Security Issues in Wireless Networks

Irena Bojanic, Alvaro Cardenas, Behnam Neekzad, Svetlana Radosavac, John S. Baras

MAC Layer Fault Detection

- **MAC and routing layers interact**
- Possible to cause an attack by **manipulating traffic in the MAC layer** and propagate attack to the routing layer
- **Goal:** Detect the intrusion, minimizing detection time t_D and the number of false alarms, while maximizing the probability of detection P_D.
- We consider attacks that **employ legitimate communications which result in node misbehavior** and attack propagation through the network
- Single and colluding malicious nodes utilize legitimate communication patterns to **isolate one or multiple nodes** in the network
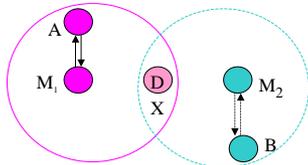
- The attacks **start in the MAC layer and propagate to the routing layer**, breaking old (legitimate) routes and creating new routes that contain malicious nodes
- **We represent MAC protocols in the form of Extended Finite State Machines**
- For attack detection formulate series of rules a fault-free MAC protocol cannot violate
- Automatic Model Checking is executed with input of the relevant rule parameters from the nodes under examination
- Rules are input in the form of Computation Tree Logic (CTL) formulas.

Routing Anomaly Detection

- Node mobility pattern is modeled by an **Hidden Markov Model (HMM)**
- The hidden states of the **HMM** can be viewed as abstractions of different spatial configurations of the mobile nodes
- The observed variables are the **hop count distribution** (i.e. packet flow pattern)
- The goal is to use the **allowable/normal state transitions** for change detection


Hidden state   **Observations**
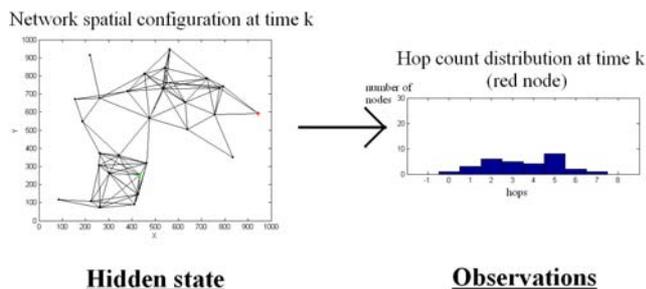
Security of Distributed Sensor networks

- **What's different?**
- No physical security
- Interaction with the physical environment
- Unknown topology before deployment
- Resource Constraint
- **Challenges:**
- Must avoid complex protocols
- Crypto must run on wimpy devices
- Need to minimize packet overhead

Application Layer Intrusion Detection

- Probabilistic Virtual Space
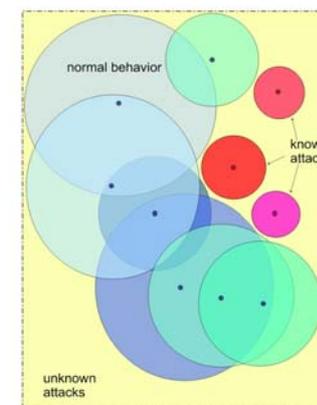
- **Initialization**: creation of probabilistic models and databases
- **Parallel testing and training**: probabilistic testing of current behavior while creating its model for possible future use
- **Logic**: testing via assignment of weight probabilities to attack logic transitions
- **Verification**: probabilistic cross-testing of suspicious behavior
- **Adaptive phase**: adaptation of relevant databases
- **False Alarm Rate Reduction:**