Security in Sensor Networks:

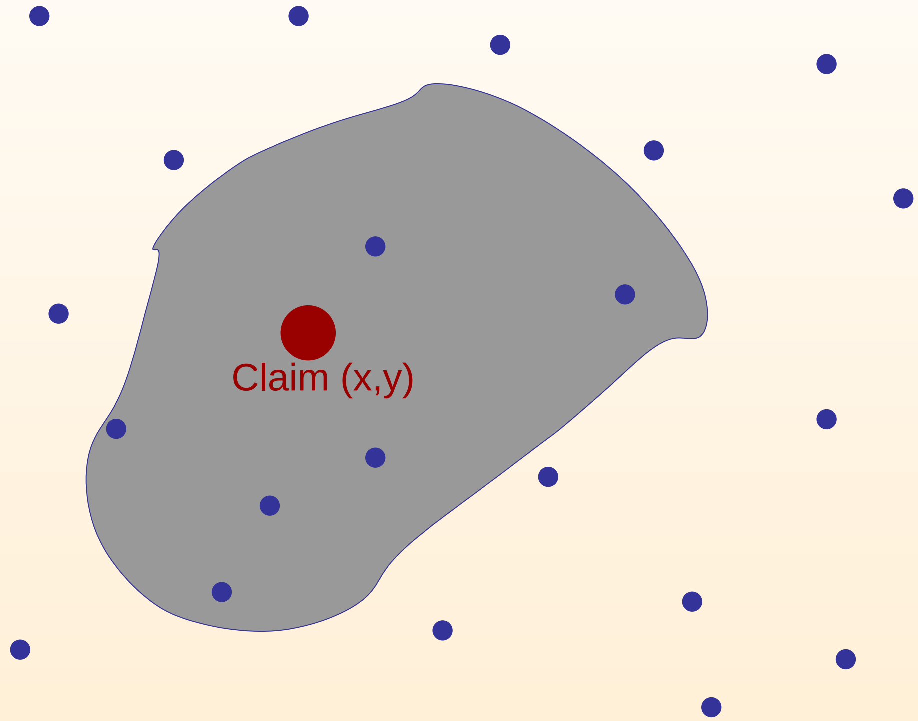
Proving location claims

Naveen Sastry with David Wagner

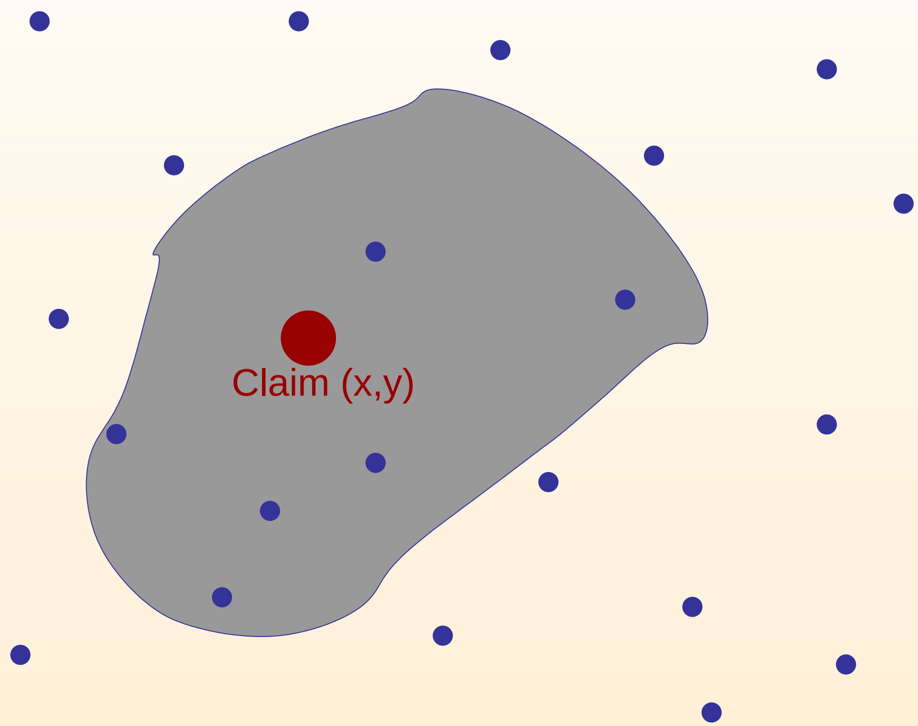
{nks, daw}@cs.berkeley.edu

June 17, 2002

Motivation: Granting Resource Based on Location



Motivation: Granting Resource Based on Location



Grant resources based on location

- Control of resources if mote is in "critical region"; eg, turn on lights if in room
- Allow proven motes to participate in protocols and have access to data

Formal Problem Description

A field of trusted motes with known locations

- Location known via localization or hardcoded
- Secure channels with each other – cannot be spoofed and messages get through.

An adversary a with unknown location, making a statement:

"a is at location (x, y)"

- An incorrect adversary does not have to follow protocol [more later].
- Adversary a may or may not be truthful

Mote field engages in a protocol.

Outputs a binary value: validity of claim

Does Cryptography Work?

Does Cryptography Work?

NO!

- Cryptography helps us validate the integrity of the message, not the contents
- Need to detect something different between a proper and forged location claim
  - ▷ A computation by the adversary is not the answer!

Need to correlate physical world to the motes.

- Properties that we can use to help corroborate
  - ▷ Sensing I: who detected an event by the claimant
  - ▷ Sensing II: can the claimant detect an event generated by the field?

A Diversion: Threat Models Under Traditional Cryptography

Threat Model: a description of the adversary's power

- eg: does the adversary have access to prior messages encrypted messages?
- eg: can the adversary generate encrypted messages?

Design protocols for the expected threat models.

- Defense against stronger threat models $\longrightarrow$ adversary with greater ability.

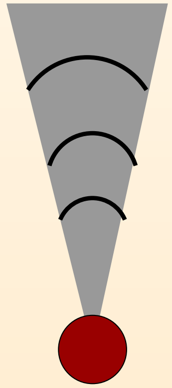
Can be seen as encapsulating the resources (money, computational power, . . .) that the adversary posesses.

Adversarial Powers in the Sensor Network Regime

Strength in numbers

- Obviously more adversaries $\longrightarrow$ harder to overcome / detect
- Placement of adversaries matters

Adversarial powers



- Its Radio Prowess
  - ▷ The sensitivity of the RF Listening
  - ▷ The RF Power
  - ▷ Transmission beam width (omni- vs. uni- directional)
- Similarly, adeptitude of other sensors and actuators
- Imitating motes
  - ▷ Spoofing legitimate mote communications
  - ▷ Listening in on legitimate mote communications

A First Crack at Mote Threat models

At least MICA like capabilities

- Entertain the possibility of hijacking one of the "good guys"
- i.e. Omni-directional RF transmission

Many adversaries

- assume have a means to coordinate with each other

Can listen in on traffic

No spoofing

- May be an orthogonal problem – can be solved using public key cryptography, for example.
- Easy attack: retrieve secret key from mote

Comparison to Localization

Localization is hard!

We're utilizing localization components – trying to find adversary in a localization field

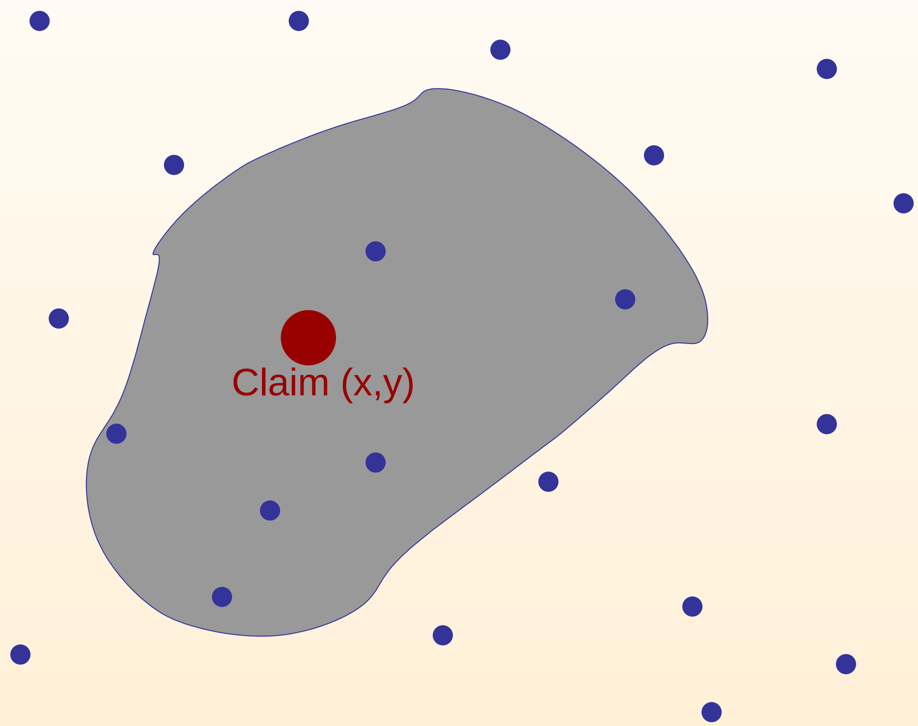
Similarities

- Generate a likelihood of where a particular mote is.

Key Differences

- Non-cooperating claimant
  - Don't need to follow protocols
  - i.e., data may not make sense
- Unknown hardware abilities [within security model]
- Localization: ignore spurious readings
- Spurious readings may be our only hints regarding anamolous behavior
  - less tolerant of false-positives and false-negatives

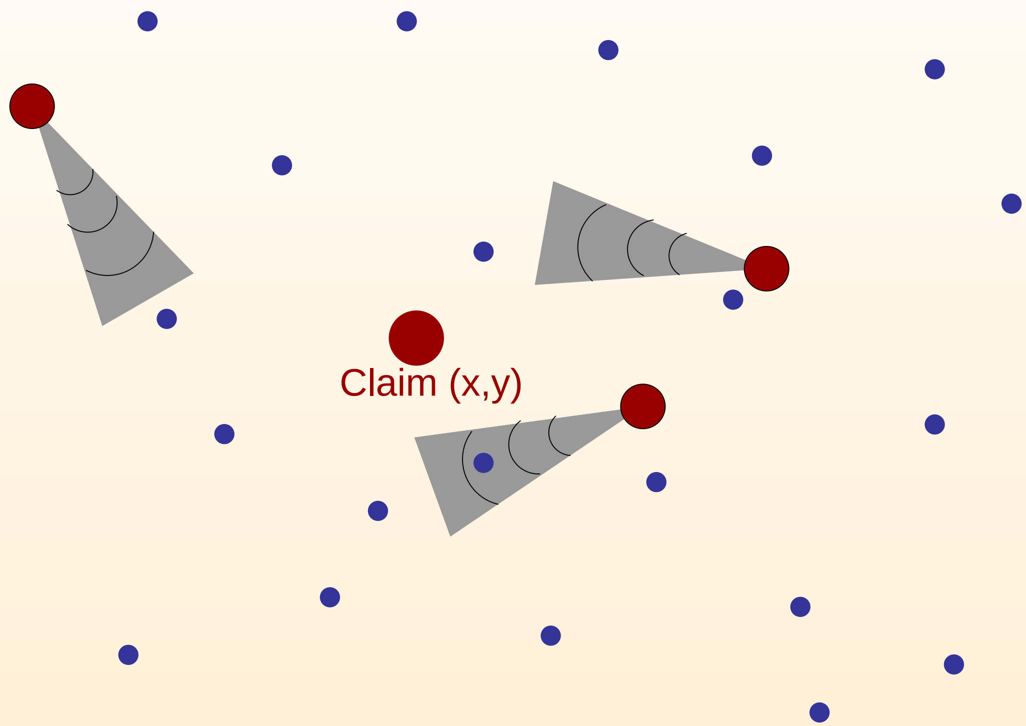
A Potential Solution I (beacon send)



The adversary acts as a beacon

- The field tries to corroborate the adversaries location
  - ▷ If claim correct, expect a falloff from the claimed location
  - ▷ Can check falloff; nearby nodes should ’hear loudly’, far nodes should hear quietly

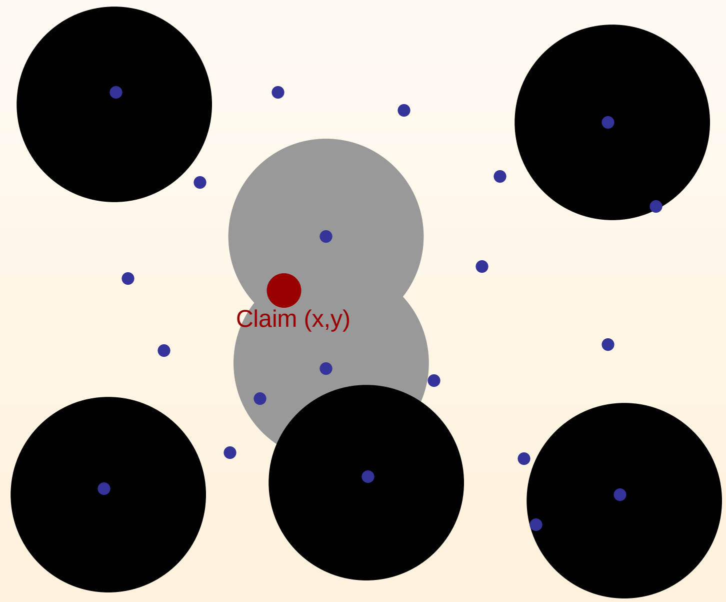
A Potential Solution I (Cont: beacon send)



How an adversary could thwart the scheme

- Place transmitters and broadcast to each node so that they hear what they expect to hear
- More nodes $\longrightarrow$ harder to fool

A Potential Solution II (adversary recv + occlude)



Alternatitively, can have the adversary listen to a signal and report it back to us

Use the rest of the network to shield signal – harder to heard outside of claimed area.

- Banking on their sensing ability to be not-very sensitive
- Harder to guarantee

Independence WRT localization media

Different localization techniques

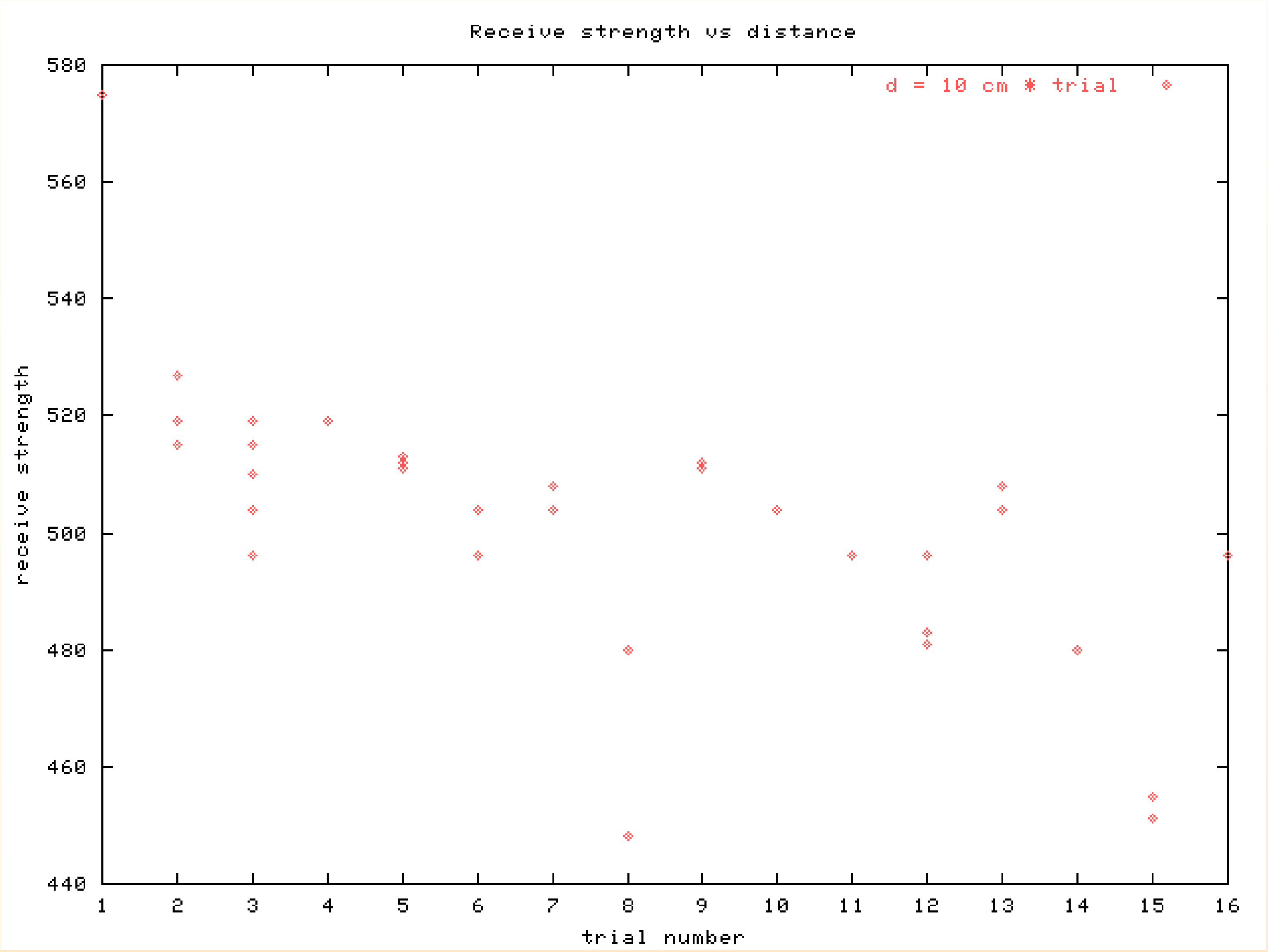
- Radio receive strength, nominally r^{-n}
- TOF [Kamin]: $\propto r$

Techniques which are more difficult to directionalize are better

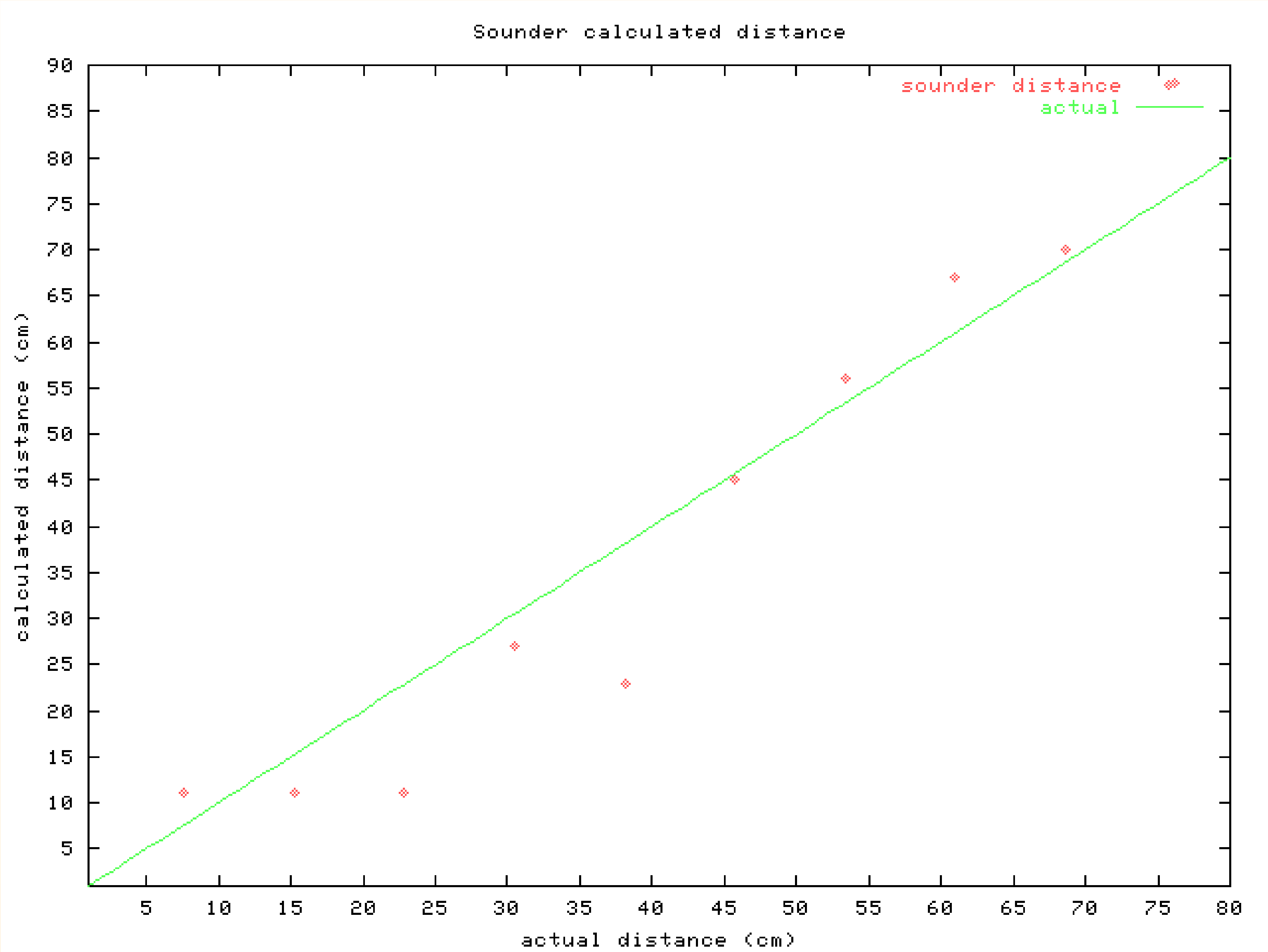
Problems and relation to threat model

- Each of the prior techniques can be spoofed in different ways

Preliminary Results: Recv strength plot



Preliminary Results: TOF Reading



Noise

Noise is the chief problem in dealing with real sensor networks

- Current sensors don't behave as an ideal model would indicate

With multipath effects [sound & rf], distance correlations hard to make as spurious readings are quite possible

Main technique recap:

- Correlate listener data
- Rely on physical properties to tell about propogation data
- Noise is an issue

Acknowledgements:

- Kamin: help with Matlab / motes / localization
- TinyOS folks