Securing Geographic Routing in Wireless Sensor Networks

KD Kang, Ke Liu, Nael Abu-Ghazaleh

kang@cs.binghamton.edu

Computer Science Dept.

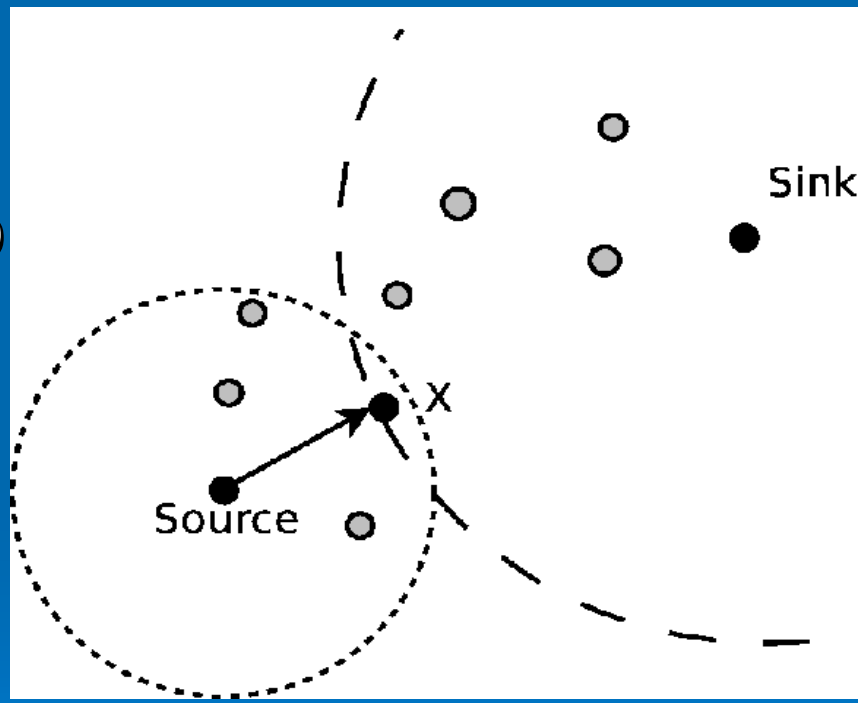
State University of New York at Binghamton

Outline

- Background: Geographic Routing
- Security Threats and Threat Model
- Localization and Location Verification
- Flooding Attack Prevention via Rate Control & Scheduling
- Secure Trust-based Multi-path Routing
- Conclusions

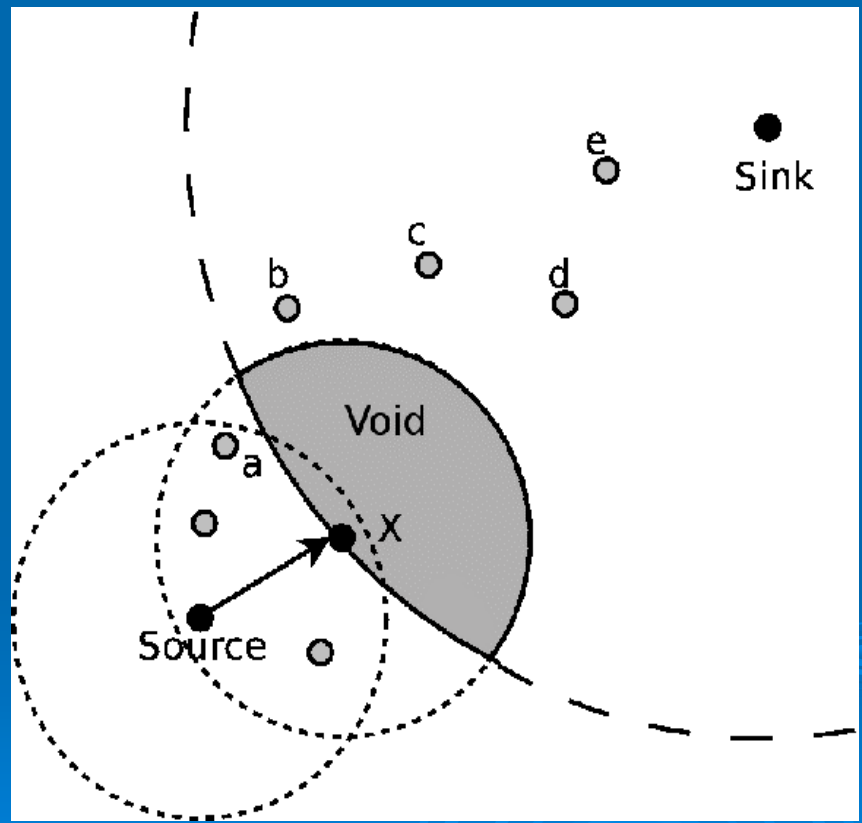
Geographic Routing

- Keep track of neighbors location
- Forwarding set is set of neighbors closer to destination than self
- Pick next hop as a member of the forwarding set
- Greedy forwarding – pick closest to destination



Geographical Routing (2)

- Local interactions only – no local state maintained
- Can get stuck in voids; void traversal algorithm needed (e.g., perimeter routing)



Assumptions

- Two types of nodes:
  - Anchors:
    - Know their location (e.g., using GPS)
    - Act as reference points for localization
    - Sufficient density to enable localization
    - First assume they are trusted; later relax the assumption
  - Sensor Nodes:
    - Can be compromised
    - Key pre-distribution to provide cryptographic keys
      - Confidentiality, authentication, message integrity, can be supported if needed

Threat Models

- We do not consider MAC/physical level attacks
  - Orthogonal techniques apply there
- Sybil attack (node claiming multiple locations) are possible
- Flooding, blackhole, wormhole, and selective forwarding attacks are possible

Location Verification

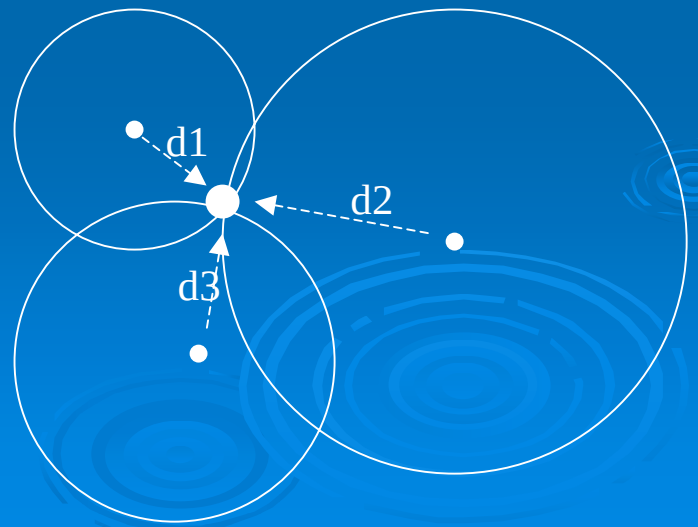
- Our Previous Work: ACM Q2SWinet 2005
- Each node is responsible for reporting its location information
  - Trusted to provide the correct information
  - No mechanism to verify using traditional localization approaches
- If nodes can falsify their location GR fails
  - Sybil attacks, blackholes, and other attacks easily possible
- Location Verification: Prevent nodes from lying about their location

Localization via Triangulation

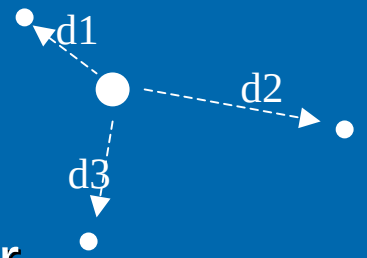
Lateration is the calculation of position information based on distance measurements from three known points (anchors)

- 2D position requires three distance measurements.
- Signal Strength, Time of Arrival, Time Difference of Arrival, etc.. used to estimate distance
- Triangulation measures angle

of arrival



Key Idea for Location Verification – Anchors Localize

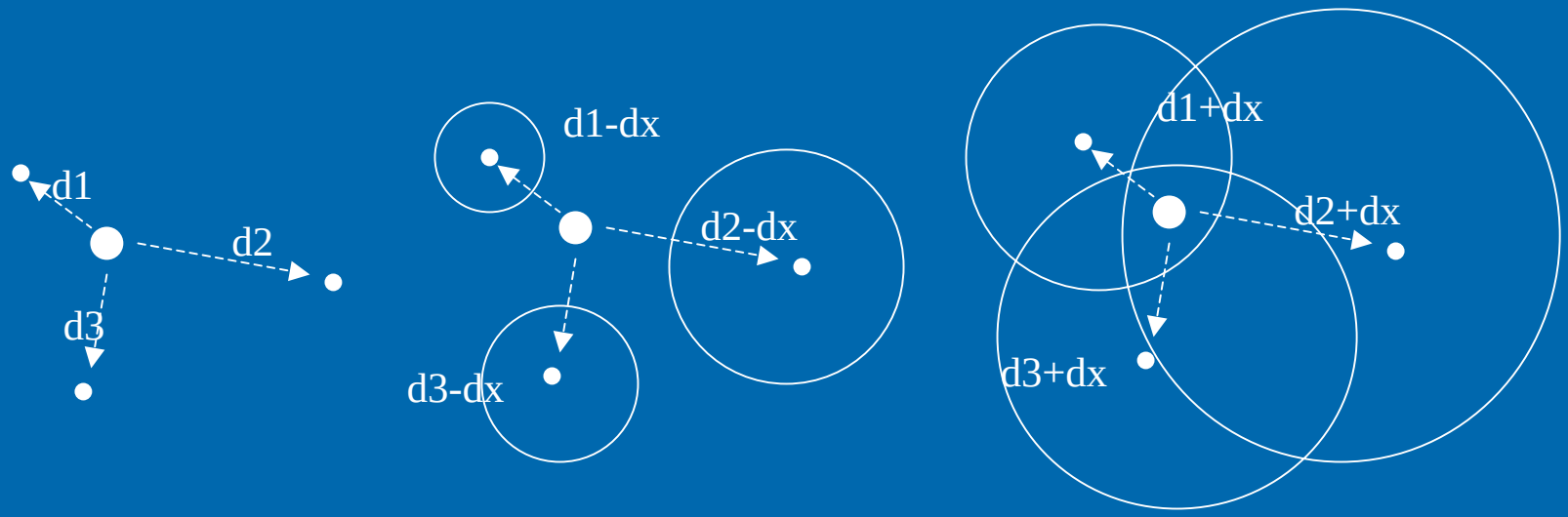


- Protocol
  1. Node transmits localization packet
  2. Anchors receive it concurrently; each anchor estimates distance to node
  3. Anchors exchange estimates to calculate location
- Localization responsibility moved to trusted anchors
- Location passed to node with certificate or supplied by anchors
- Limitation: range based localization – range free localization requires extension

Possible Attacks (1)

- Nodes cheat by manipulating the localization transmission
  - E.g., in signal power based ranging
    - Transmit at a higher power to appear closer
    - Lower power to appear farther
  - In TDOA
    - Send ultrasonic pulse before RF pulse to appear closer
    - Send RF pulse before ultrasonic to appear further
    - Use a random nonce

Defense



- Key observation: Node will appear closer to, or further, from all anchors concurrently
- Detectable when anchors exchange ranges
  - Leads to Non-feasible location in all non-trivial anchor placements

Possible Attacks (2)

- Directional antenna version of previous attack
  - Use directional antenna to send different localization beacons to each anchor
    - Other anchors cannot hear the directional packet
    - Falsifying distance to each anchor separately can allow undetectable (consistent) forgery
- Two versions:
  - Sequential: attacker sends the beacons sequentially to the different anchors
  - Concurrent: attacker has multiple radios and can concurrently forge distances

Defense

- Sequential version can be defended by having anchors be loosely synchronized
  - Can detect the different time stamps on the packets received by the different anchors
- Concurrent version challenging
  - A sophisticated attacker with expensive H/W
  - MAC level authentication?
  - Moving anchors?
  - Other sensors detecting inconsistency?

Secure Routing

- Defense against Flooding Attacks
- Trust-based Multipath Routing

Flooding Attacks

- Malicious nodes can flood neighbors
- Serious problem if receiving nodes blindly forwards the received packets to their neighbors
- Cannot be prevented via cryptographic methods

Defense against Flooding Attacks

- Base station disseminates queries, e.g., report temperature measured in area (x1, y1, x2, y2) at every second for 10 minutes
  - Queries can be disseminated via authenticated broadcast, e.g., uTESLA
- Derive the expected data incoming rate based on the received queries
  - Basis of defense

Defense against Flooding Attacks

- Assign low priority to the packets from a suspicious neighbor
  - Transmit packets from well-behaving nodes first
  - Drop excessive packets from suspicious nodes
- Use a packet from a suspicious node to explore the trustworthiness of a neighbor
  - Forward to one random node in the FS
  - Proactively build trust information for future routing by overhearing

Forwarding Misbehavior

- Misbehaving nodes can misdirect or selectively forward packets
- Since GR is completely localized, problem is difficult to detect
  - A node has no idea where the packet should be sent beyond its current next hop

Proposed Solution

- Multi-path routing:
  - Select next hop probabilistically among forwarding set
    - Probability proportional to *trust (aka reputation)*
- Trust estimate is adapted over time
  - Based on observed behavior of the nodes
- How to detect misbehavior?

Detecting Misbehavior/Updating Trust

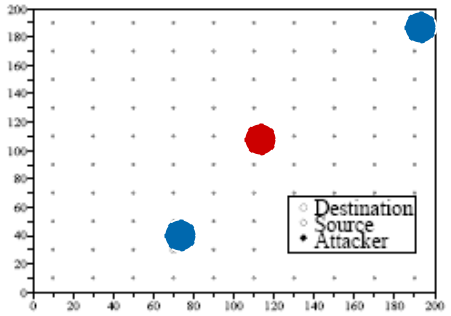
- Trust updated up or down depending on observed behavior of neighbors
- Rebroadcast check
  - A sending node hears if the next hop forwards it again
    - Drop reputation if not
  - Not fool proof
    - Can miss rebroadcast due to collision or fading
    - Next hop can pretend to forward the packet to a non-existing next hop neighbor
      - Securely building 2-hop neighbor cliques can help
- Trust consensus
  - Exchange trust estimates with neighbors among neighbors that are trustworthy

Simulation

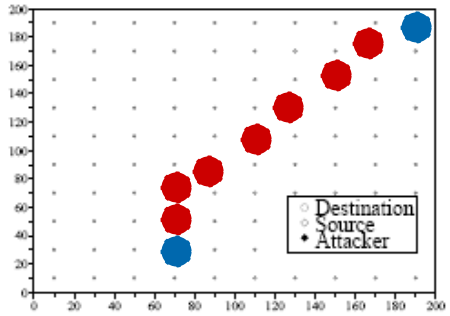
- Implemented secure GPSR in ns-2
- Basic simulation parameters

Radio Range	30 m
Bandwidth	2Mbps
Data Payload	64B
Packet Size	158B
Data Rate	2 packets/s
Queue Length	100 packets
Hello Period	5 s
Traffic duration	200 s
T_i initial value	0.5
Δt	0.1
Transmit Power	0.5 Watt
Receiving Power	0.2 Watt

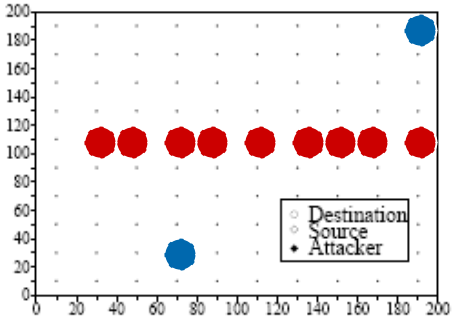
Attack Scenarios



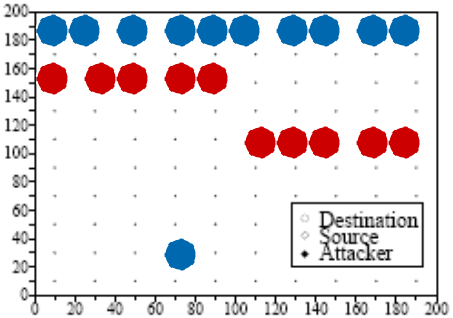
(a) Scenario 1



(b) Scenario 2

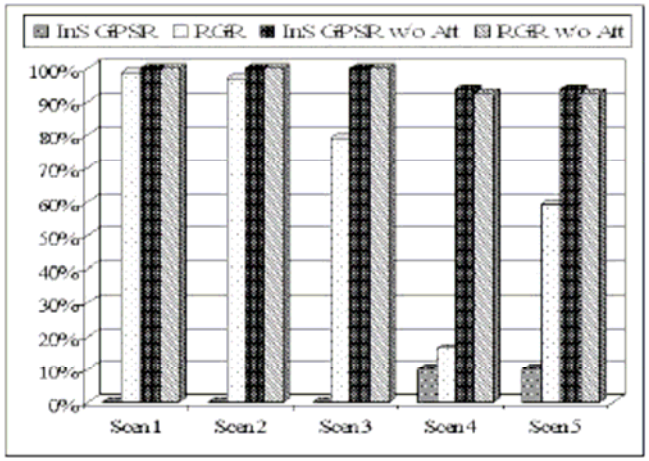


(c) Scenario 3

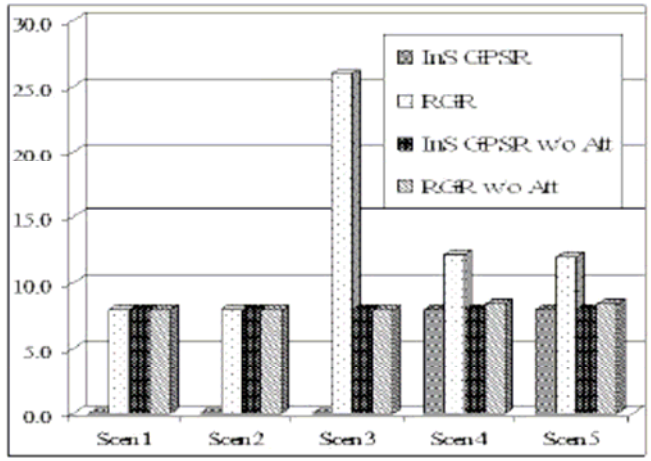


(d) Scenarios 4 and 5

Experimental Results



(a) Delivery Ratio



(b) Path Length of the Received Packets

Summary

- Sybil, blackhole and wormhole attacks require location falsification in GF
  - Prevented using location verification mechanism
- Forwarding misbehavior does not depend on location falsification
  - Rate control & packet scheduling to alleviate flooding attacks
  - Multi-path routing helps avoid bad paths even when misbehaving nodes are not known
  - Building and tracking reputation helps ostracize misbehaving nodes

Future/Ongoing Work

- Extend to range-free localization
- More research on trust-based routing
- Virtual Coordinate routing
  - Initialize node coordinates and use them as identifiers and for routing
  - Similar to GR, but some unique and more difficult attacks
- Explore interaction with localization errors

Thank you!
Any questions?