UNIVERSITY OF Waterloo

Randomly Directed Exploration
An Efficient Node Clone Detection Protocol in Wireless Sensor Networks

Zhijun Li and Guang Gong
University of Waterloo

Research Review Seminar
February 25, 2010

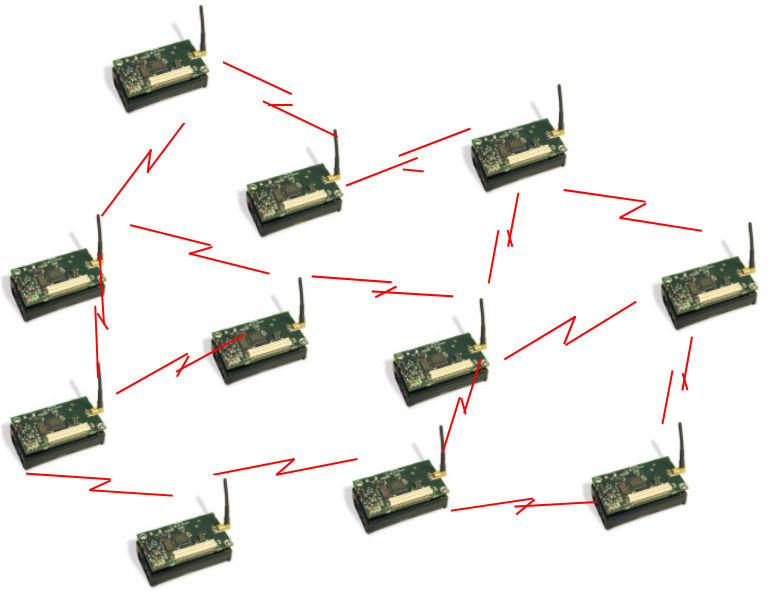
UNIVERSITY OF Waterloo

Overview

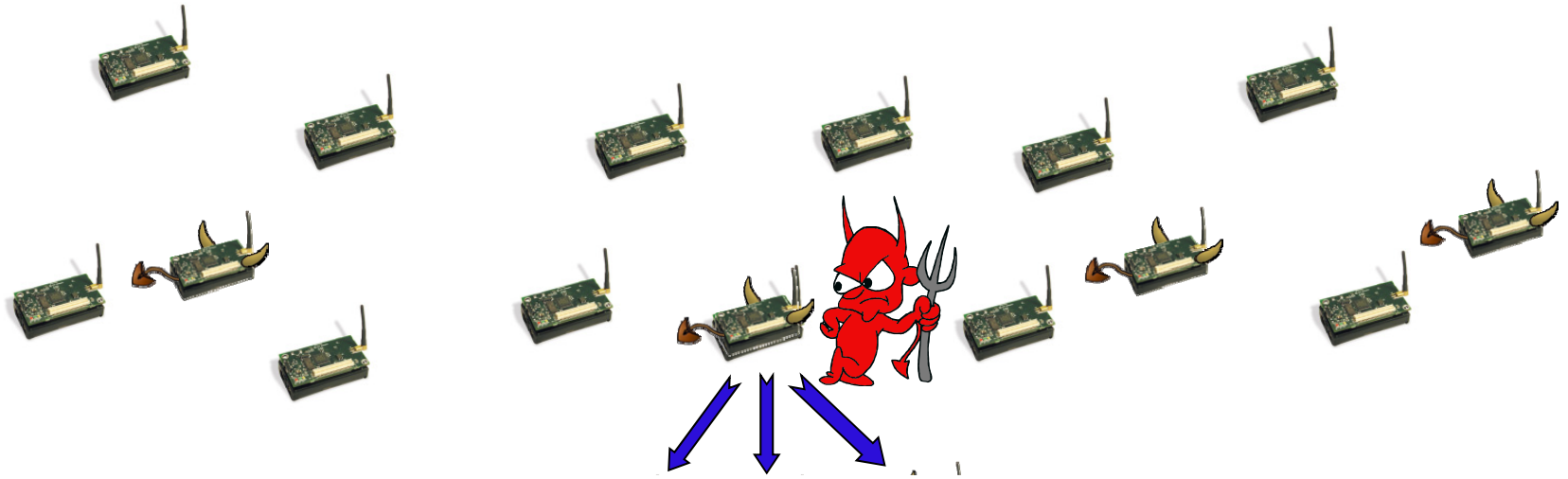
- Node Clone Attack and Previous Schemes
- Proposed Distributed Detection Protocol
- Simulations

Wireless Sensor Networks

- Ad-hoc
- A Large Number of Low-Cost Sensor Nodes
- Multi-Hop
- Infrastructureless



Node Clone Attack in WSNs

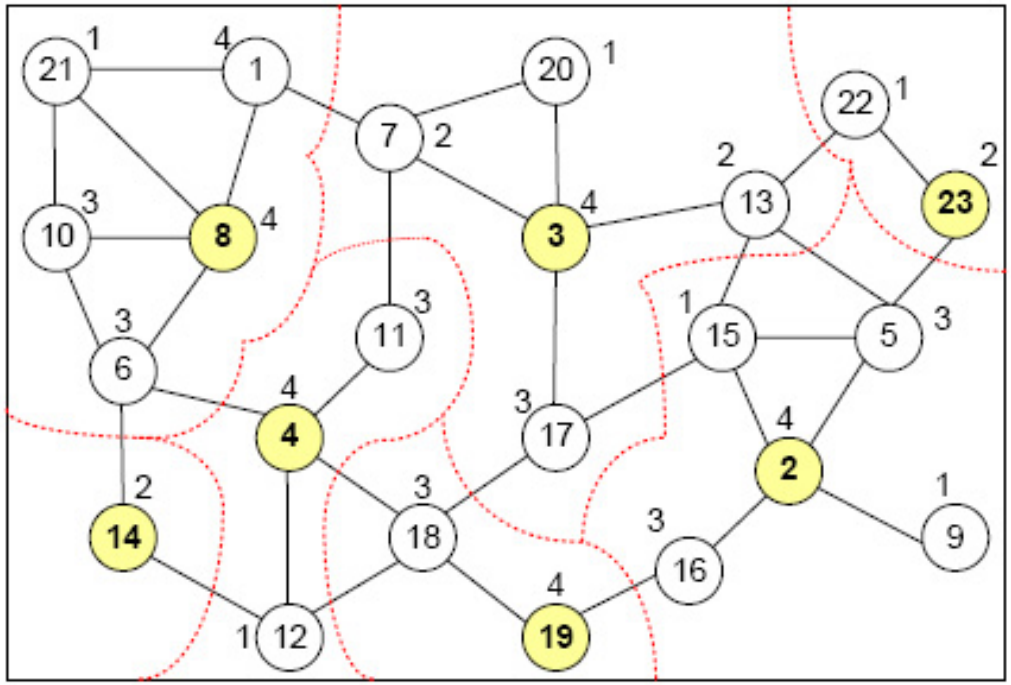


- Corrupt the collected information
- Spread abnormal behavior
- Exacerbate most of inside attacks

Centralized Approaches

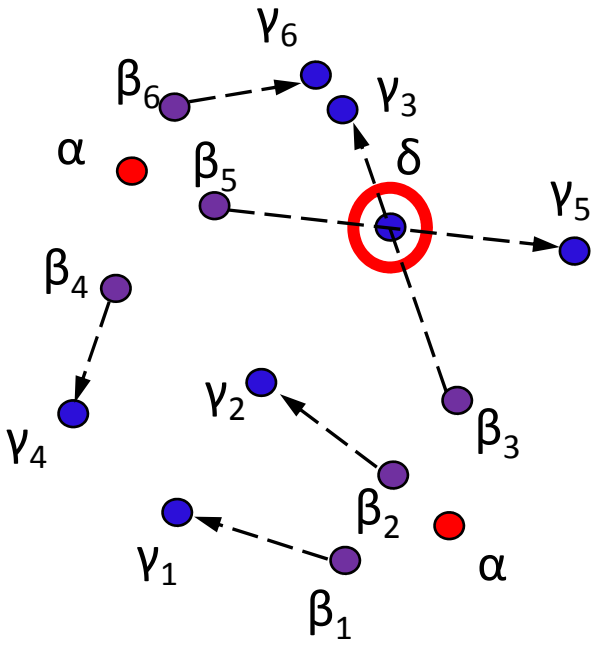
- Nodes report all neighbors to base station
- **SET**, [*Choi, Zhu,* and *Porta*, 2007]

Exclusive
Subset
Maximal
Independent
Set
Algorithm

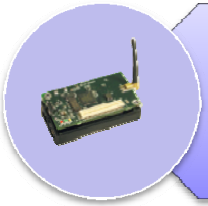


Distributed Approaches

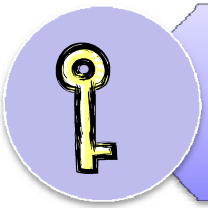
- Node-to-Network Broadcast
- *Parno, Perrig*, and *Gligor*, IEEE S&P 2005
  - Randomized Multicast
  - Line-selected Multicast
- GHT/DHT Based Schemes



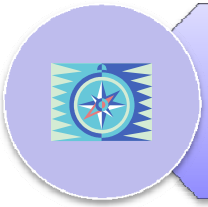
Network Model



Homogeneous Sensors Densely Deployed

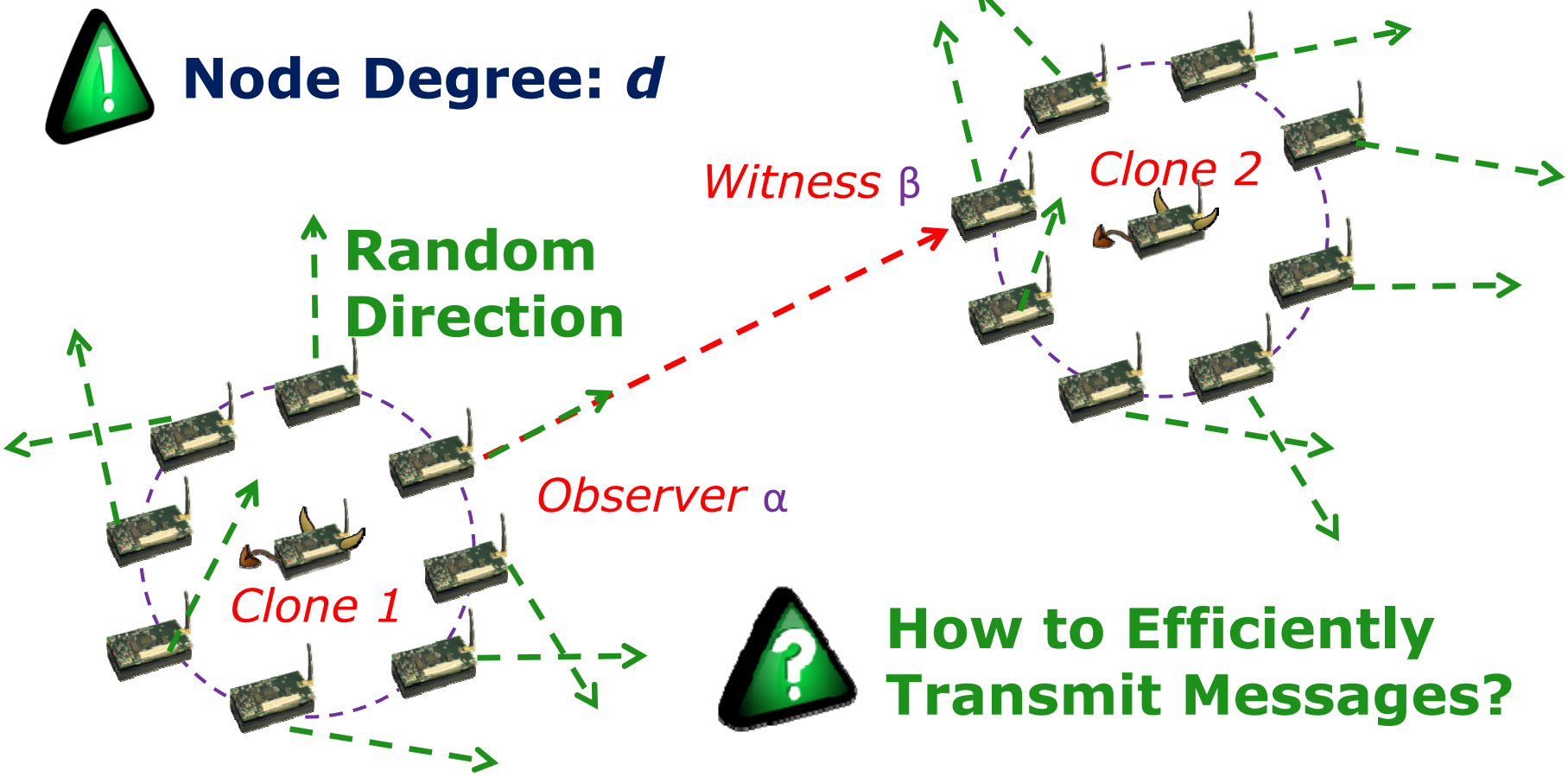


Identity-based Public-key Cryptography

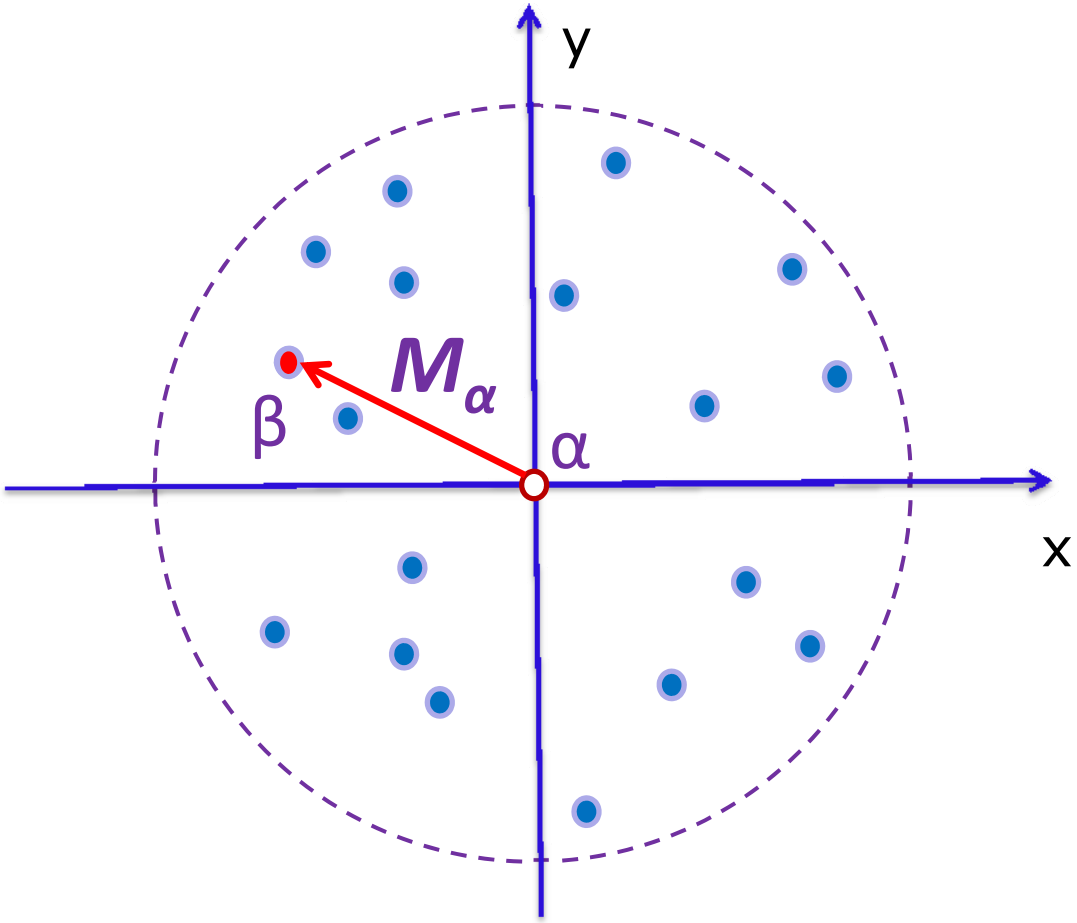


Secure Localization Mechanism

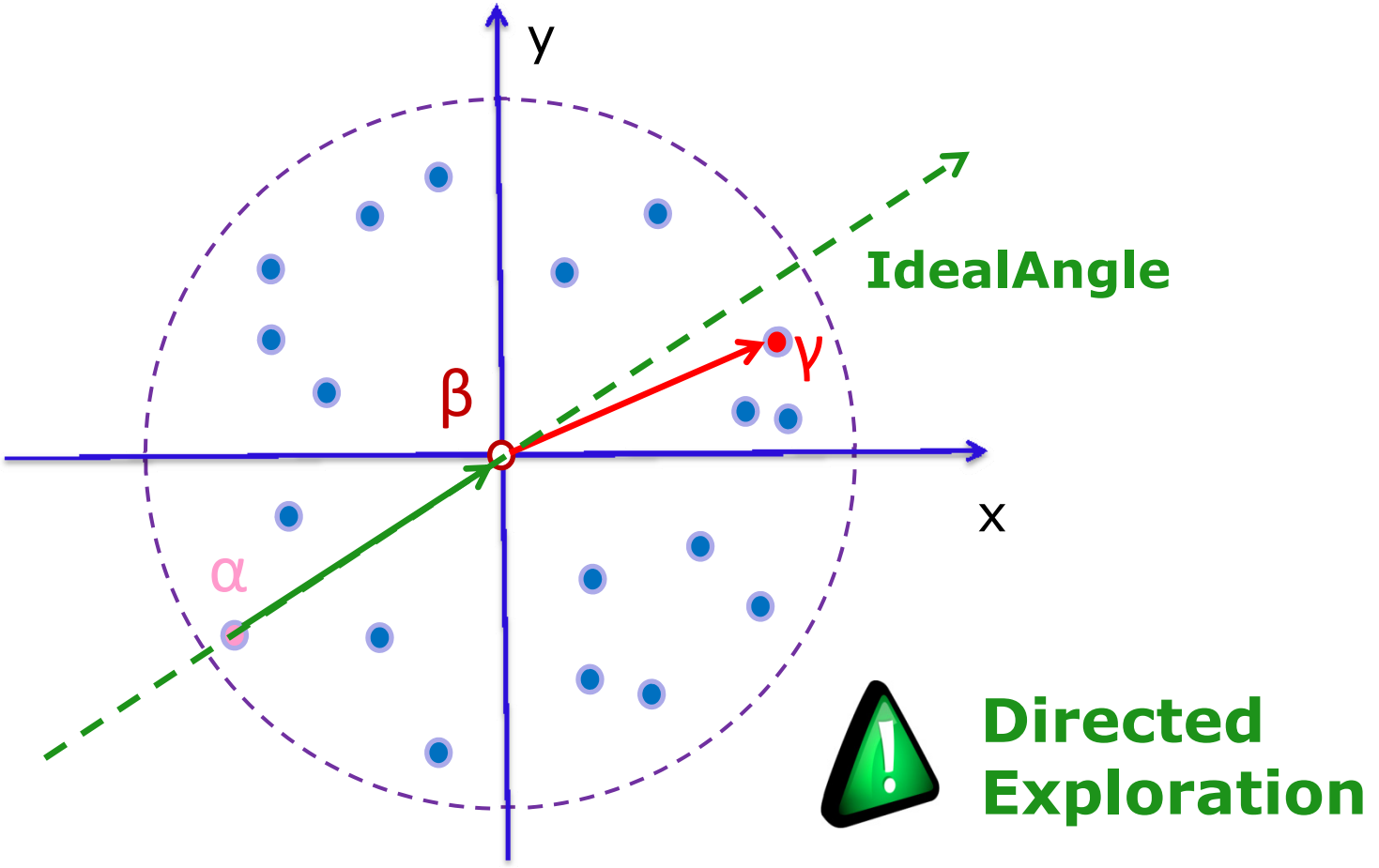
Proposed Protocol
Main Idea



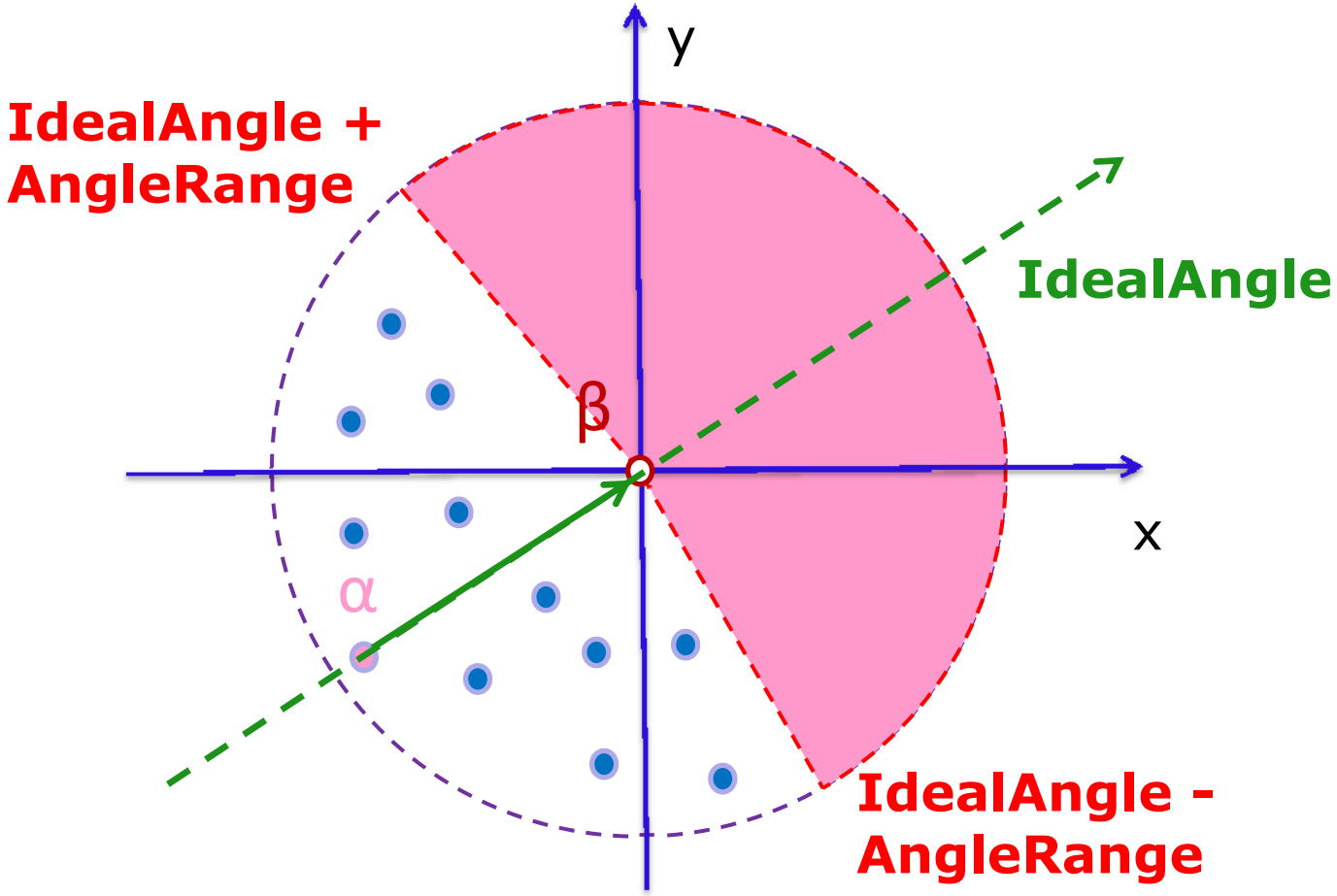
Initial Direction: Random



Forwarding Messages(Routing)



Boundary Case



Protocol Parameters

- ***TTL***--- time to live

- ***Type*** --- routing type
  - Type 1: Discard a message only if *ttl*=0
  - Type 2: In addition to *ttl* = 0, discard a message when it reaches a boundary.

    AngleRange

Algorithm: HandleMessage(M_α)

1: verify the signature of M_α
2: **if** found clone **then**
3: broadcast the evidence;
4: $ttl \Leftarrow ttl - 1$
5: **if** $ttl \leq 0$ **then**
6: discard M_α
7: **else**
8: $nextnode \Leftarrow getnextnode(M_\alpha)$
9: **if** $nextnode =$ NIL **then**
10: discard M_α
11: **else**
12: forward M_α to $nextnode$

$$M_\alpha = ttl, ID_\alpha, L_\alpha, NeighborList_\alpha, \{ID_\alpha, L_\alpha, NeighborList_\alpha\}_{K_\alpha^{-1}}$$

$$M_{evidence} = M_\alpha, M_\beta$$

Performance Comparison

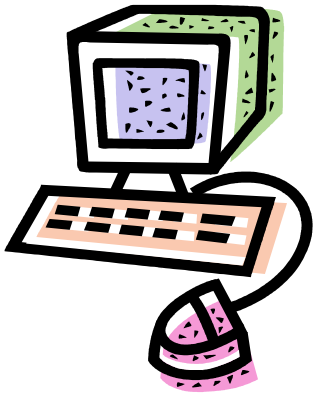
Protocol	Comm. Cost	Memory Cost
Node-To-Network Broadcasting	$O(N)$	$O(d)$
Randomized Multicast	$O(N)$	$O(\sqrt{N})$
Line-Selected Multicast	$O(\sqrt{N})$	$O(\sqrt{N})$
Randomized, Efficient, and Distributed	$O(\sqrt{N})$	$O(d\sqrt{N})$
Single Deterministic Cell	$O(\sqrt{N})$	$< O(\sqrt{N})$
Parallel Multiple Probabilistic Cells	$O(\sqrt{N})$	$< O(\sqrt{N})$
Randomly Directed Exploration	$O(\sqrt{N})$	$O(d)$

Security Analysis

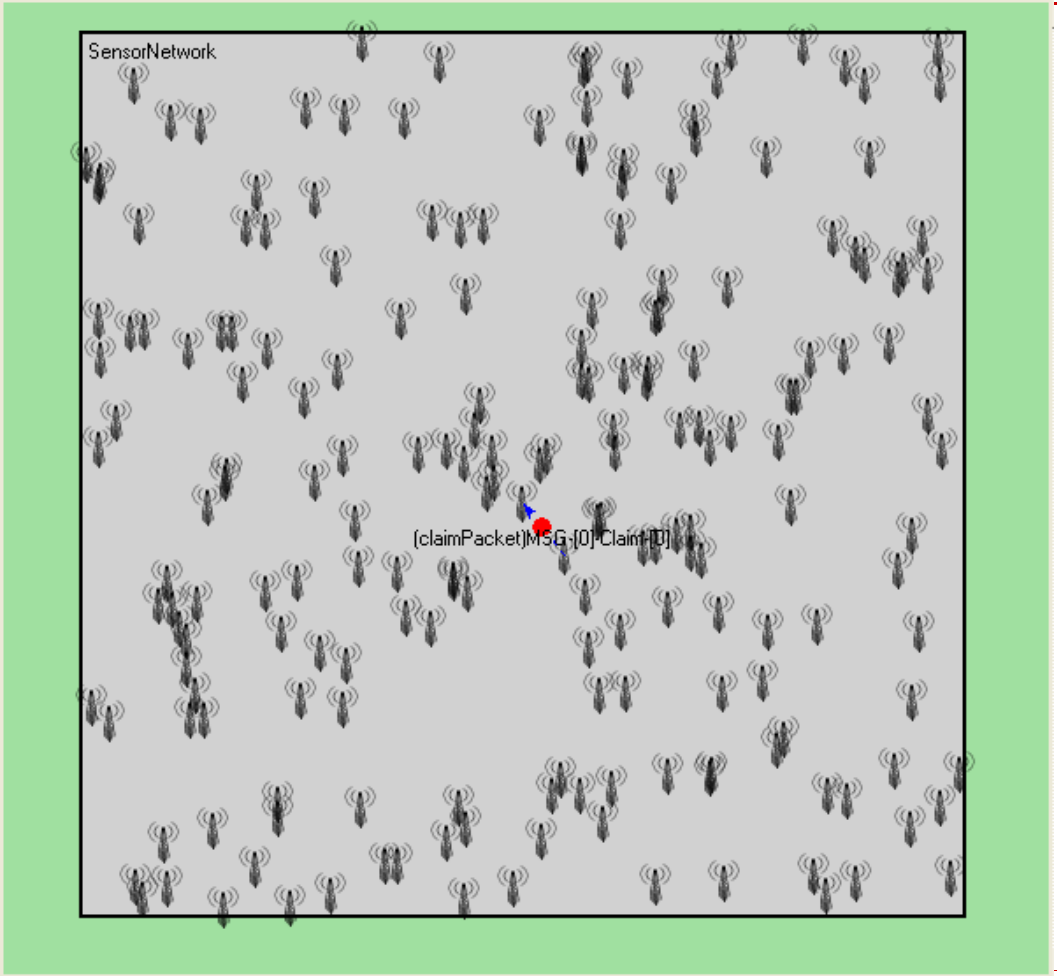
- Identity Authentication
- Message Authentication
- A cloned node cannot lie to its neighbors about its location

Simulations

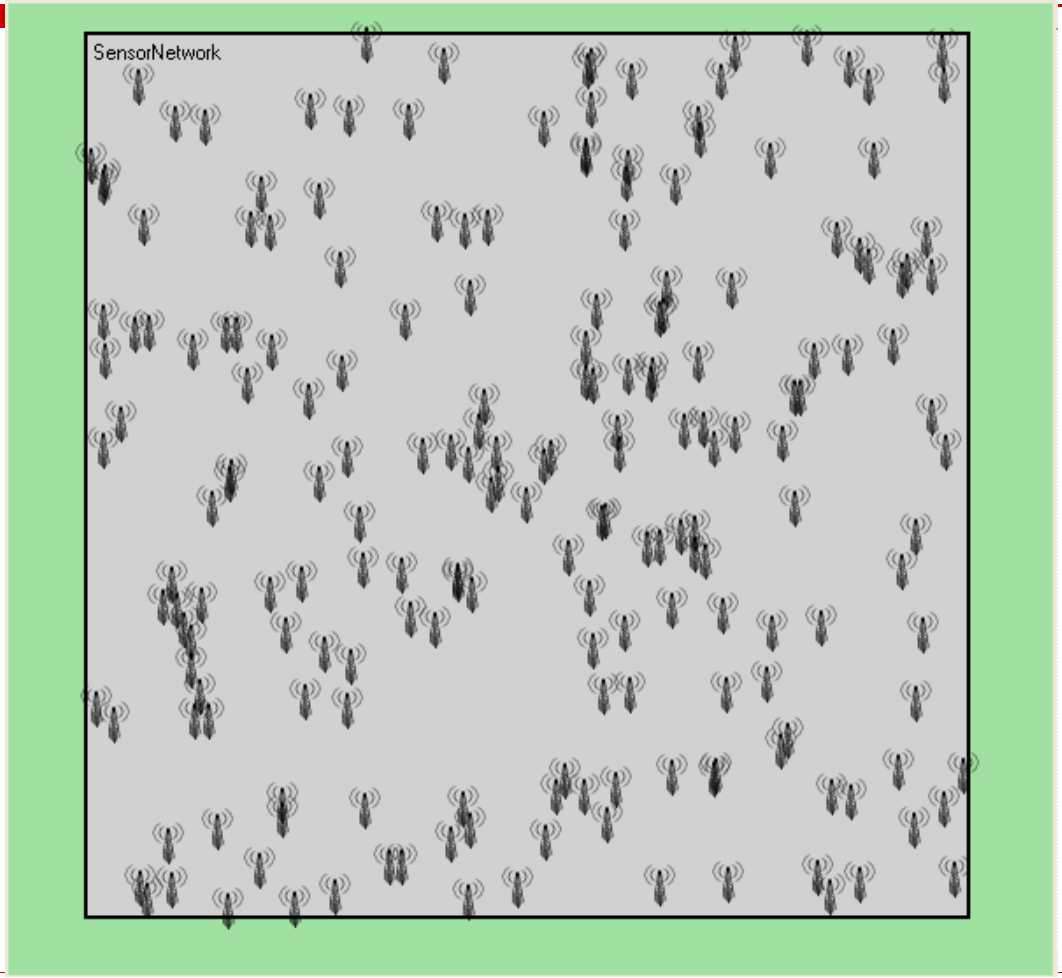
- OMNeT++ Platform
- Unit-Disc Graph
- Parameters:
  - $d = 20$
  - $ttl = \sqrt{N}$
  - Two cloned nodes



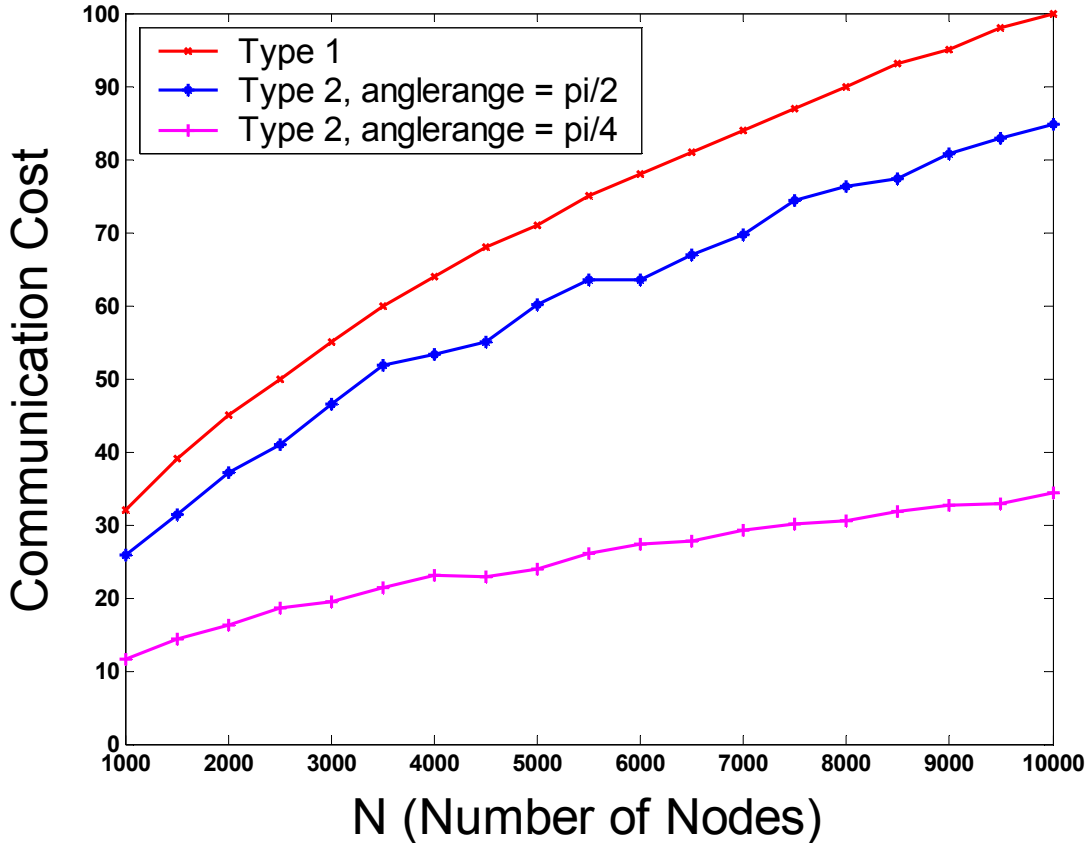
Simulation Demo: ***Type 1***



Simulation Demo: *Type 2*

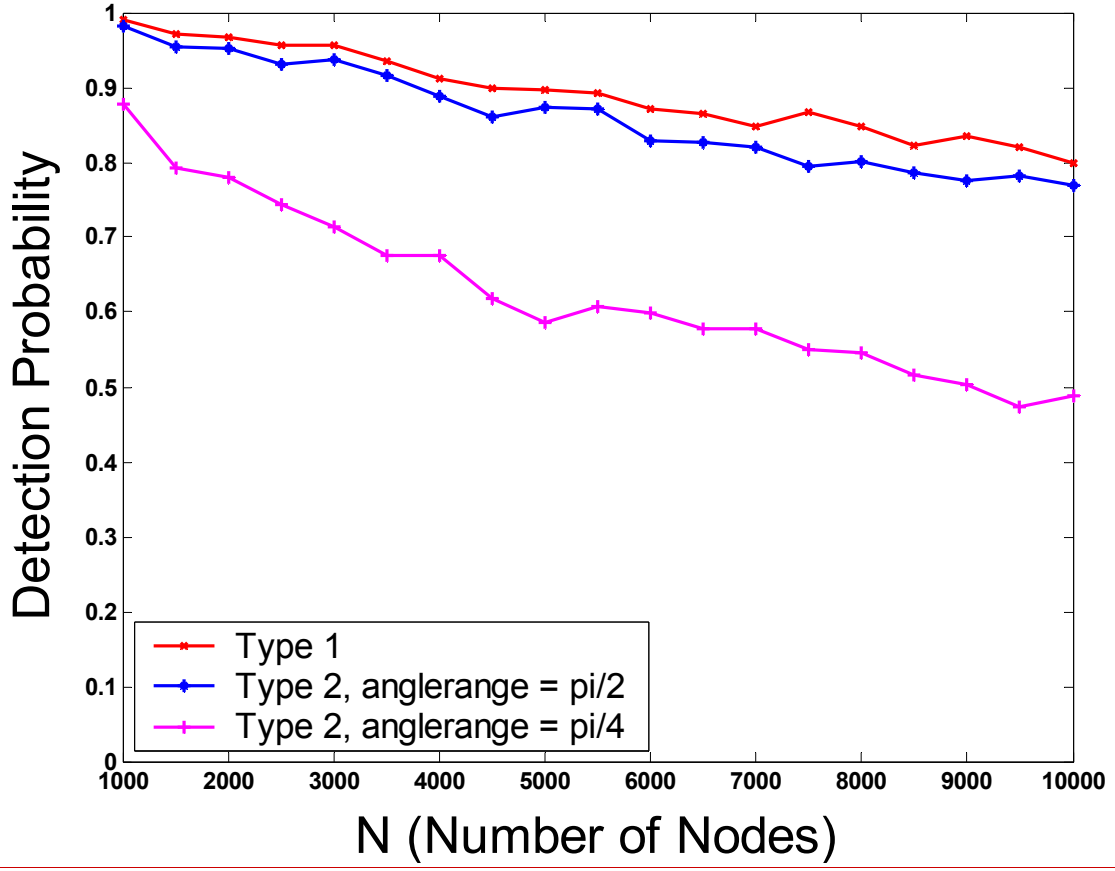


Simulation Results
Communication Cost



Simulation Results

Success Probability of Detection



Conclusions

- Directed-Forwarding
- Initial Randomness
- Achieves High Detection Probability
- Remarkable Communication and Memory costs

- Z.J. Li and G. Gong, Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks, Proceedings of IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS '09), October 12-15, 2009, Macau SAR, P.R.C, pp. 1030-1035