What are Wireless Sensor Networks?

- Collection of small nodes, wirelessly connected
- Typically used to sense environmental changes (temperature, motion).
- Often deployed unattended in hostile settings.
- Both military and civilian usecases.

Critical to secure these networks due to its usage
- Protocols developed for securing those systems.
- Typically verified using simulation/testing.
- Incomplete, may leave some errors undetected.

Project Objectives: Formally Verify these Protocols.

Challenges in Formal Verification: Building Models

- Time consuming, challenging, and erroneous
- Unfamiliarity with modeling language (e.g. Promela).
- Need to spend efforts to produce models.
- May lead to differences between model and code.
- Need to keep model and code synchronized, hard.
- Solution: Automatic Model Extraction
  - Some work already, e.g. Banderra [Corbett et al.]
  - We address important domain-specific challenges.

Key Challenges in Model Extraction/Composition

- Objective is to verify security properties.
- Requires presence of malicious activity or Intruders
  - e.g. Dolev-Yao’s intruder model.
- One Intruder does not fit all (large state space).
- Need protocol specific customization of Intruders
  - ... further increasing cost of building models.

Acknowledgements

This work is supported by the US NSF grant CNS-0627354 on Specification and Verification Challenges for Security Protocols in Sensor Networks.