WiSe (Wireless Sensornet) Laboratory

WESTERN MICHIGAN UNIVERSITY

Lightweight Intrusion Detection for Sensornets

Vijay Bhuse,[1] Ajay Gupta[1] and Leszek Lilien[1,2]
[1]WiSe Lab, Western Michigan University [2]Affiliated with CERIAS

1. Outline

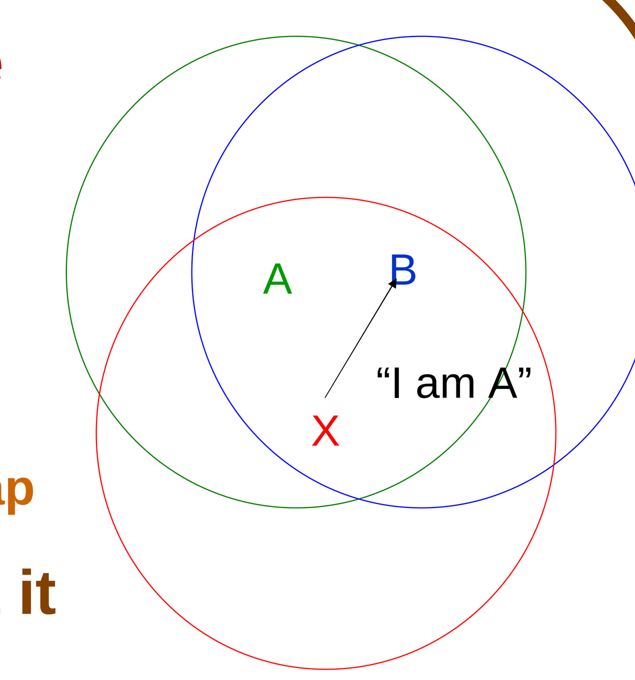
- Motivation (2)
- Current work
  - Masquerade detection (3, 4)
  - Detection of packet dropping (5, 6)
  - Detection of unacceptable information source (7,8)
  - Anomaly-based techniques across multiple layers (not reported here)
- Future work (9)
- Selected publications (9)

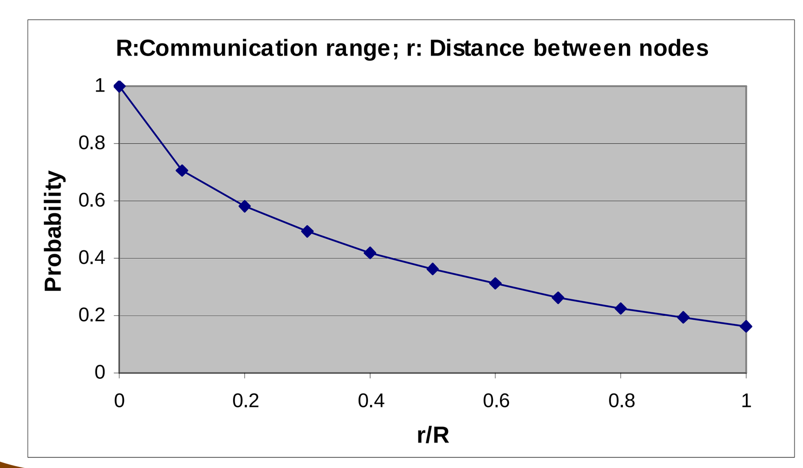
2. Motivation for lightweight intrusion detection

- Cryptography for prevention is computationally expensive for resurce-contrained 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 masque-rades as A
  Due to range overlap
- A alerts B about it

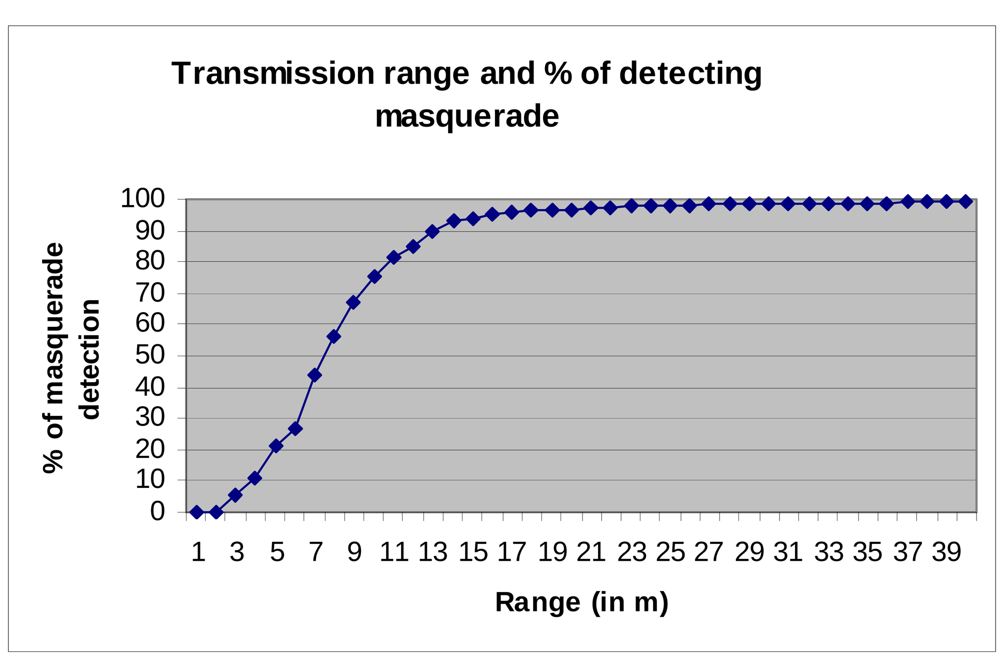




Detection probability inversely proportional to r/R

4. Simulation results for masquerade detection

- In an area 100m x 100m, success probability $\geq$ 95% for a network of 100 nodes with antenna range $\geq$ 15m

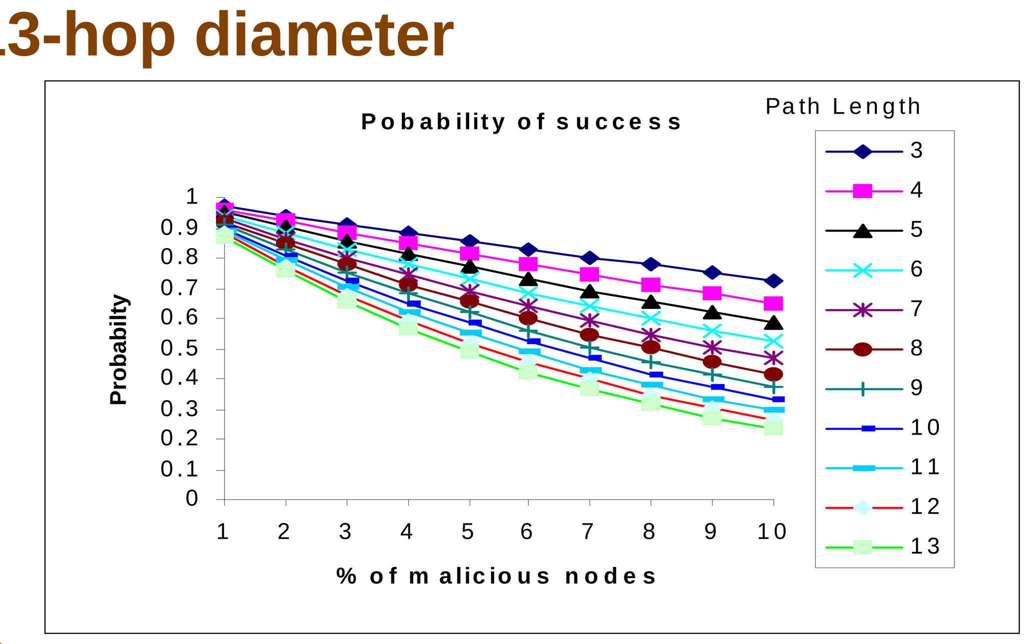


5. Detection of packet dropping

- 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

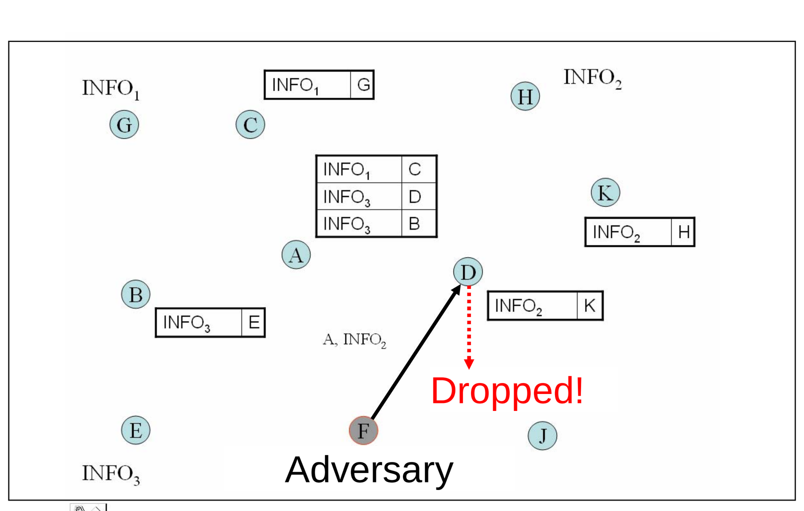
6. Simulation results for detection of packet dropping

- Probability of detection is 80% when ratio of packet-dropping nodes < 4% and path length $\leq$ 5 in network with 13-hop diameter



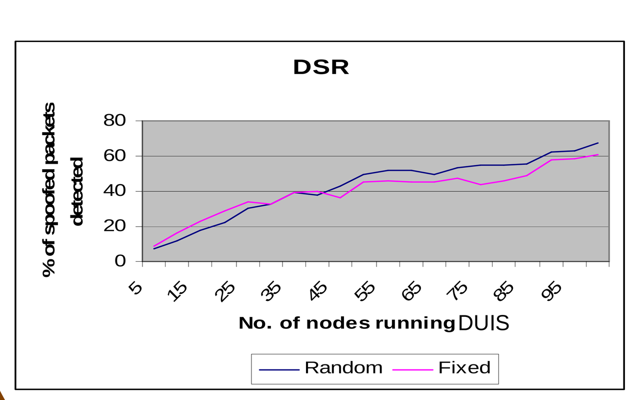
7. Detection of unacceptable information source (DUIS)

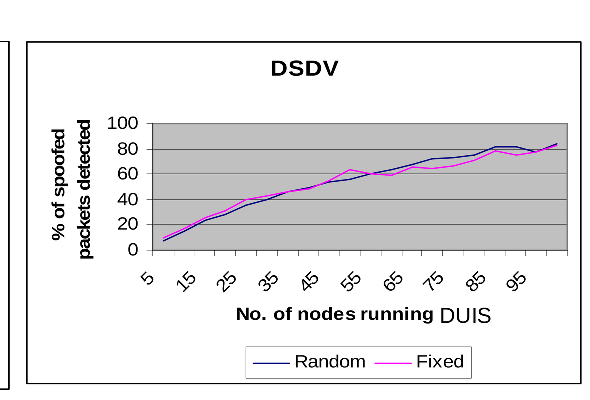
- Nodes know what information to expect from which neighbors
- D expects info of type $INFO_2$ from K only; drops $INFO_2$ forwarded by F



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

- V. Bhuse and A. Gupta, "Anomaly Intrusion Detection in Wireless Sensor Networks," *J. of High Speed Networks*, vol. 15, issue 1, Jan.-Mar. 2006.
- V. Bhuse, A. Gupta and L. Lilien, "DPDSN: Detection of packet-dropping attacks for wireless sensor networks," *Proc. Trusted Internet Workshop, Intl. Conf. on High Performance Computing*, Dec. 2005.
- V. Bhuse, A. Gupta, M. Terwilliger, Z. Yang and Z. Kamal, "Using Routing Data for Information Authentication in Sensor Networks," *Proc. 3rd Intl. Trusted Internet Workshop (TIW), Intl. Conf. on High Performance Computing*, Dec. 2004.