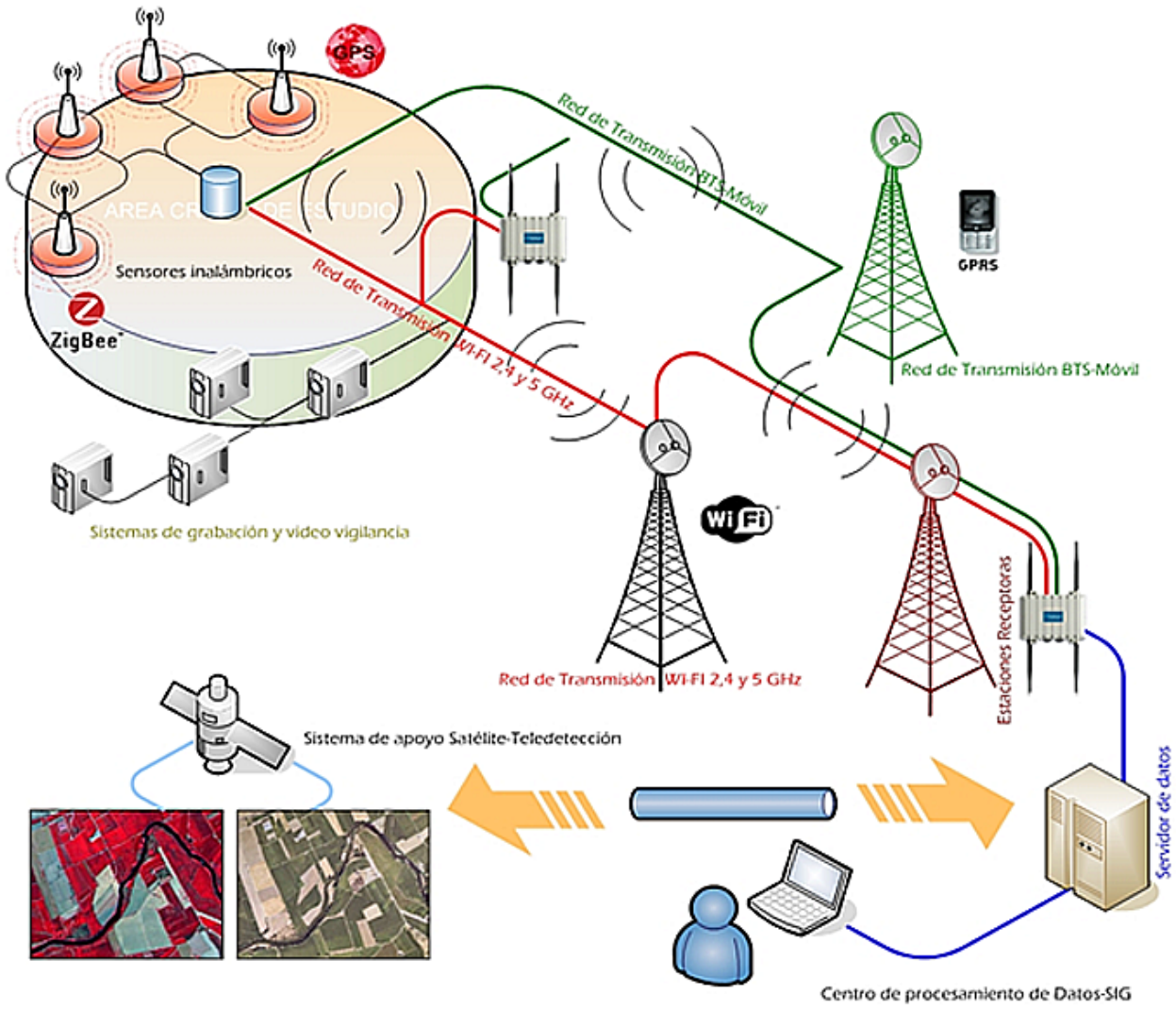
Brief Intro to Wireless Sensor Networks(WSNs)

- A **wireless sensor network(WSN)** is a network of **Sensor Nodes**
- **Sensor Nodes** send and receive wide varieties of data.
- **Sensor Nodes** are developed in bulk for mass deployment
- **Sensor Nodes** operate in one of two states:
  - **Sleep Mode** - less power draw, can't receive and transmit
  - **Active Mode** - more power draw, can receive and transmit
- **WSNs** can be applied to many problems

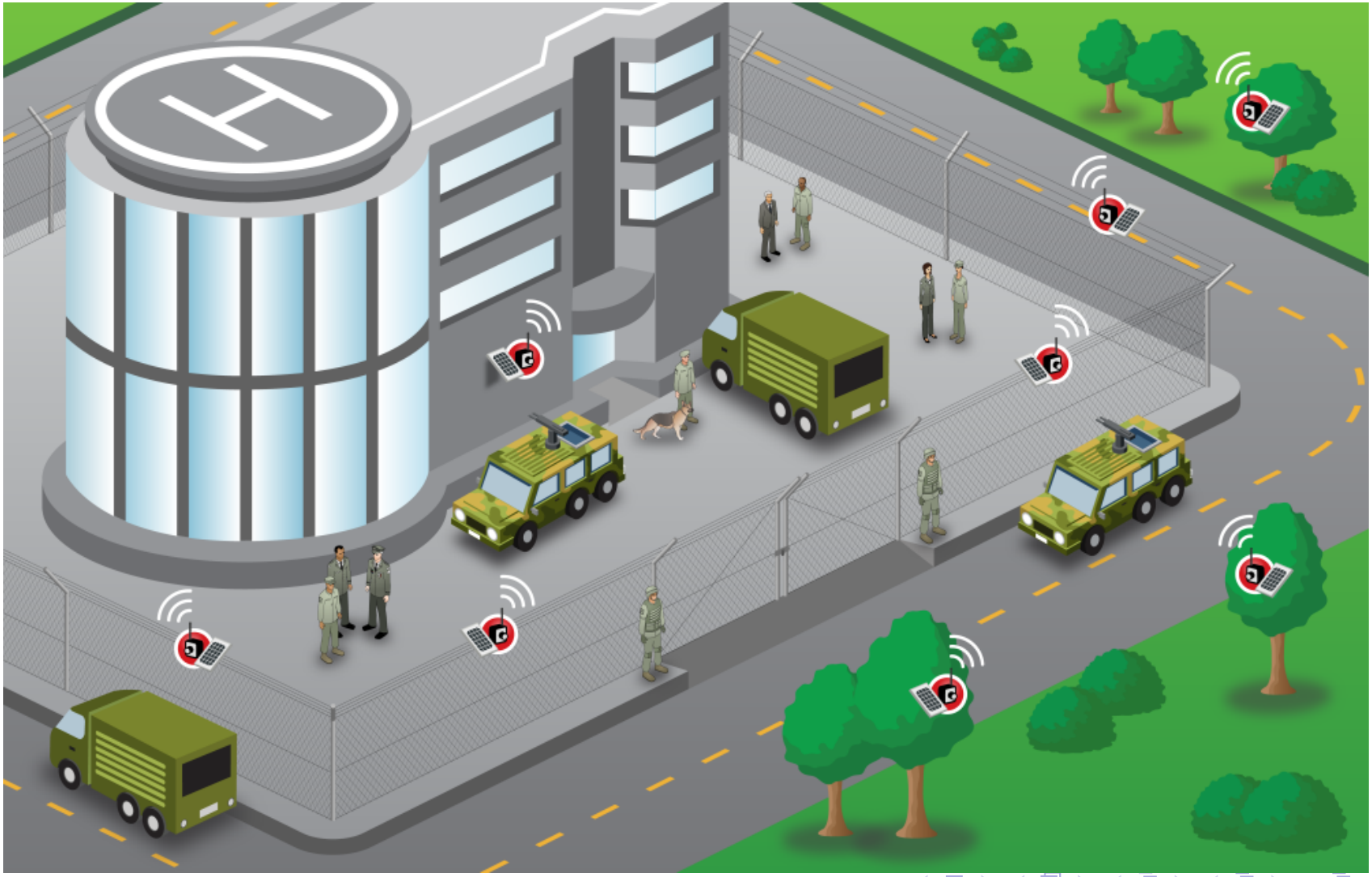
WSN examples (1)



WSN examples (2)



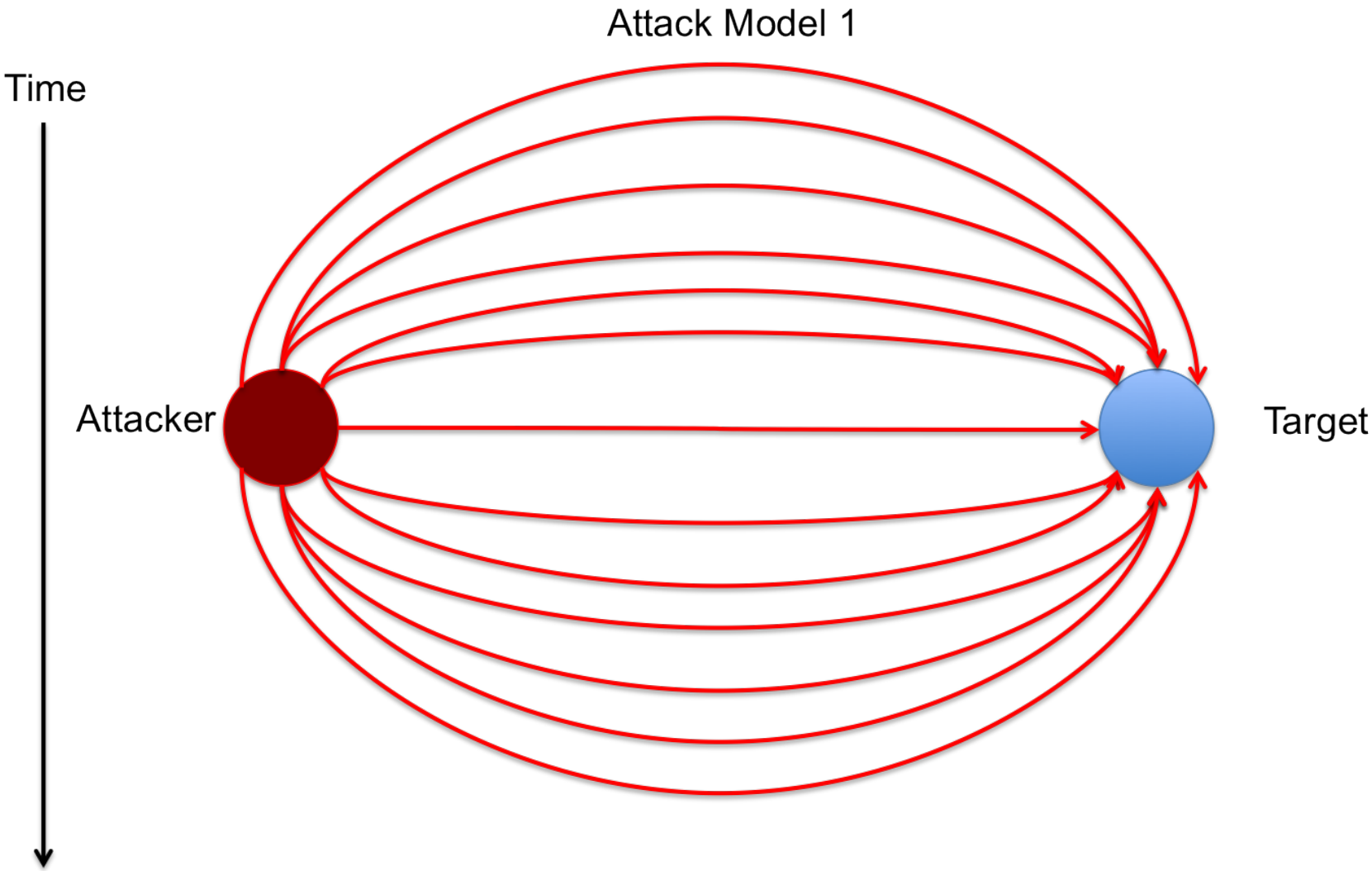
WSN examples (3)



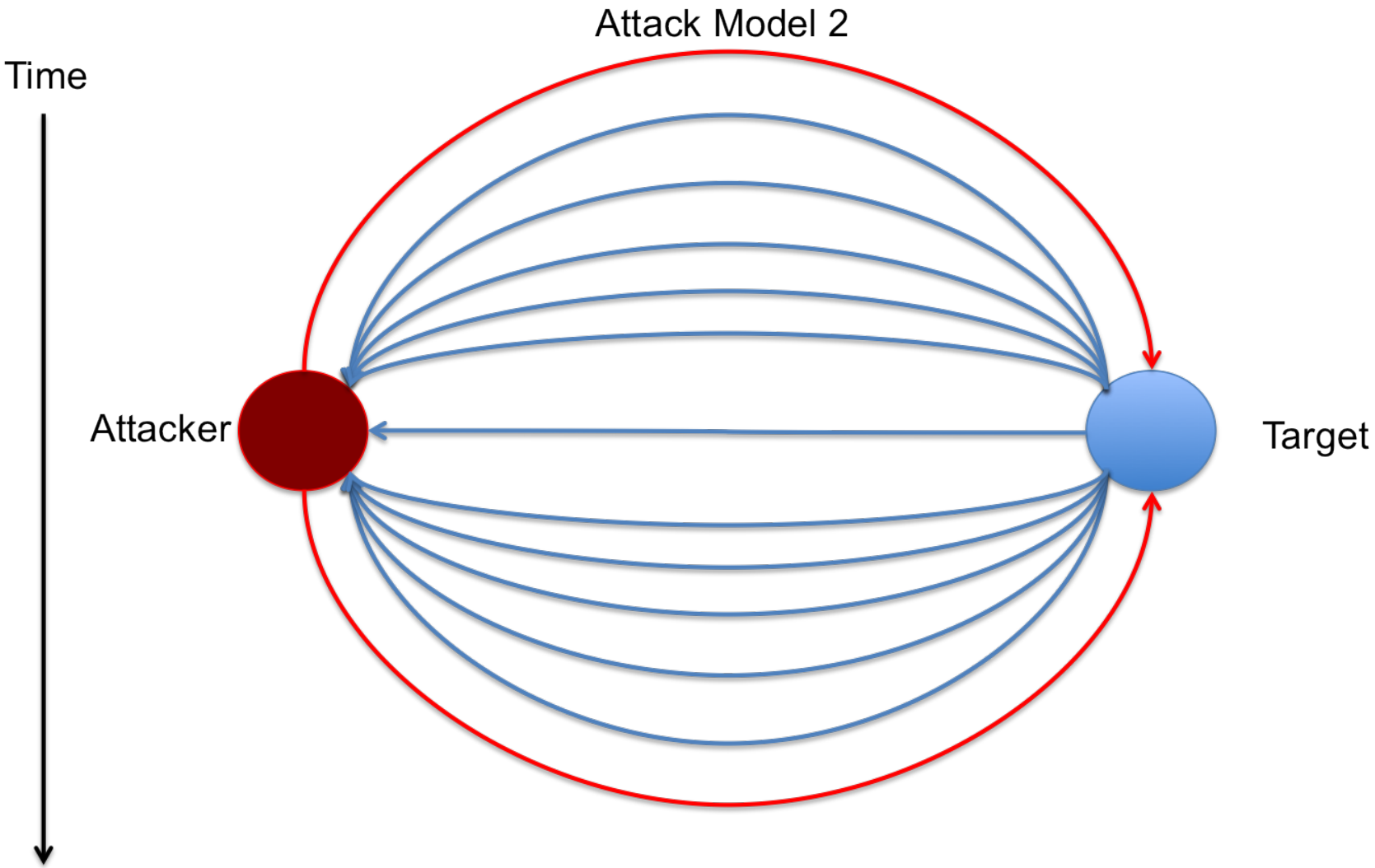
Attacks on WSN power supplies

- Bulk production has robbed WSNs of more robust **battery lives**
- The nature of WSNs makes them easy targets for **Power Consumption Attacks**
- A **Power Consumption Attack** exploits the small battery life of Sensor Nodes by draining the battery
- This attack can have devastating effects on the WSN
- **Power Consumption Attacks** are performed in multiple ways

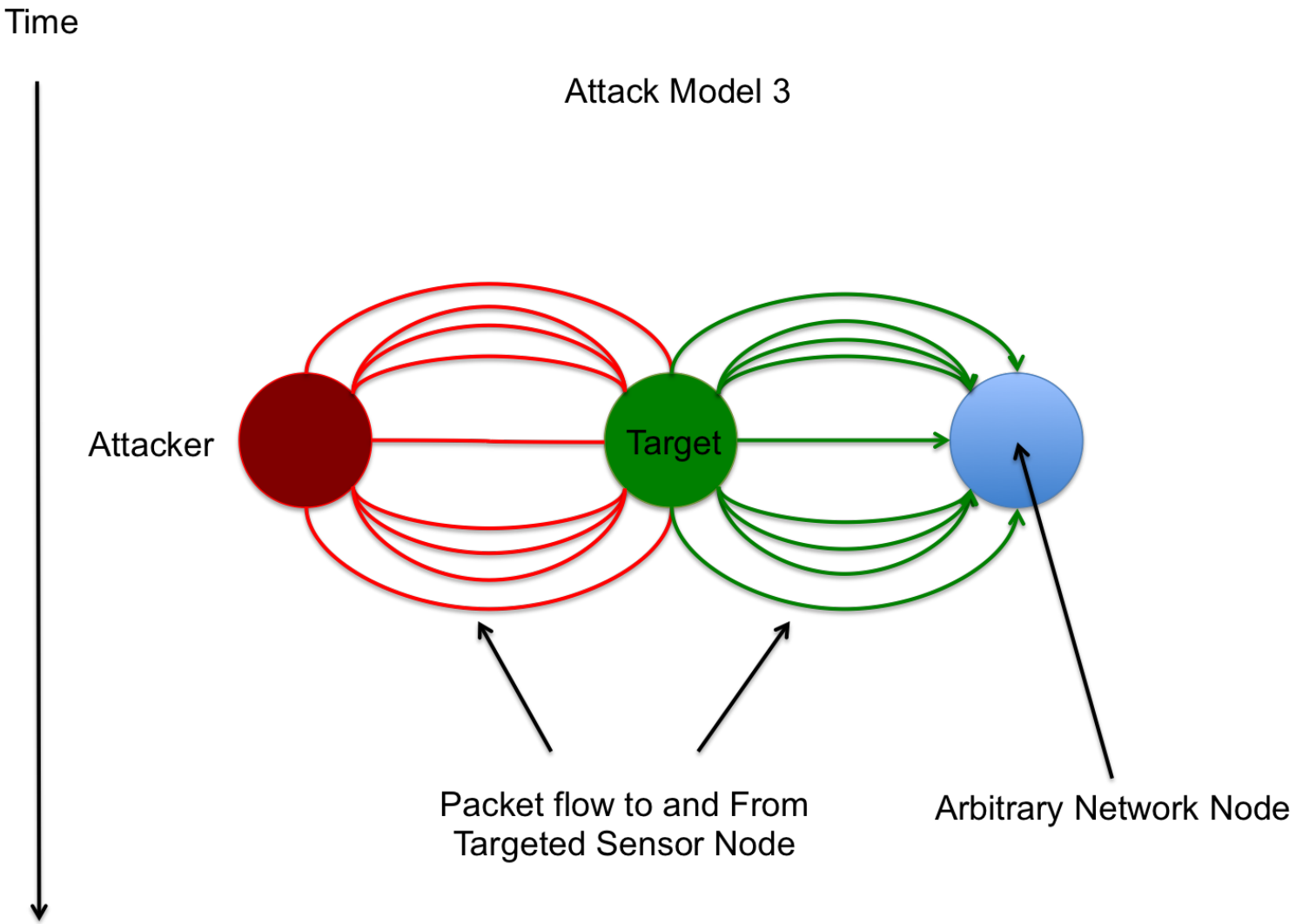
Power Consumption attack models



Power Consumption attack models (2)



Power Consumption attack models (3)



Problem

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

Outline

Attack Simulation

- The **Standard Power Consumption attack** refers to the attack seen in model 1
- It was simulated in an environment that allowed for user defined:
- The **Routing Power Consumption attack** refers to the attack seen in model 3

Battery Tests

- The first simulation results tested different types of **batteries**
- The logical conclusion to mitigate risks of **Power Consumption Attacks** is to use more powerful **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**

Outline

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