Lightweight Intrusion Detection for Sensornets

Vijay Bhuse,1 Ajay Gupta1 and Leszek Lilien1,2
1WiSe Lab, Western Michigan University  2Affiliated with CERIAS

1. Outline
- Motivation (2)
- Current work
  - Masquerade detection (3, 4)
  - Detection of packet dropping (5, 6)
  - Detection of unacceptable information source (7,8)
  - Anomaly-based techniques across multiple layers (not reported here)
- Future work (9)
- Selected publications (9)

2. Motivation for lightweight intrusion detection
- Cryptography for prevention is computationally expensive for resource-constrained sensor nodes
  - Hence lightweight techniques are needed
- Prevention fails when an unguarded node is captured leading to an easy secret key compromise for symmetric cryptography
  - Hence intrusion detection is needed
- DoS attacks disrupt the sensornet
  - Hence intrusion detection is needed

3. Masquerade detection
- A can overhear that X masquerades as A
  - Due to range overlap
- A alerts B about it

4. Simulation results for masquerade detection
- In an area 100m x 100m, success probability ≥ 95% for a network of 100 nodes with antenna range ≥ 15m

5. Detection of packet dropping
- Use alternate paths to detect if packets are dropped by nodes on the original path
- Detect and isolate packet-dropping paths periodically
  - Instead of monitoring packet-dropping nodes continuously
- Detection overhead: 2.6% of energy the network consumes on DSR path discovery

6. Simulation results for detection of packet dropping
- Probability of detection is 80% when ratio of packet-dropping nodes < 4% and path length ≤ 5 in network with 13-hop diameter

7. Detection of unacceptable information source (DUIS)
- Nodes know what information to expect from which neighbors
- D expects info of type INFO2 from K only; drops INFO2 forwarded by F

8. Simulation results for DUIS
- Detection overhead: 1.4% of energy the network consumes on DSR path discovery and packet transmission
  - 1.1% for Directed Diffusion (DSDV)
- More packets from unacceptable sources are detected when more nodes perform DUIS

9. Future work
- Detection of Sybil attacks, code tampering, wormholes & blackholes
- Secure distribution of local detection information
- Design of uniform framework for different attacks

10. Selected publications