Department of Computer Science

Slede: Framework for Automatic Verification of Sensor Network Security Protocol Implementations

Youssef Hanna and Hridesh Rajan

Iowa State University

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.

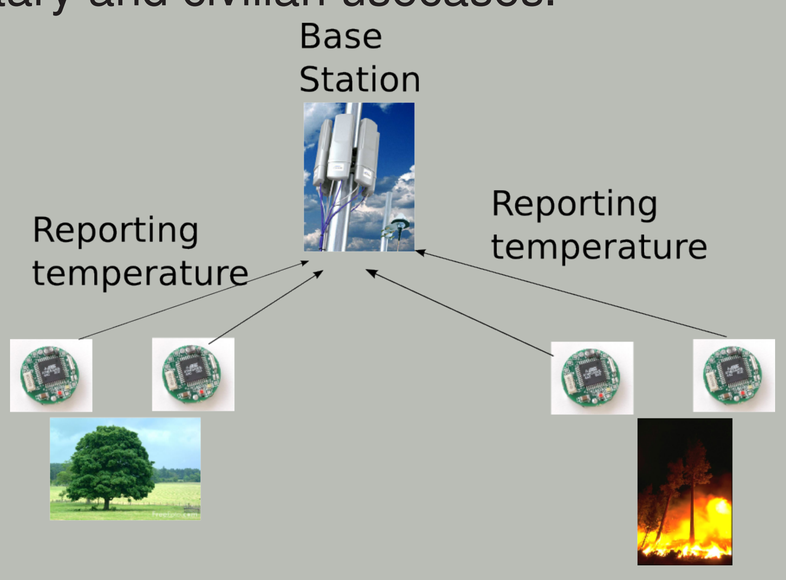


Figure: Example of a sensor network for fire detection in forests

- 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.
- **Advance**: Automatic Model Extraction and **Language-based technique for Intruder-Model Composition** for Sensor Network Security Protocols.

Acknowledgements

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

Solution: Extract Verifiable Model from Code

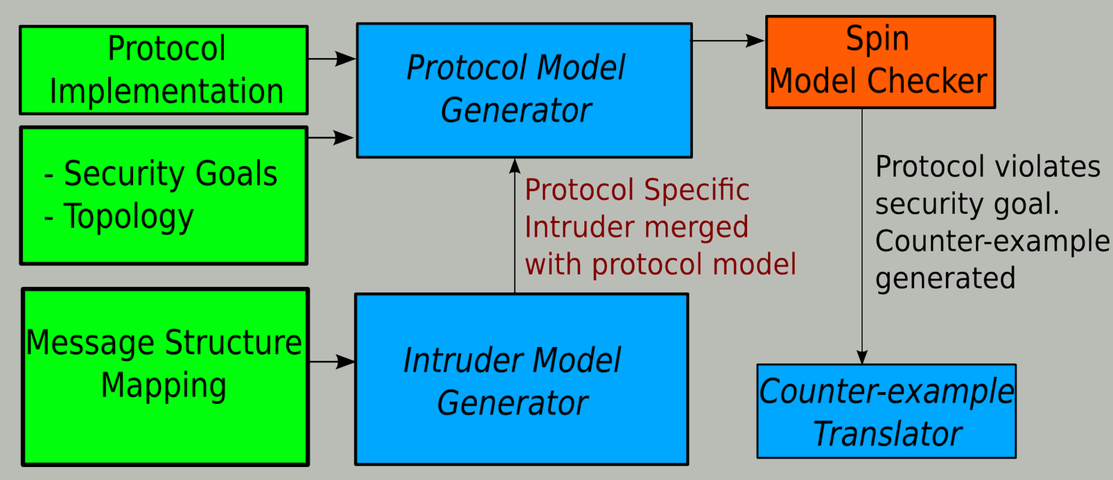
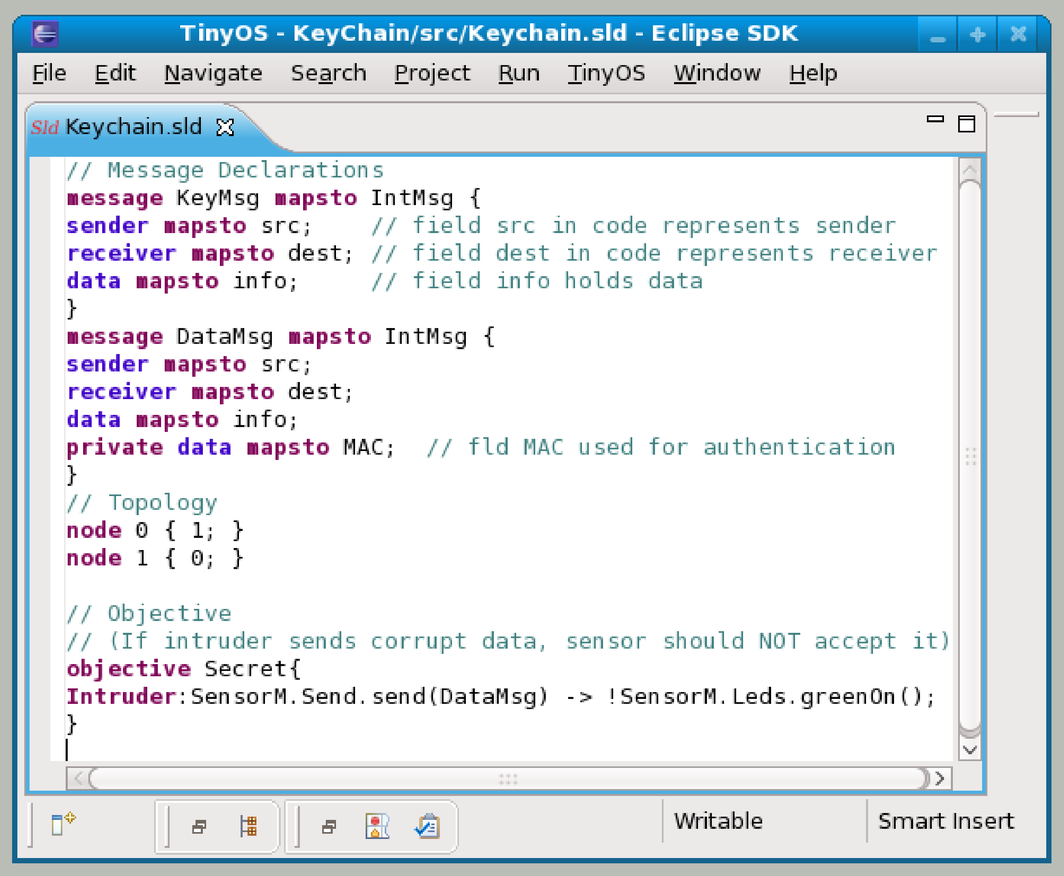


Figure: Framework for verification from implementation



- Information about security goals and message structure mapping can be written using our annotation language.
- Protocol model generator extracts the model representing the protocol behavior.
- Intruder model generator uses information about message structure of implementation to generate a **protocol specific intruder model**.
- The generated intruder model can now launch attacks customized to the protocol implementation.
- Example: Intruder can alter the data or change the sender (impersonation attack) of intercepted messages and forward the modified version.

Key Features of Slede

- Ultra-lightweight protocol specification.
- Completely automatic generation of verifiable model from nesC code of the sensor application.
- Automatic generation of protocol-specific intrusion model and its composition with the verification model of the protocol.
- Automated verification of the composed model.
- User-friendly output, in case of protocol faults.
- Tight-integration with existing tool-set for nesC developers.

[ywhanna,hridesh]@cs.iastate.edu