An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks

Sensor networks

A sensor node (mote)

- 4Mhz processor, 128K flash memory
- magnetism, light, heat, sound, and vibration sensors
- wireless communication up to 100m
- costs “in bulk” ~$5 (now $80~$150)

Applications include

- ecology monitoring, precision agriculture, civil engineering
- traffic monitoring, industrial automation, military and surveillance

Energy and resource limitation is a key challenge in WSN

- communication-efficient, lightweight programs are needed

Sybil attack

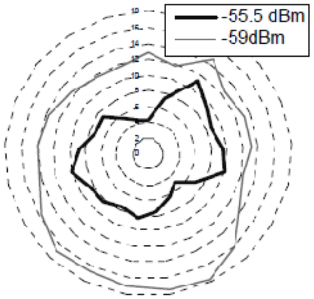
- A sybil node tries to forge multiple identification in a region
- Sybil attack is particularly easy to perform in WSN
  - the communication medium is broadcast
  - same frequency is shared among all nodes
- A sybil node can rig the vote on group-based decisions and disrupt network middleware services severely

Existing solutions are costly

- Existing solutions for sybil attack prevention are too costly for the resource-poor sensor platforms
  - excessive communication burden on nodes are not acceptable since they drain the battery power quickly
- Solutions that adopt key exchange for identification
  - severely effect the energy consumption due to distribution and piggybacking of randomly generated keys in messages, and
  - consume precious memory space as every node is required to store pairwise keys with neighbors

RSSI-based solution?

- Upon receiving a message, the receiver will associate the RSSI of the message with the sender-id included, and later when another message with same RSSI but with different sender-id is received, the receiver would detect sybil attack
- Lightweight solution !



- Problem: RSSI is unreliable and time-varying !
- Problem: RSSI is a function of transmission power !
  - a sybil node can send messages with different IDs using varying transmission power to trick the receiver

Our contributions

- We implement a sybil attack detection technique based on using ratios of RSSIs from multiple nodes
  - The technique was first introduced as a localization solution by Zhong et. al., but this is the first time it is implemented in WSN
- Our solution is robust & lightweight
  - We detect all sybil attack cases with very little false-positives
  - We show that instead of 4 detectors prescribed in theory, two detectors performs just as well in practice

Outline

- **Problem statement**
- **RSSI-based localization**
- **RSSI-based sybil detection**
- Experiments with RSSI
  - Variance of RSSI
  - Variance of ratios of RSSI
- Experiments with sybil detection
  - 4 detectors (completeness / accuracy)
  - 2 detectors (completeness / accuracy)

Problem statement

Model

- Static network: nodes are immobile after initial deployment
- We assume an initial set of nodes that are trustworthy
- New nodes are introduced to network (some may be sybil)
  - ➢ For repopulation, or due to topology-control and sleep-wake up protocols
- Sybil nodes can vary transmission power to trick other nodes

- Completeness: If there is a sybil attack in the network, detect the attack with probability greater than 99%
- Accuracy: Do not identify non-sybil nodes as sybil

RSSI-based localization

- Using 4 nodes as detectors it is possible to localize any node
  - RSSI at i for a transmission from node 0 with power P0 is $R_i = P_0 K / d_i^\alpha$
  - RSSI ratio of node i to node j is $R_i/R_j \; = (\frac{P_0 \cdot K}{d_i^\alpha})/(\frac{P_0 \cdot K}{d_j^\alpha}) = (\frac{d_i}{d_j})^\alpha$
  - Since P0 values cancel out in the ratio of RSSIs, this technique is unaffected by the changes to the transmission power P0

- The location (x,y) of a node can be calculated if locations of i, j, k, l are known

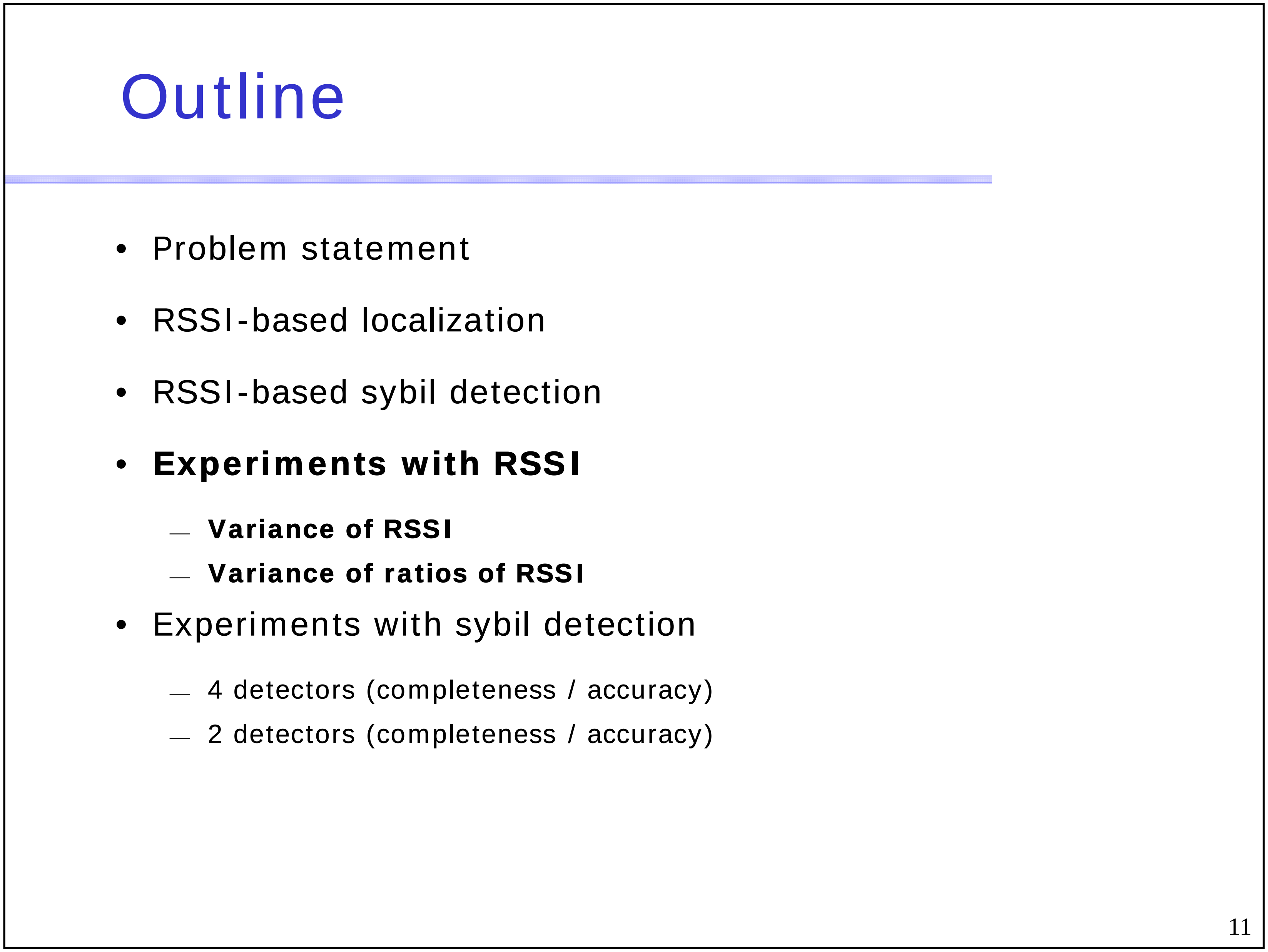
$$\begin{aligned}(x - x_i)^2 + (y - y_i)^2 \quad &= (\frac{R_i}{R_j})^{\frac{1}{\alpha}}((x - x_j)^2 + (y - y_j)^2) \\ &= (\frac{R_i}{R_k})^{\frac{1}{\alpha}}((x - x_k)^2 + (y - y_k)^2) \\ &= (\frac{R_i}{R_l})^{\frac{1}{\alpha}}((x - x_l)^2 + (y - y_l)^2)\end{aligned}$$

RSSI-based sybil detection

- No need to calculate node locations; we can detect sybil attack by comparing the ratio of RSSI for received messages

- Let D1, D2, D3, D4 be detectors, and sybil node tries to forge ids S1 and S2 at time t1 and t2
- Accumulating RSSI messages wrt HELLO(S1), and later HELLO(S2) D1 computes $\frac{R^{S1}_{D1}}{R^{S1}_{D2}}, \frac{R^{S1}_{D1}}{R^{S1}_{D3}}, \text{ and } \frac{R^{S1}_{D1}}{R^{S1}_{D4}}$ $\frac{R^{S2}_{D1}}{R^{S2}_{D2}}, \frac{R^{S2}_{D1}}{R^{S2}_{D3}}, \text{ and } \frac{R^{S2}_{D1}}{R^{S2}_{D4}}$

- D1 detects a sybil attack iff $(\frac{R^{S1}_{D1}}{R^{S1}_{D2}} - \frac{R^{S2}_{D1}}{R^{S2}_{D2}}) < \sigma, (\frac{R^{S1}_{D1}}{R^{S1}_{D3}} - \frac{R^{S2}_{D1}}{R^{S2}_{D3}}) < \sigma$ $, \text{ and } (\frac{R^{S1}_{D1}}{R^{S1}_{D4}} - \frac{R^{S2}_{D1}}{R^{S2}_{D4}}) < \sigma$

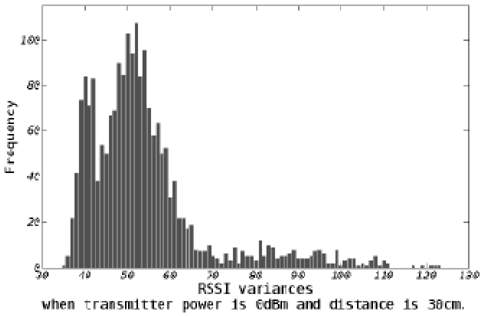


Outline

- Problem statement
- RSSI-based localization
- RSSI-based sybil detection
- **Experiments with RSSI**
  - **Variance of RSSI**
  - **Variance of ratios of RSSI**
- Experiments with sybil detection
  - 4 detectors (completeness / accuracy)
  - 2 detectors (completeness / accuracy)

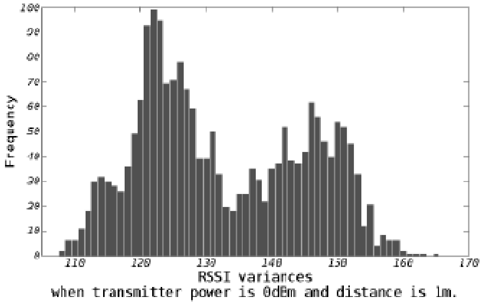
Variance of RSSI

- A node transmits messages >2000 times with constant transmission power
- Receiver (at 30cm and 1m) records RSSI
- TinyOS provides RSSI via TOS_Msg->strength



(a) ρ =51.00, μ =53.84, and σ =14.04 with distance of 30cm

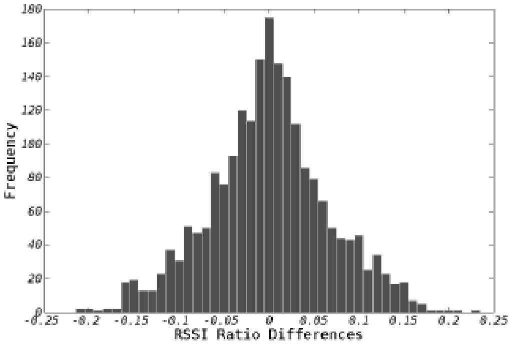
- Histograms show nonuniform nature of RSSI



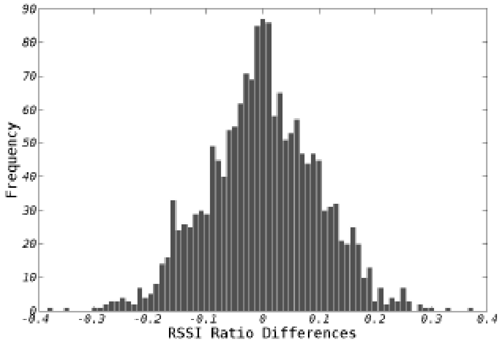
(b) ρ =129.00, μ =132.50, and σ =12.56 with distance of 1m

Variance of ratios of RSSI

- A node transmits messages >2000 times with **varying** transmission power
- Two receivers record RSSI, difference of ratios of RSSIs for each pair of transmissions are graphed
  - Since ratio of RSSIs are used, varying transmission power does not cause any problem
- Histograms show uniform distribution
  - Gaussian PDF with std. dev. 0.06 and 0.106



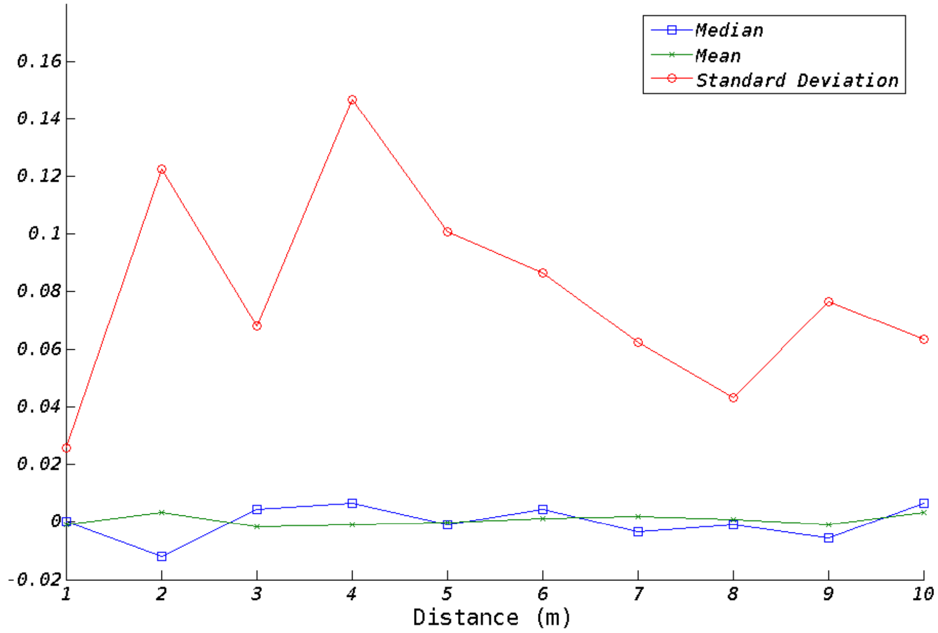
(a) $\rho = 0.000$, $\mu = 0.000$, and $\sigma = 0.066$



(b) $\rho = 0.000$, $\mu = 0.000$, and $\sigma = 0.100$

Effect of distance on ratio variance

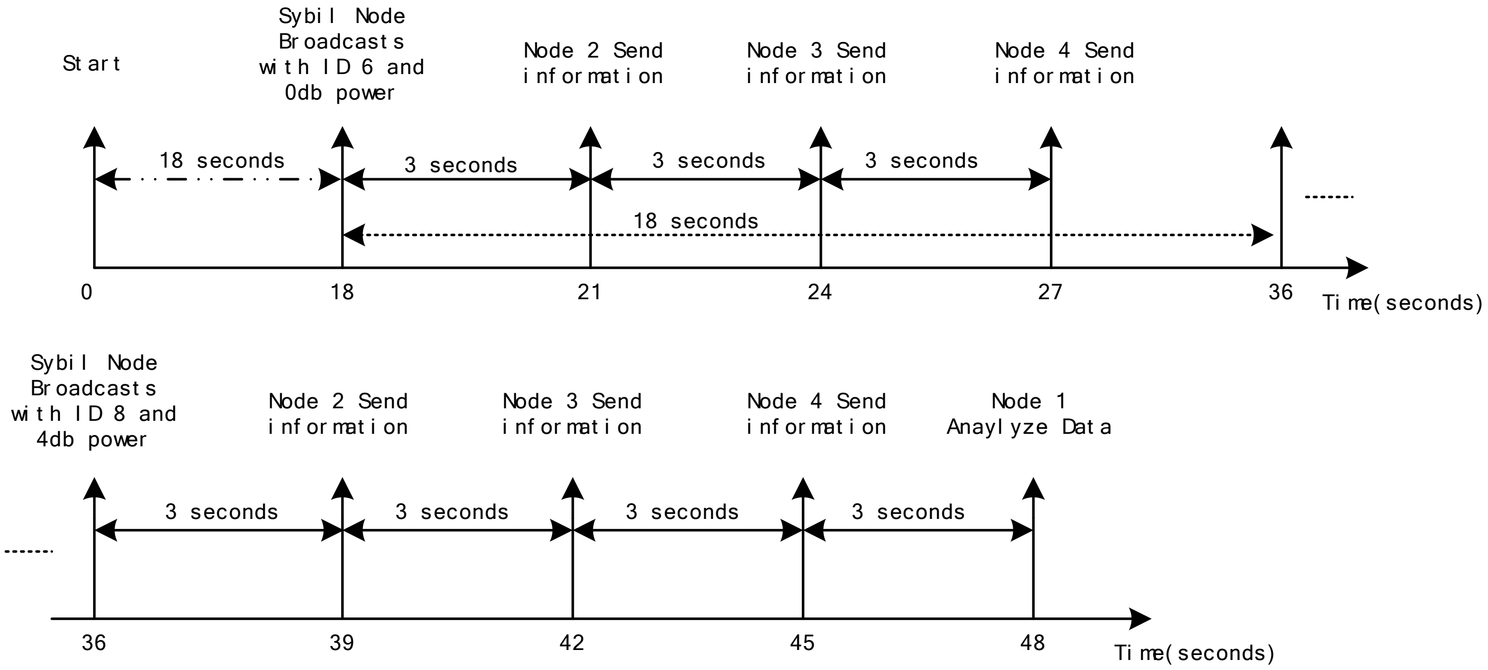
- std. dev. is around 0.1, so difference threshold is set to 0.5



Outline

- Problem statement
- RSSI-based localization
- RSSI-based sybil detection
- Experiments with RSSI
  - Variance of RSSI
  - Variance of ratios of RSSI
- **Experiments with sybil detection**
  - **4 detectors (completeness / accuracy)**
  - **2 detectors (completeness / accuracy)**

Experiment Scenario



Start

Sybil Node Broadcasts with ID 6 and 0db power

Node 2 Send information

Node 3 Send information

Node 4 Send information

18 seconds

3 seconds

3 seconds

3 seconds

18 seconds

0 18 21 24 27 36

Time(seconds)

Sybil Node Broadcasts with ID 8 and 4db power

Node 2 Send information

Node 3 Send information

Node 4 Send information

Node 1 Anaylyze Data

3 seconds

3 seconds

3 seconds

3 seconds

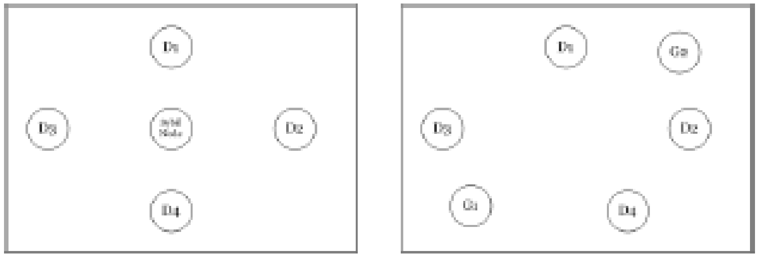
36 39 42 45 48

Time(seconds)

- Node 1 detects sybil node, based on input from 2, 3, 4

4 detectors

- Completeness: sybil node is detected 100%
- Accuracy: 0% false-positive rate

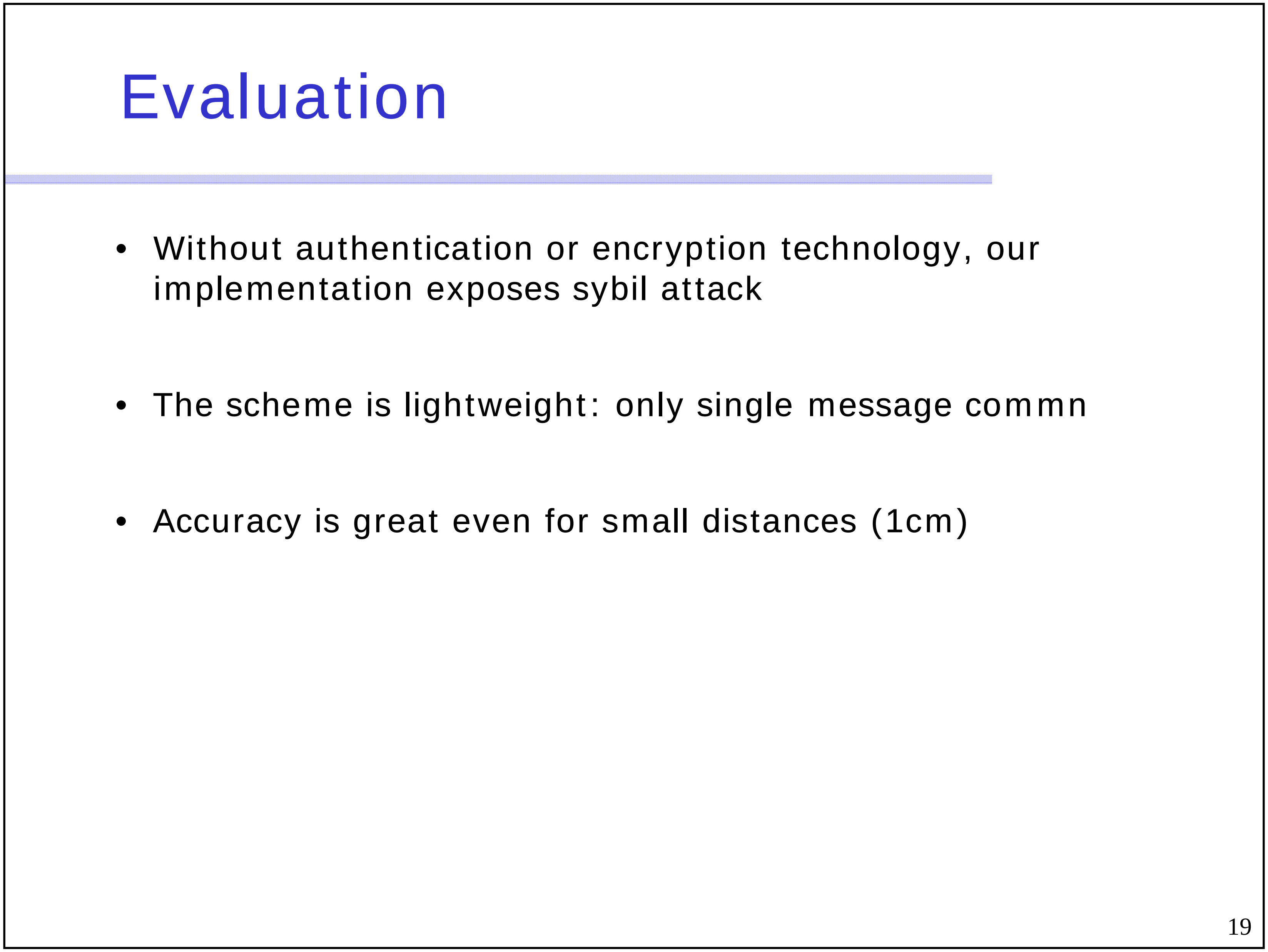


(a) Topology in case of four monitoring nodes and one sybil node

(b) Topology in case of four monitoring nodes and no sybil node. Gx represents good nodes, Dx, detectors

2 detectors

- Completeness: sybil node is detected 100%
- Accuracy: less than 5% false-positives
  - — Completeness is more critical than the accuracy
    - ➢ Not detecting a sybil node has severe implications for security, whereas falsely detecting upto 5% nodes as sybil only reduces the system performance
  - — Since 2 detectors has much less communication overhead and still acceptable false-positive rate, 2 detector case is more suitable than 4 detector case



Evaluation

- Without authentication or encryption technology, our implementation exposes sybil attack
- The scheme is lightweight: only single message commn
- Accuracy is great even for small distances (1cm)

Future work

- Design a distributed sybil attack detection protocol that tolerates existing sybil nodes in the network

- Existing sybil nodes may be modeled as Byzantine nodes
  - Broadcast medium can make it easier to detect Byzantine nodes

RSSI value instead of Power

- According to [2], the received power can be gotten in mica 2 by

$$P = -51.3 \cdot V_{RSSI} - 49.2 \text{ [dbm] at 433 MHz, where } V_{RSSI} \in \text{ [0V, 1.2V]}$$

- Since the power is linear to RSSI value, and the ratio will be used, there is no problem to adopt RSSI value instead of power when we detect sybil node.
- We denote R_i^k as RSSI value which is from node k to node i.