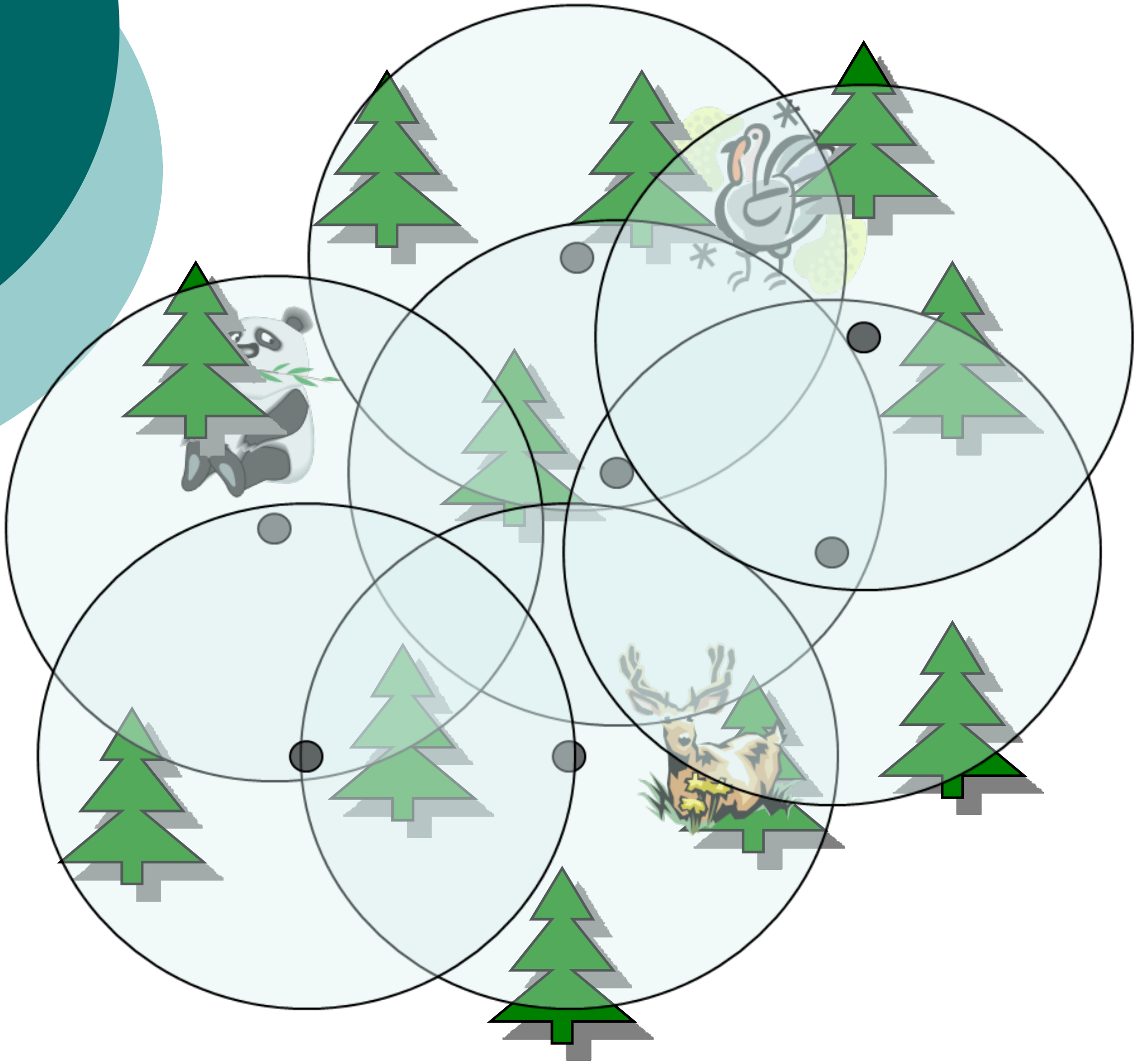
Mitigating Attacks against Virtual Coordinate Based Routing in Wireless Sensor Networks

Jing Dong, Kurt Ackermann, Brett Bavar,
Cristina Nita-Rotaru
Department of Computer Science and CERIAS
Purdue University

Wireless Sensor Networks



Data collection

Object detection & tracking

Multi-dimensional queries

Data centric storage

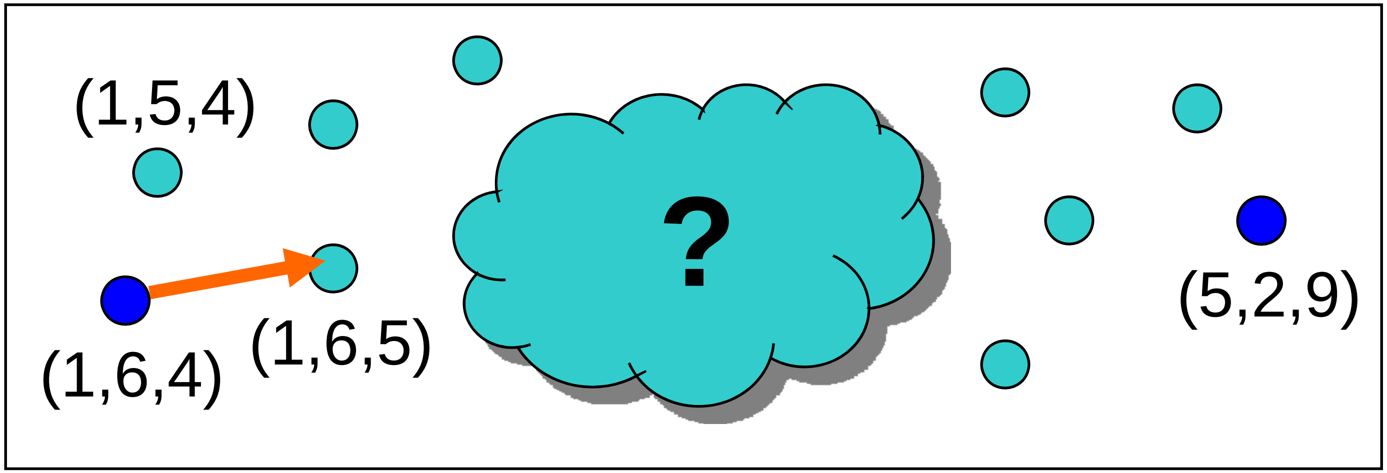
Task scheduling & coordination

Point-to-Point Communication

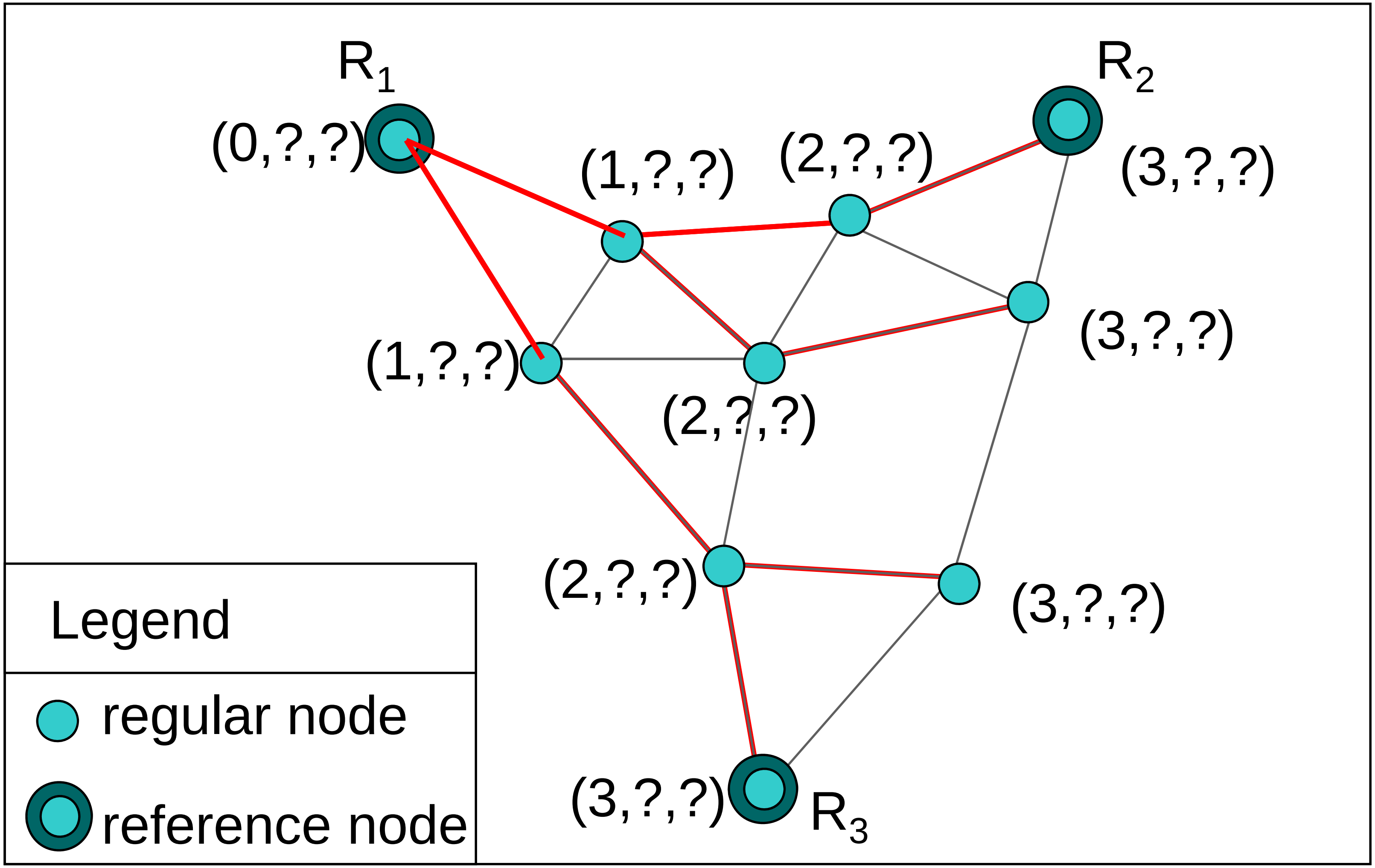
- New applications require point-to-point routing
  - Highly scalable
  - Low overhead
  - Robust
- Geographical routing based on physical coordinates
  - Each node only needs to know the coordinates of neighboring nodes and the destination
  - Greedy routing to the neighbor that is closest to destination

Virtual Coordinate-Based Routing

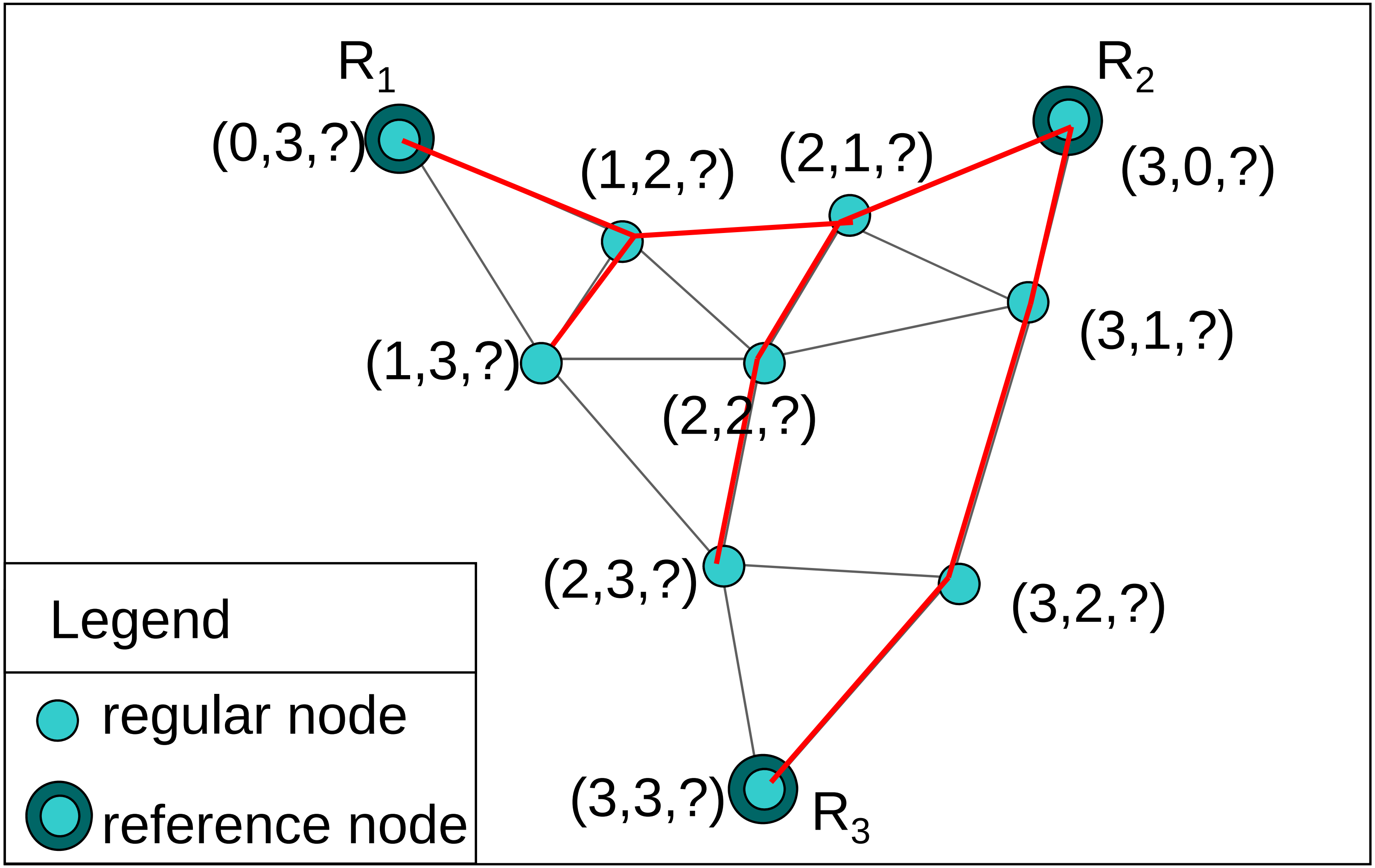
- Establish node coordinates
- *Reference nodes* store coordinates
- Obtain destination coordinates
- Greedy routing towards destination
- Fall-back procedure to address local minima



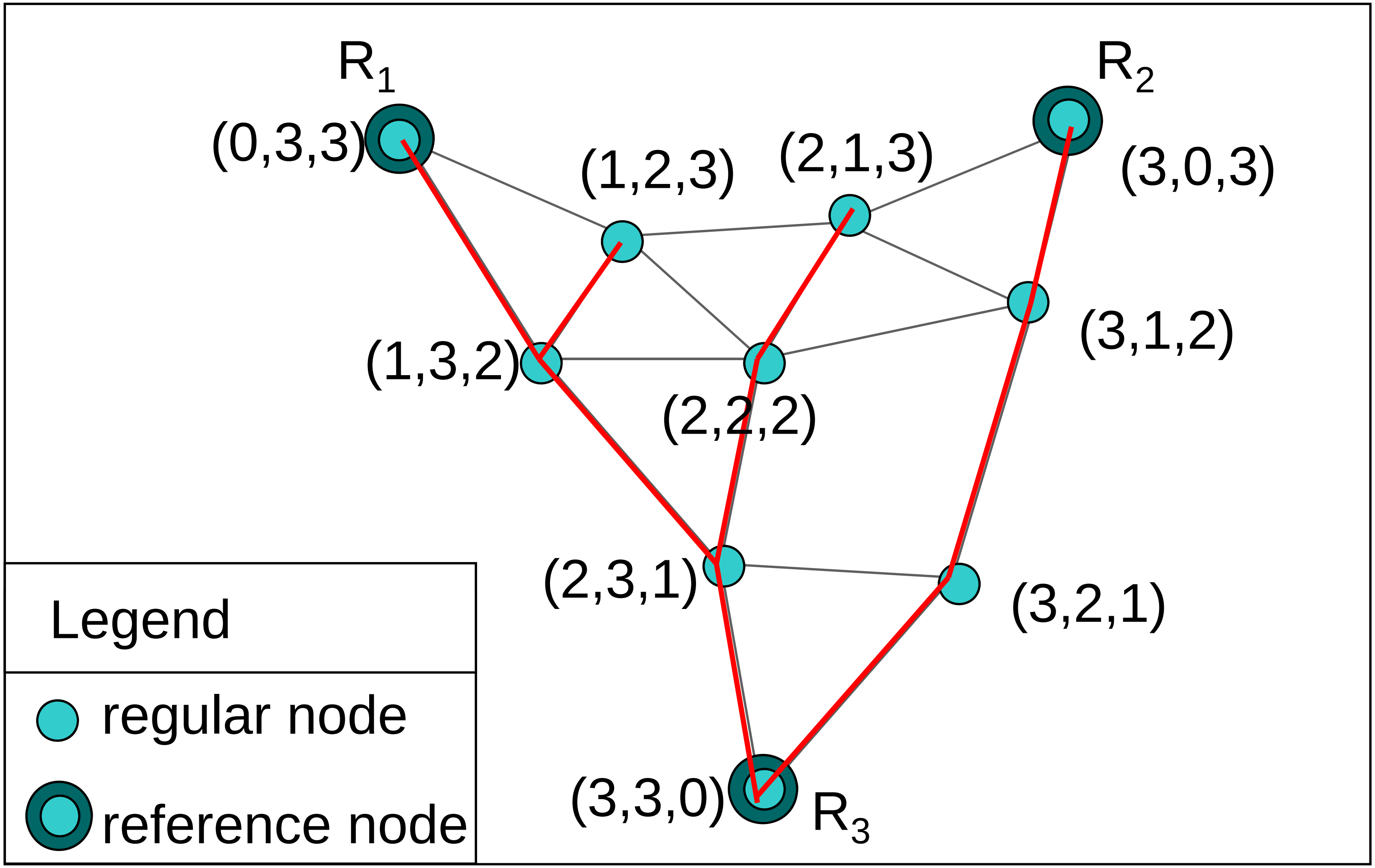
Virtual Coordinate Establishment



Virtual Coordinate Establishment



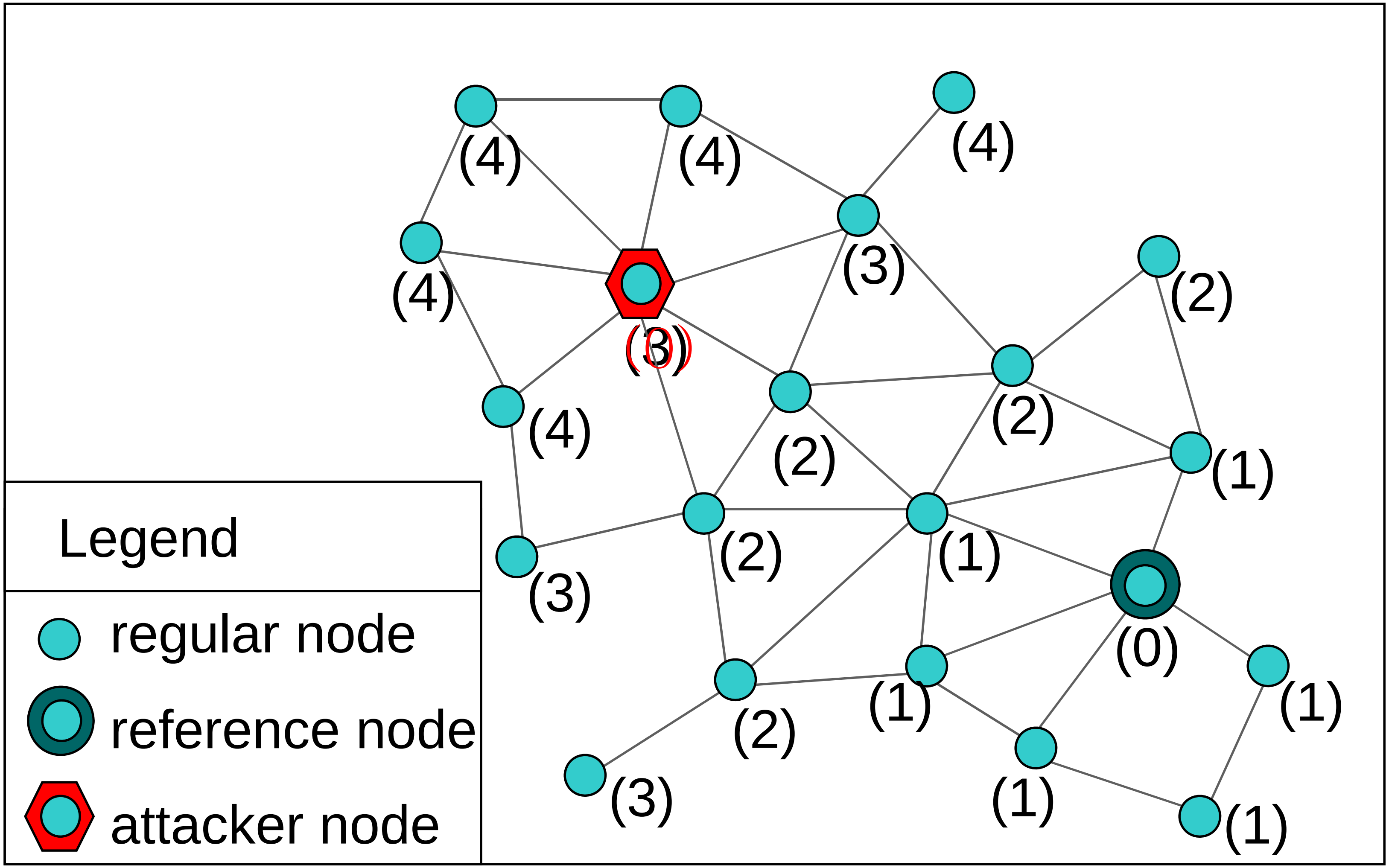
Virtual Coordinate Establishment



Attacks against VC Establishment

- Goal: generate incorrect or unstable coordinates
- Impact on routing: route failures, invocation of expensive fall-back procedure
- Attacks classified as
  - Coordinate deflation
  - Coordinate inflation
  - Coordinate oscillation
- Ways to mount the attacks
  - Reporting false coordinates to neighbors
  - Replaying legitimate coordinates in distant regions of network (wormhole attack)

Coordinate Deflation



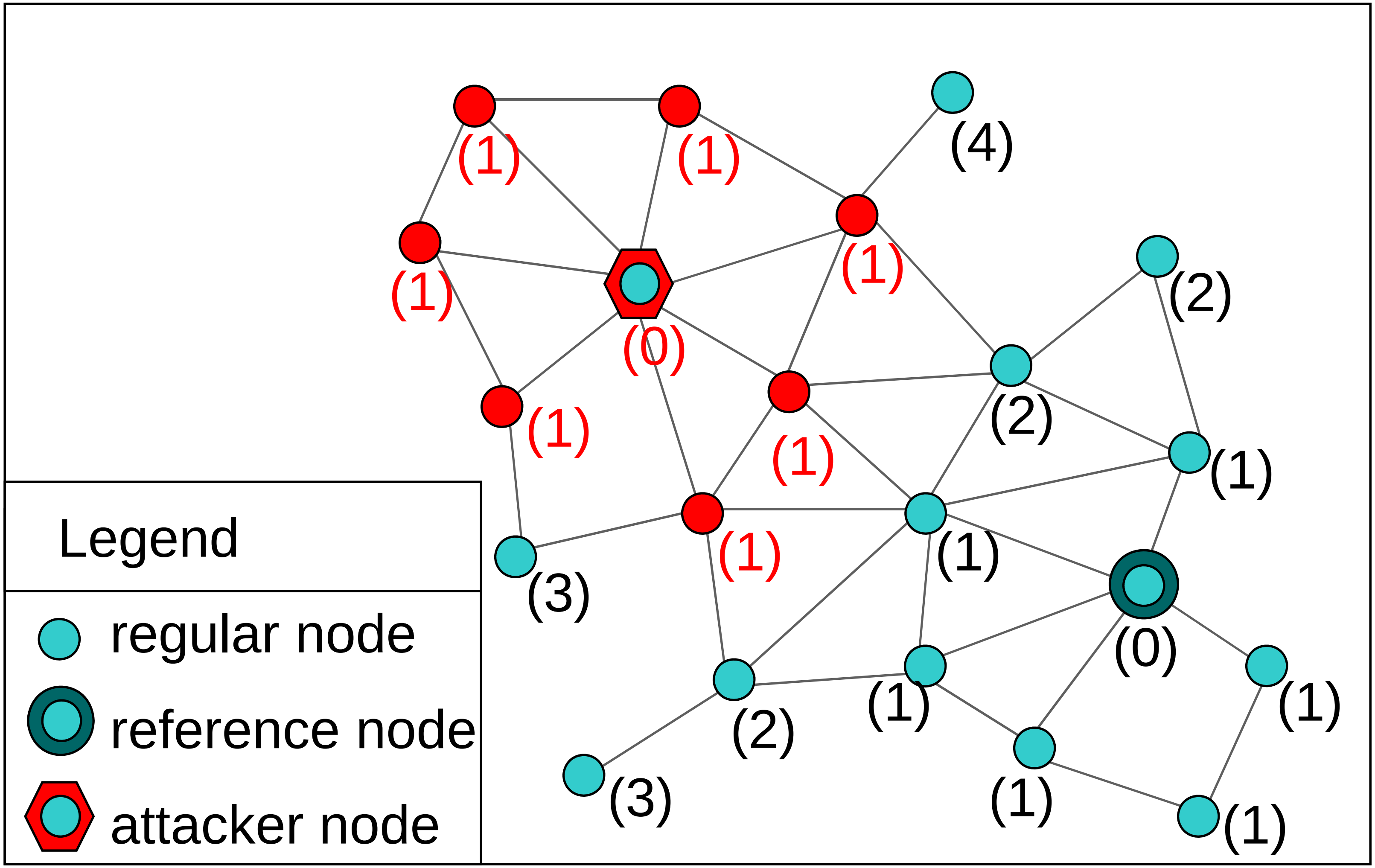
Legend

● regular node

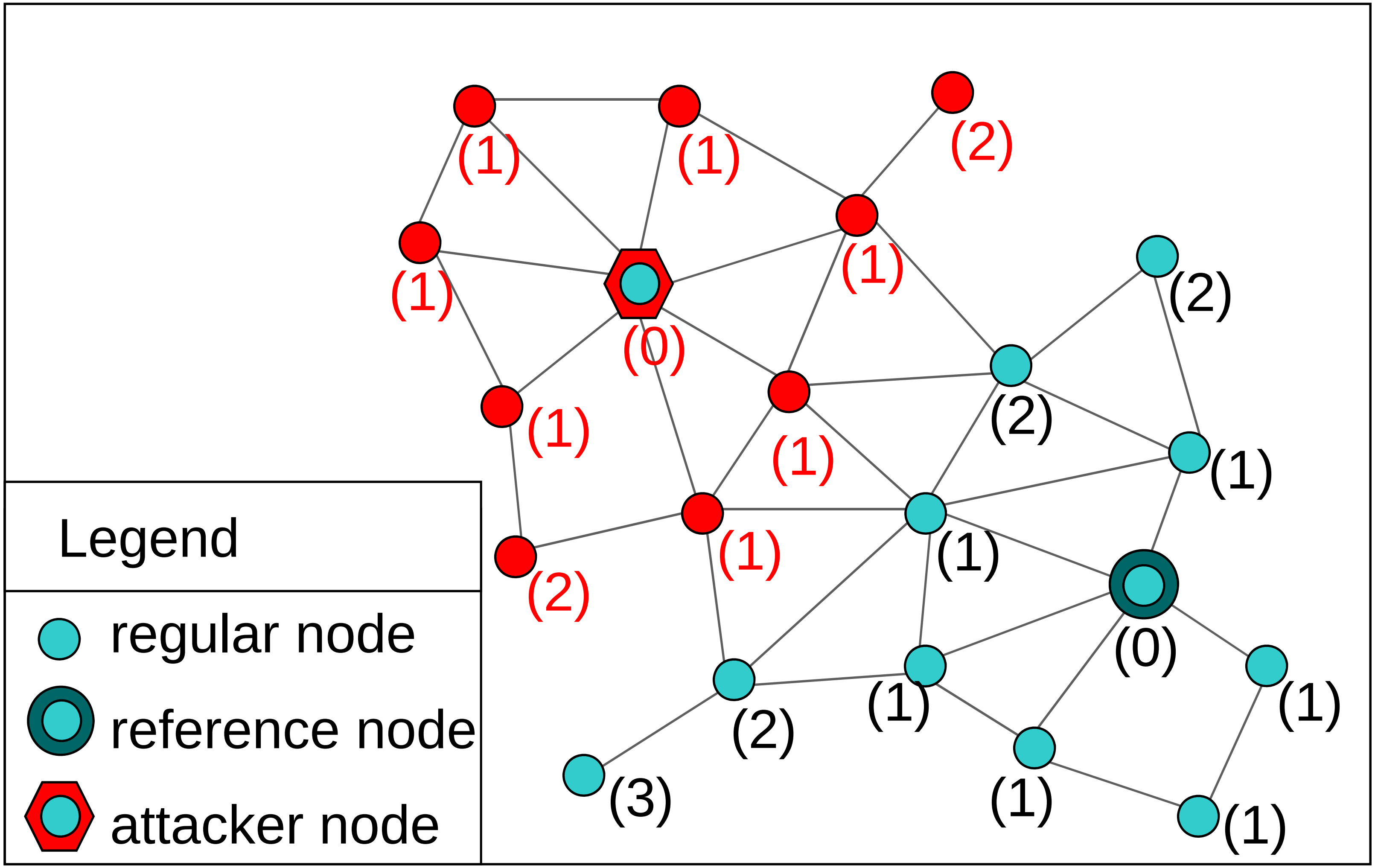
◎ reference node

⬣ attacker node

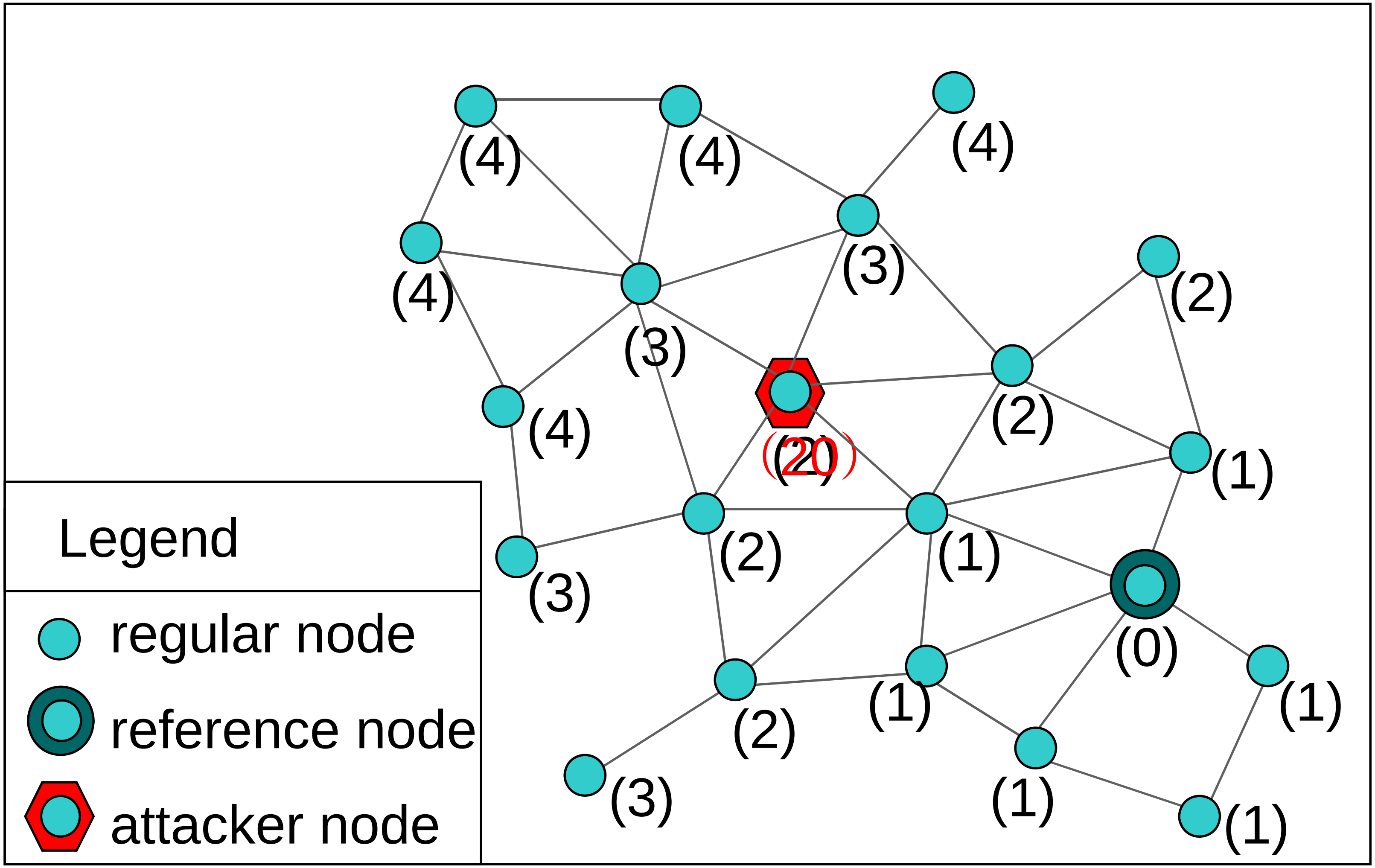
Coordinate Deflation



Coordinate Deflation



Coordinate Inflation



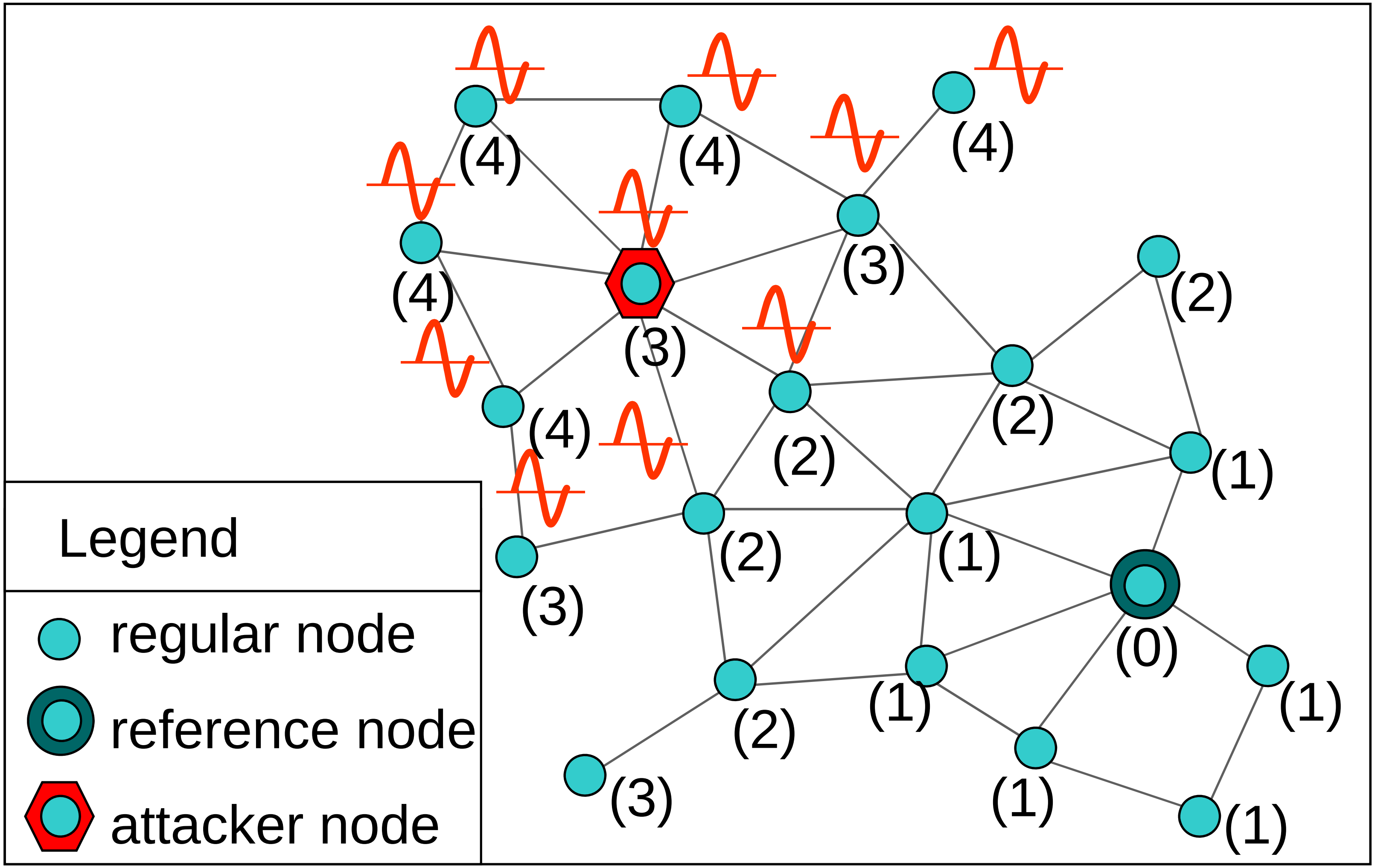
Legend

● regular node

◉ reference node

⬣ attacker node

Coordinate Oscillation



Legend

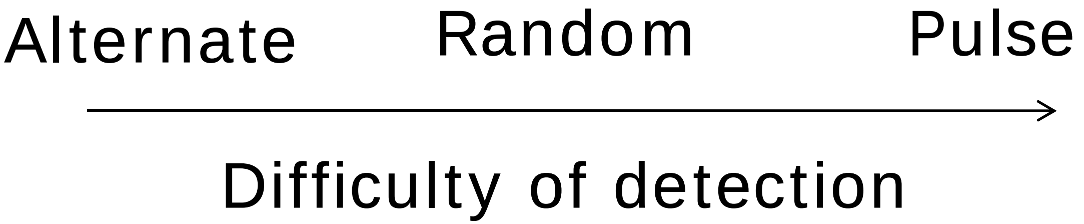
● regular node

◉ reference node

⬢ attacker node

Coordinate Oscillation Strategies

- **Alternate**: Alternate coordinates between max and min
- **Random**: Select coordinate randomly from the correct range
- **Pulse**: Oscillate coordinate once at exponentially distributed interval



Alternate Random Pulse

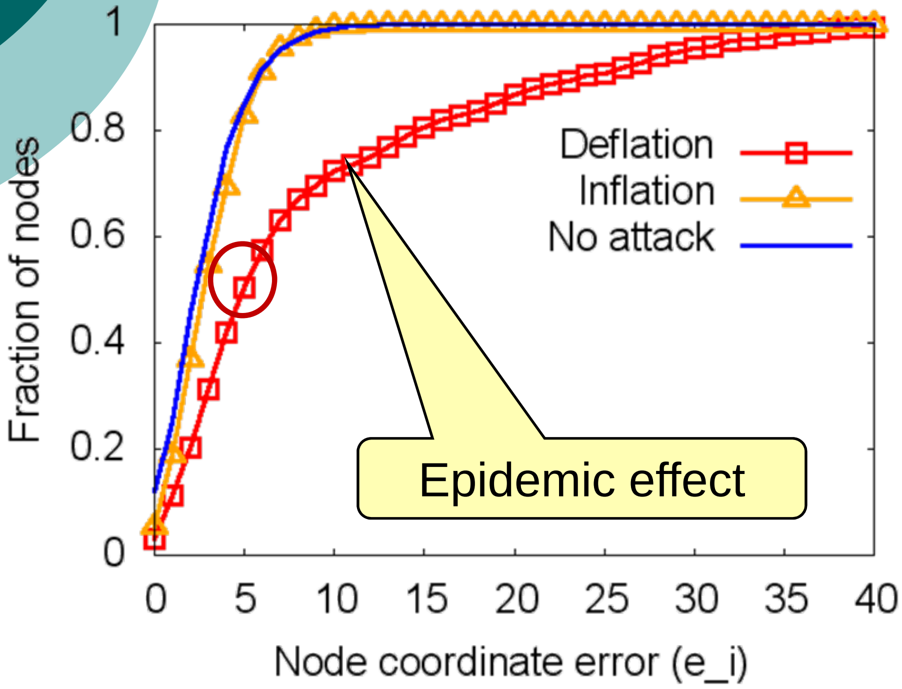
Difficulty of detection

Experiment Setup

- TOSSIM simulator and Beacon Vector Routing (BVR) [Fonseca 05] protocol
- 100 nodes, 8 reference nodes
- Attacker nodes randomly selected
  - Deflation: attackers advertise 0 for max impact
  - Inflation: attackers advertise 20 for max impact
  - Oscillation: alternate, random, and pulse scenarios
- Results are averaged over 10 runs

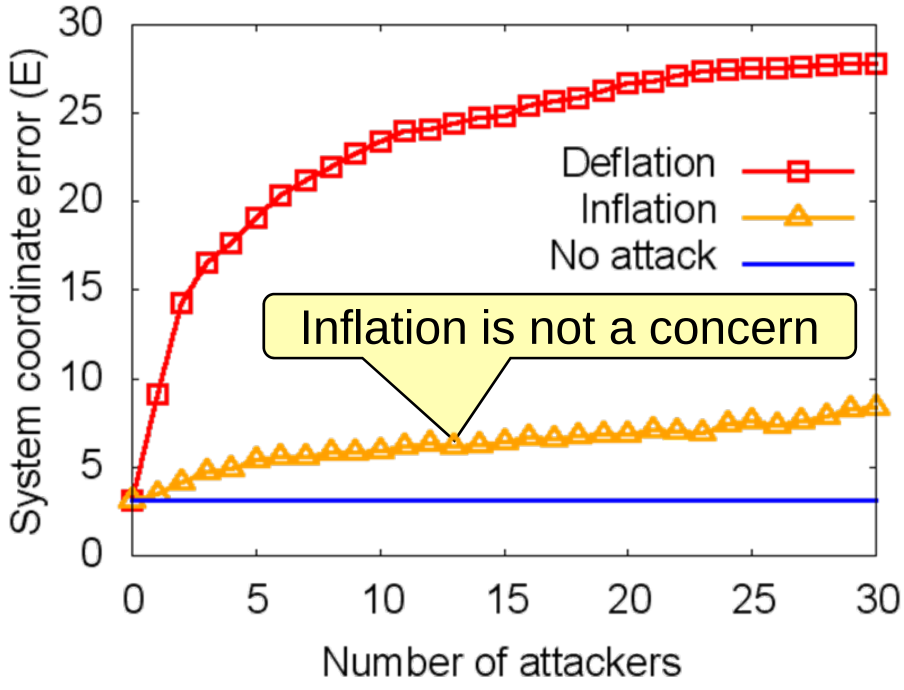
Impact on Virtual Coordinates

One single attacker



Epidemic effect

Number of attackers

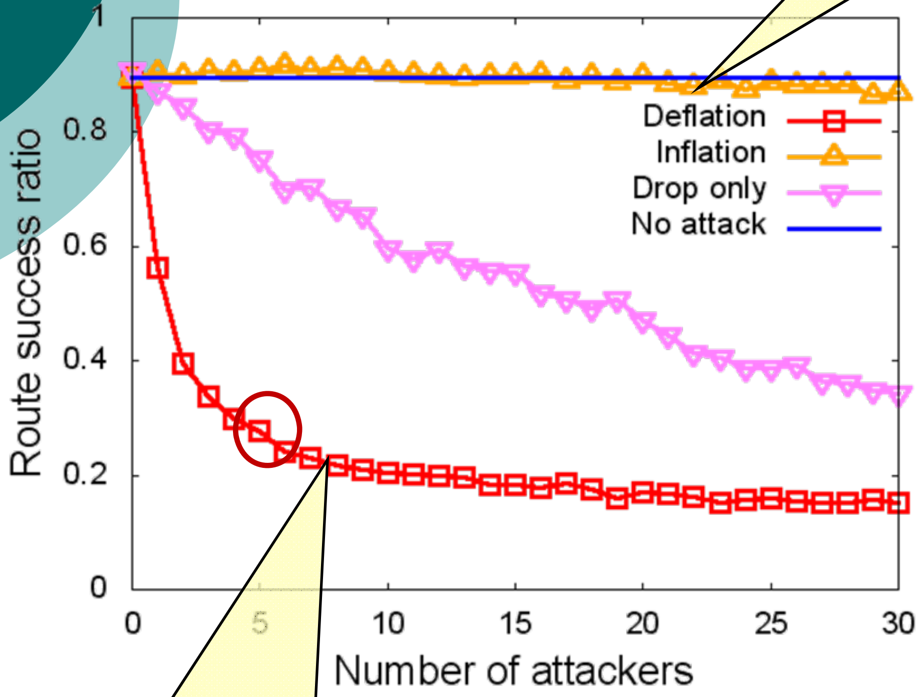


Inflation is not a concern

Impact on Routing

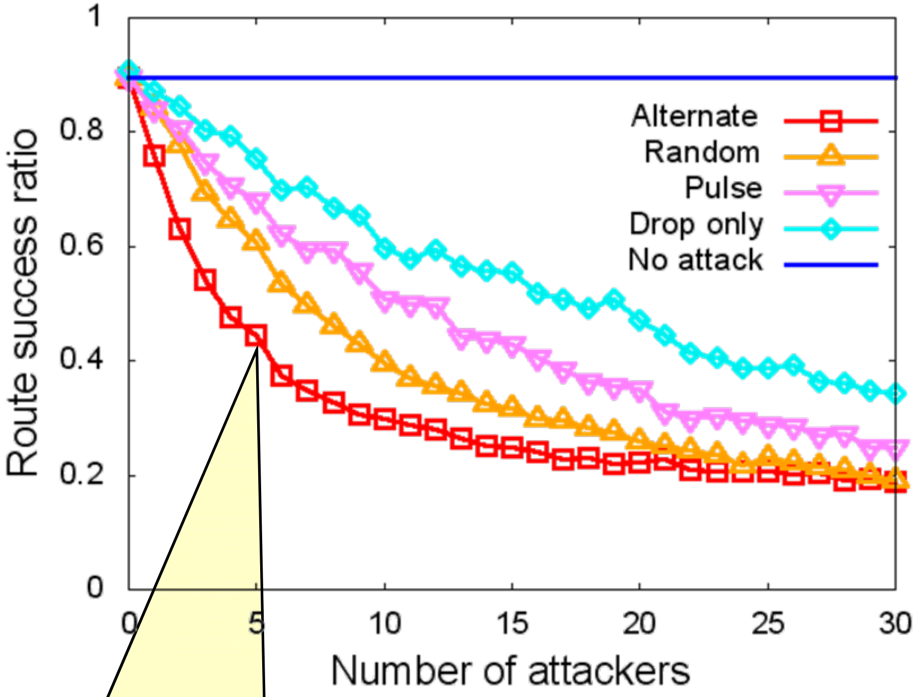
Deflation and Inflation

Inflation is not effective



Deflation is a very effective attack

Oscillation



Oscillations are dangerous

Defense for Virtual Coordinate Systems

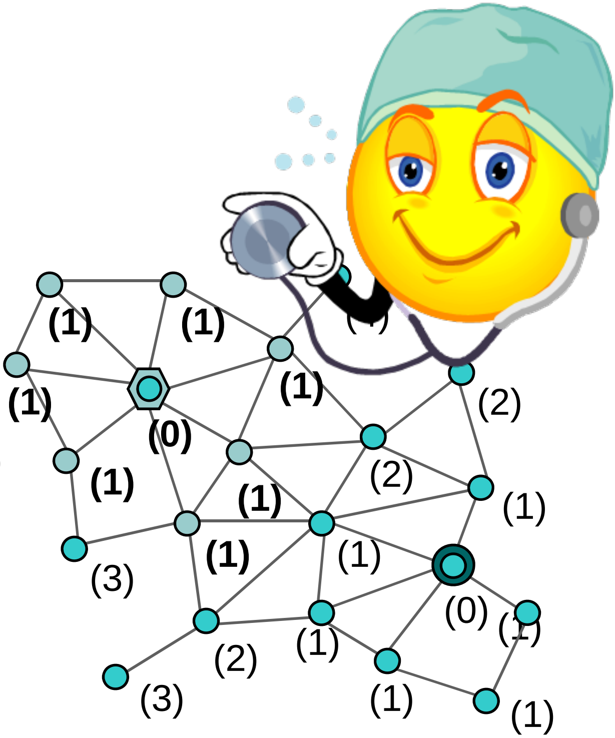
- We focus on deflation and oscillation attacks
- Assume reference nodes are trusted
- Coordinate deflation attack
  - Detecting attack with statistical test
  - Preventing attack from non-colluding attackers with hop-count authentication
- Coordinate oscillation attack
  - Stability-based parent selection

Detecting Coordinate Deflation with Statistical Test

- Observation
  - Deflation attack causes global hop count decrease in the network
- Approach
  - Use changes in a small subset of nodes to extrapolate global coordinate change with statistical test
- Implementation
  - Statistical test run by reference nodes on the set of coordinates maintained locally

Attack Detection Procedure

- Initialize
  - Record reference hop counts when no attack
- Detect
  - Compare the current stored hop count to the reference hop counts with *Wilcoxon signed rank test*
- Result
  - If test detects change, report attack detected



Benefits of Statistical Test

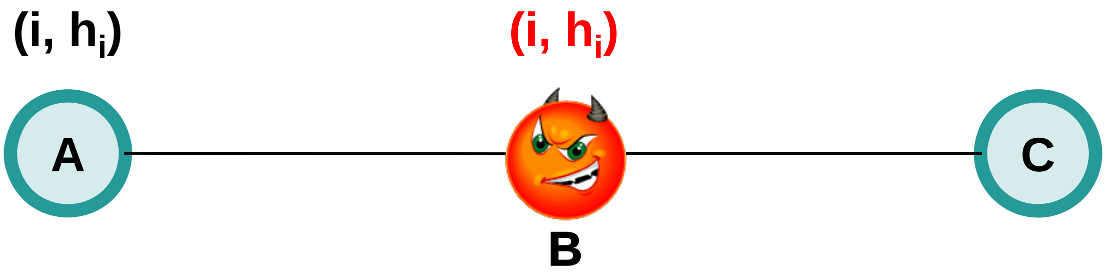
- Wilcoxon Signed-Rank Test
  - Requires small sample set
  - Uses paired measurements
  - No assumption on underlying distribution
- Uses readily available coordinates stored in reference nodes, thus zero communication overhead
- Low computation overhead

Defense for Virtual Coordinate Systems

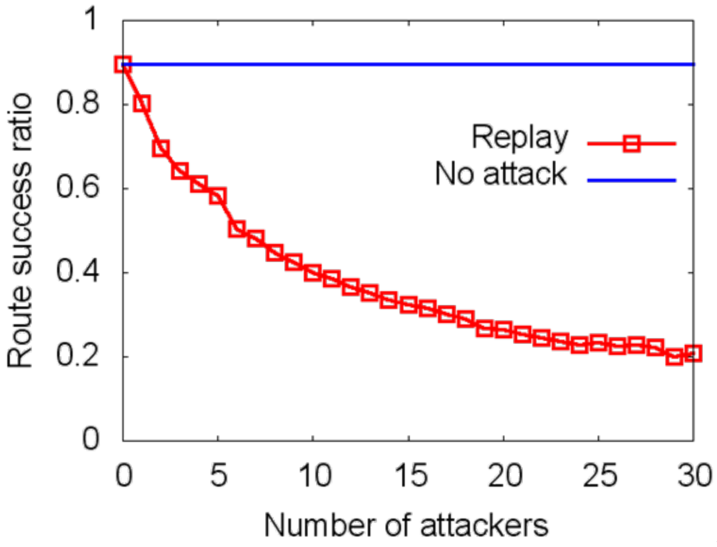
- Coordinate deflation attack
  - Detecting attack with statistical test
  - Preventing attack from non-colluding attackers with hop-count authentication
- Coordinate oscillation attack
  - Stability-based parent selection

Prevent Deflation with One-way Hash Chain

- Basic idea: use one-way hash chains
- However, it is vulnerable to *replay attack*



- Two flavors of replay
  - Same-distance fraud
  - Transparent forwarding
- Dangerous due to epidemic effect



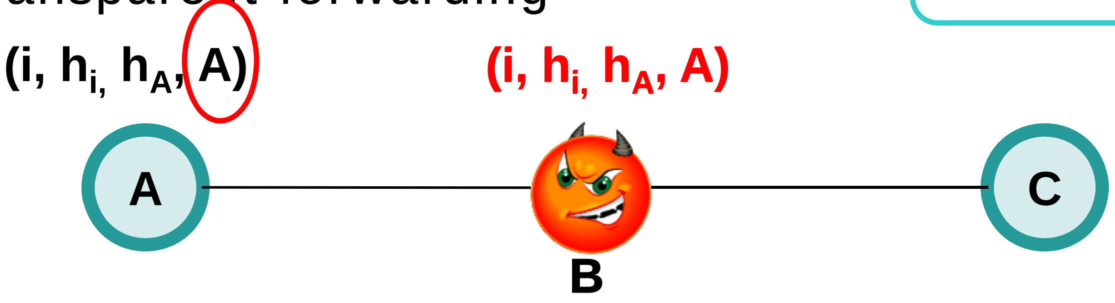
Hash Chain Replay Defense

- Approach
  - Bind the received hash value to the identity of the node
- The coordinate message for a node at hop count i is (i, h_i, h, id)
  - i, h_i are same as before
  - id is unique ID for the node
  - h = H(h_{i-1} || id), binds the received hash value to its id

Replay Detection and Response

$$h_{id} = H(h_{i-1}, id)$$

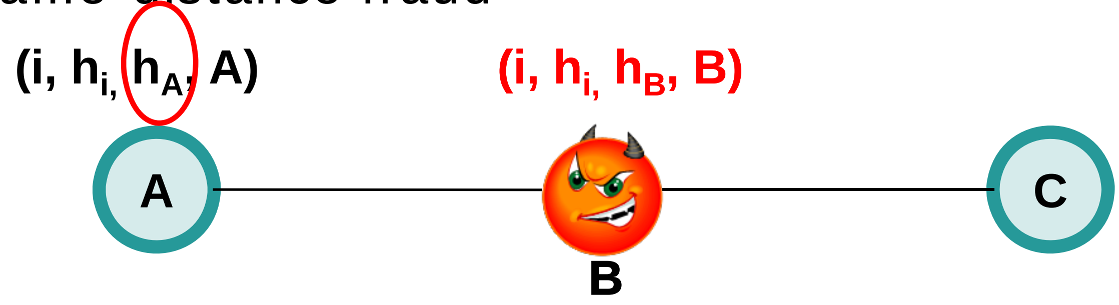
- Detection
  - Transparent forwarding



$(i, h_{i,} h_{A}, A)$

$(i, h_{i,} h_{A}, A)$

  - Same-distance fraud



$(i, h_{i,} h_{A}, A)$

$(i, h_{i,} h_{B}, B)$

- Response with self-sacrifice
  - Upstream node voluntarily inflates its coordinates

Defense for Virtual Coordinate Systems

- Coordinate deflation attack
  - Detecting attack with statistical test
  - Preventing attack from non-colluding attackers with hop-count authentication
- Coordinate oscillation attack
  - Stability-based parent selection

Mitigating Oscillation Attacks

- Challenges
  - Cannot simply ban oscillating nodes
    - Affected honest nodes also exhibit attacker-like behavior
  - Normal network variations also cause certain level coordination oscillation
- Design goals
  - Detect and isolate consistent attackers
  - Detect and isolate strategic attackers
  - Not implicate honest nodes affected by attack
  - Tolerate normal network variations

Robust Parent Selection

- Each node evaluates a coordinate volatility score for each of its neighbors
- Only neighbors with small enough volatility score can be potential parents
- Volatility score
  - Captures a nodes current behavior, historical behavior, and sudden changes in behavior

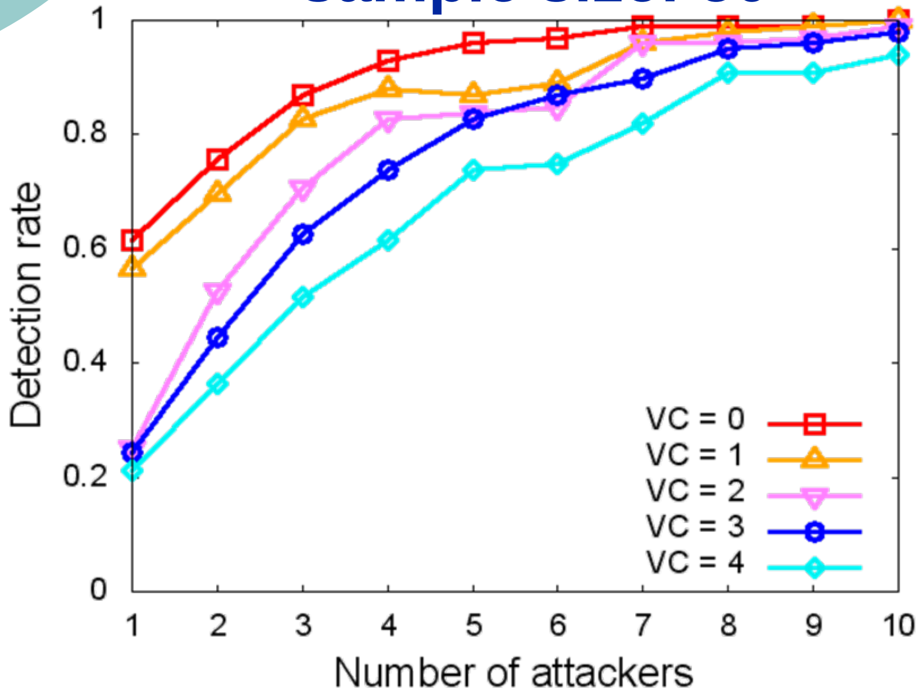
$$VS_t = \alpha v_t + \beta H_t + \gamma C_t$$

Detection of Deflation

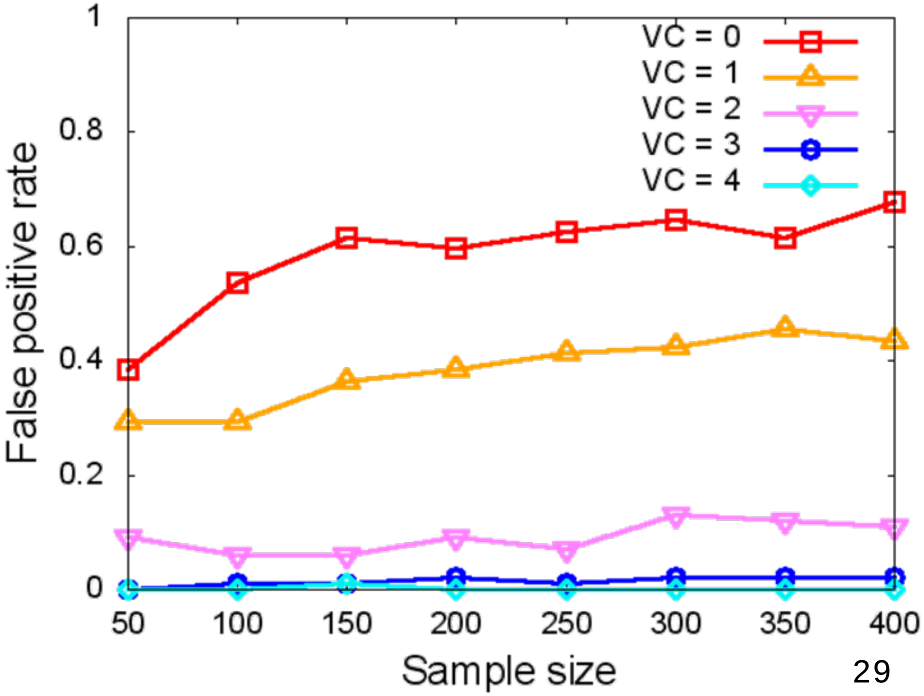
Variation Compensation (VC) accounts for normal network variations

Trade-offs: higher VC, lower false alarms, lower detection rate.

Detection rate with sample size: 50



False positive rate

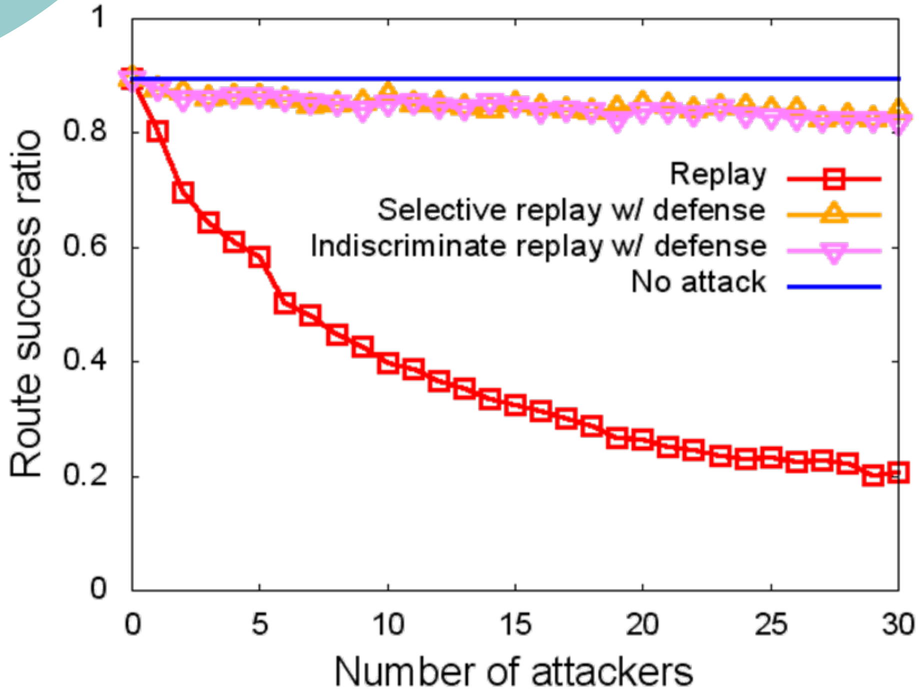


Hash Chain Replay Defense

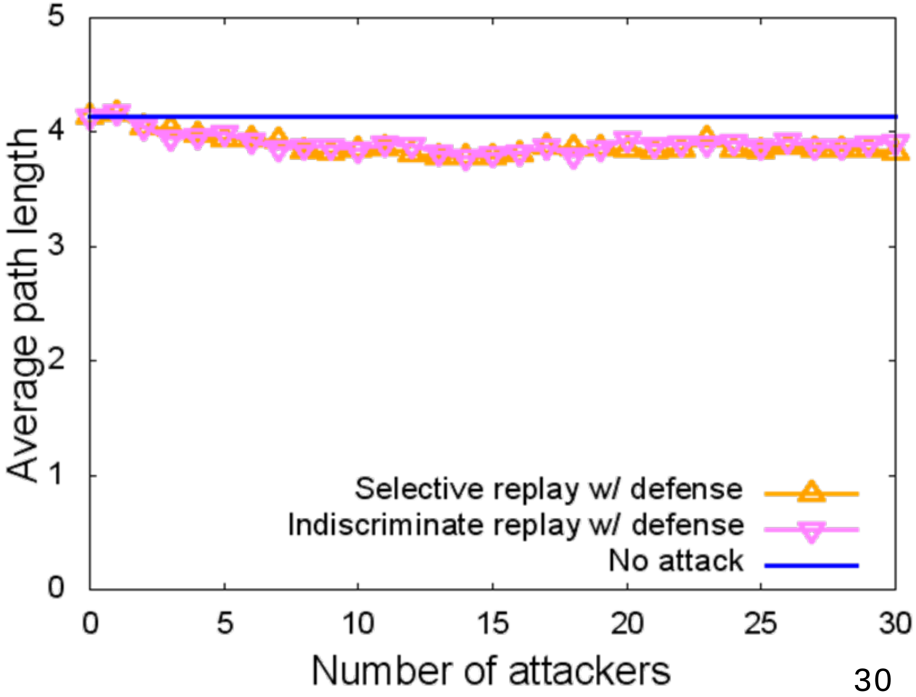
Selective replay: only replays smaller coordinates – common attack behavior

Indiscriminate replay: replays all overheard coordinates – attempts to cause many honest nodes to voluntarily raise their coordinate

Route Success Ratio

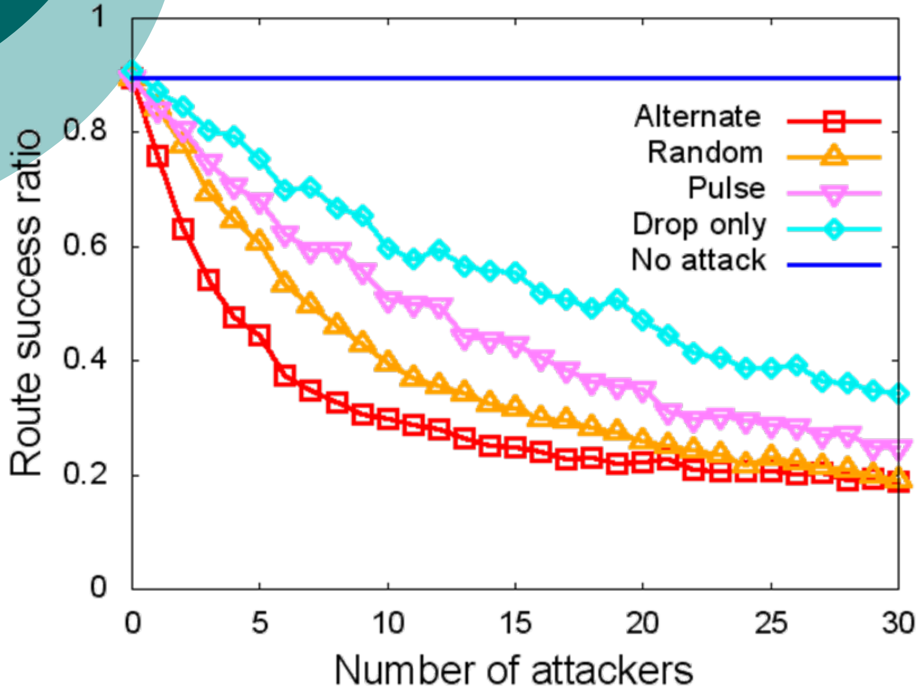


Route cost

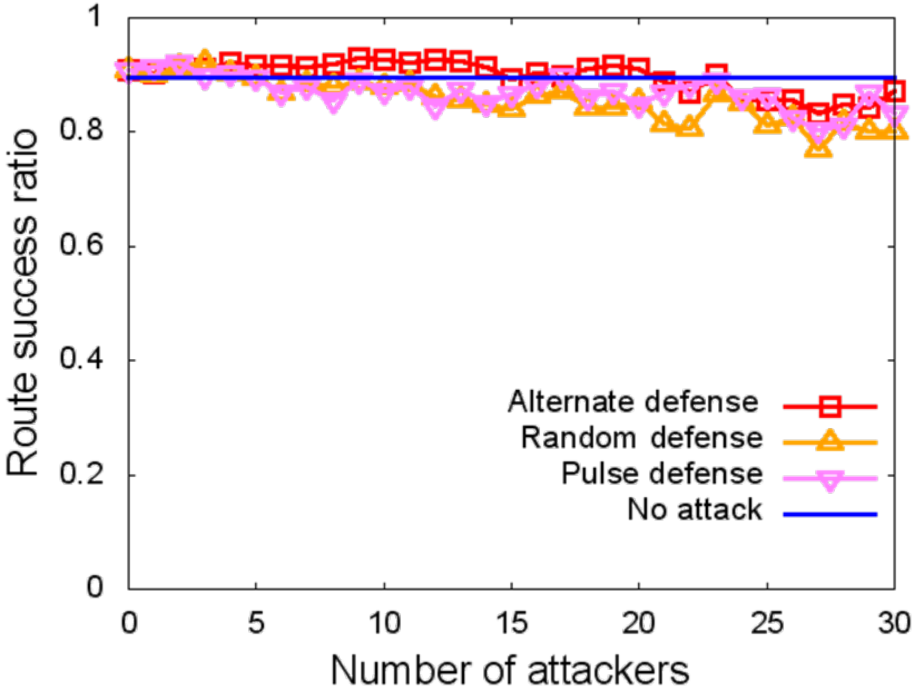


Oscillation Mitigation

No defense



Defense with stable parent selection



Summary

- We identified attacks against VCS in wireless sensor networks
  - Coordinate Deflation
  - Coordinate Inflation
  - Coordinate Oscillation
- We proposed efficient defense mechanisms
  - Wilcoxon test for deflation detection
  - One-way hash chain with replay defense
  - Stability-based parent selection
- We demonstrated the impact of the attacks and the effectiveness of the solutions

Thank You

Questions?

Contact: dongj@cs.purdue.edu