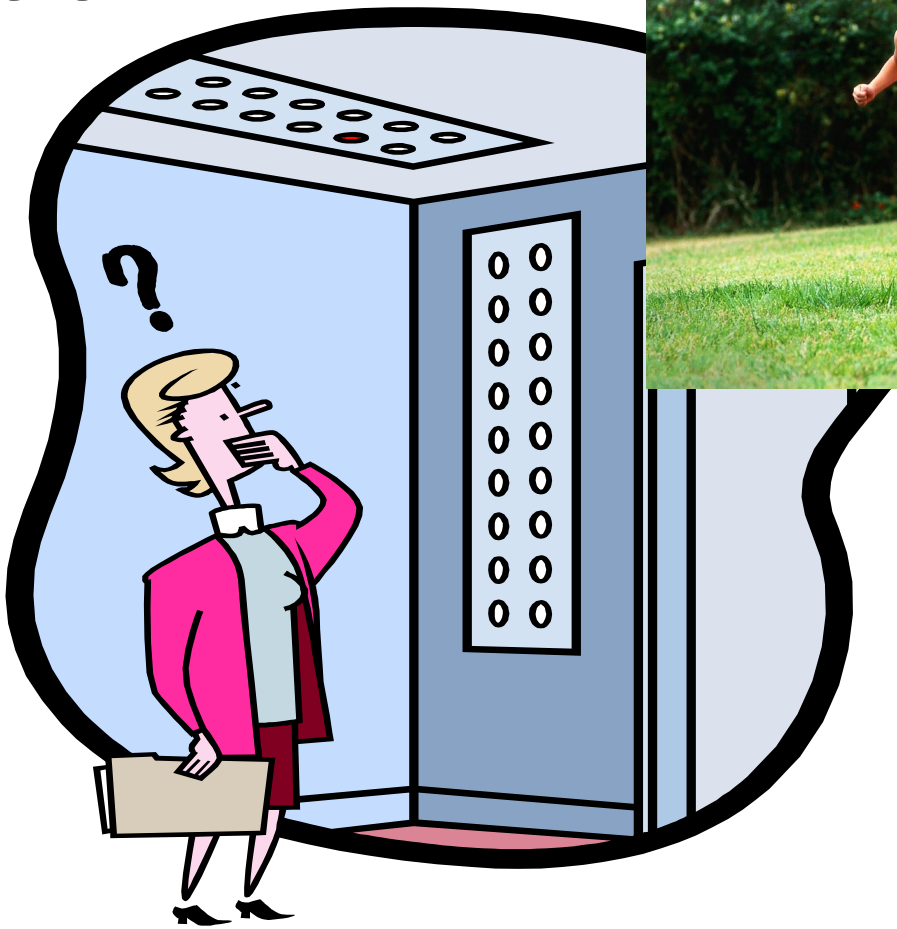
Secure Geographical Routing

Vivek Pathak and Liviu Iftode

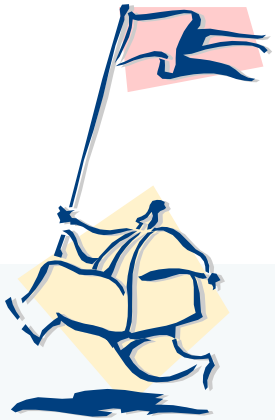
Location



- Authenticating geographical location

False Location Attacks

- Motivations
  - Economic
    - Benefit of misreporting location
  - Strategic
    - Battlefield



Privacy

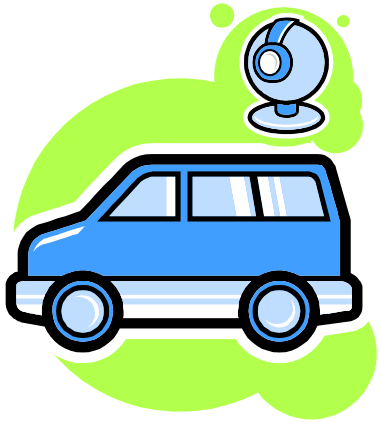
- Location privacy
  - Surveillance
  - Crime
    - Home location

Outline of the Talk

- Our solution
- Simulation studies
  - Overhead
  - Attack scenarios
- Conclusion
  - Future work

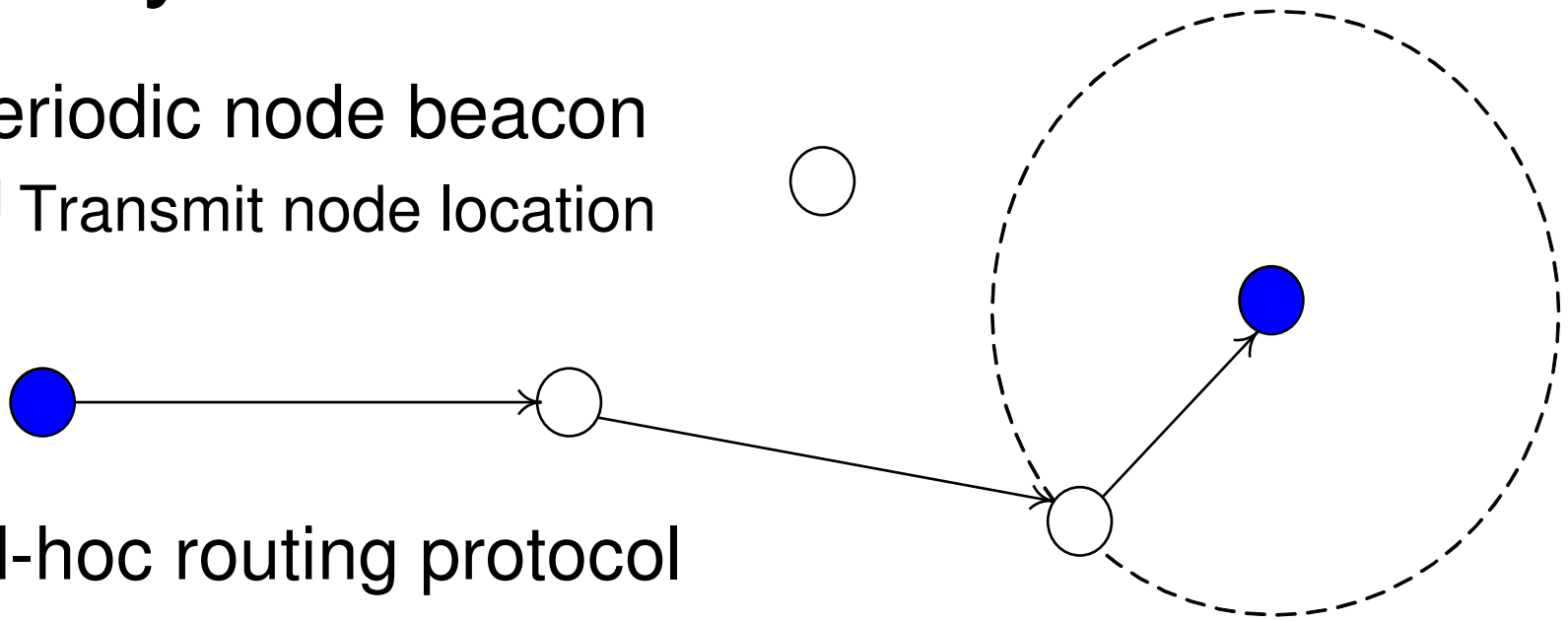
Solution Approach

- Ad-hoc network
- Nodes have GPS
  - Cell phones
  - Cars
- Geographic communication
  - Anonymous nodes
  - Location authentication



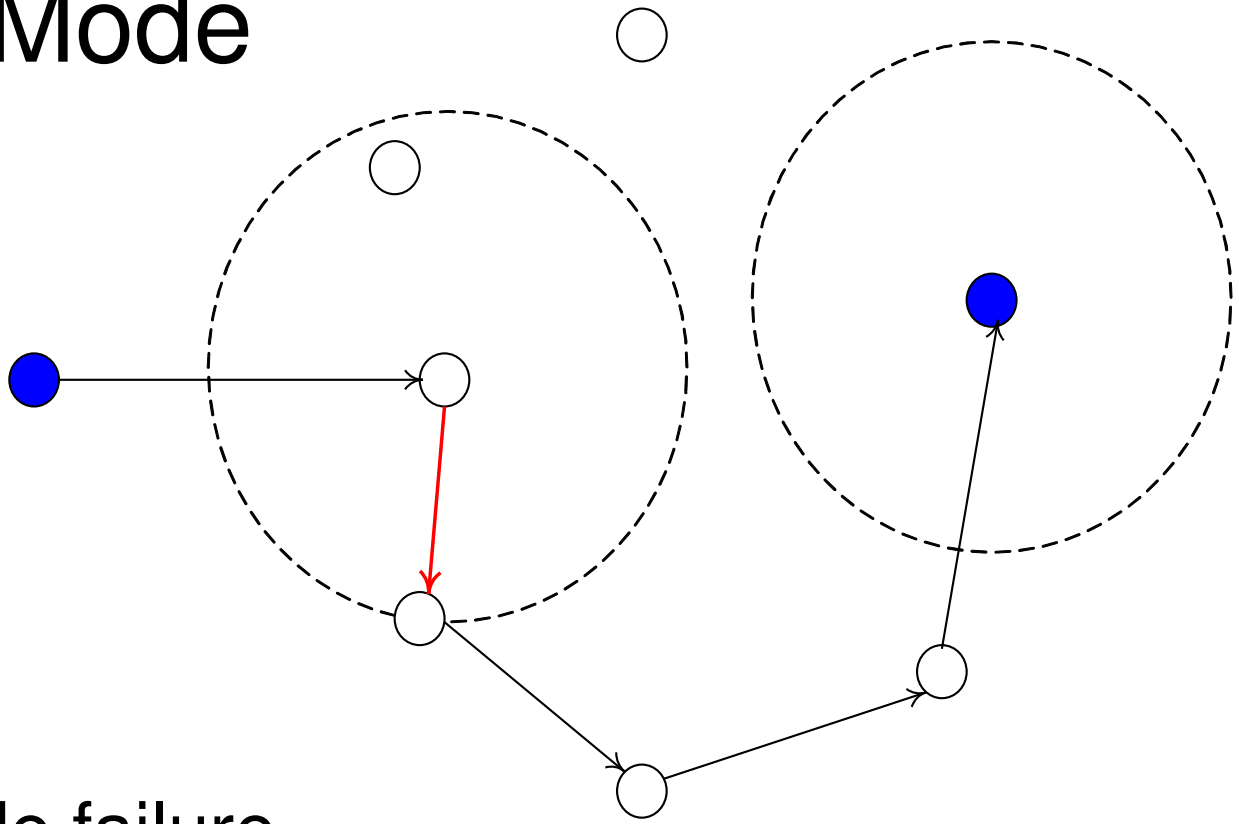
Geographical Routing Greedy mode

- Periodic node beacon
  - Transmit node location



- Ad-hoc routing protocol
  - Stateless*
  - Route closest to the destination
  - Karp and Kung – MobiCom 2000

Geographic Routing Perimeter Mode



- Greedy mode failure
  - Enter perimeter mode to route around the network hole

Features of Geographical Routing

- Highly effective ad-hoc routing protocol
  - Stateless
    - Handle mobility
    - Only local one-hop state
    - Scalable
      - Large number of nodes
      - Large number of destinations
- Nodes should “know” their location

Traditional Geographic Routing

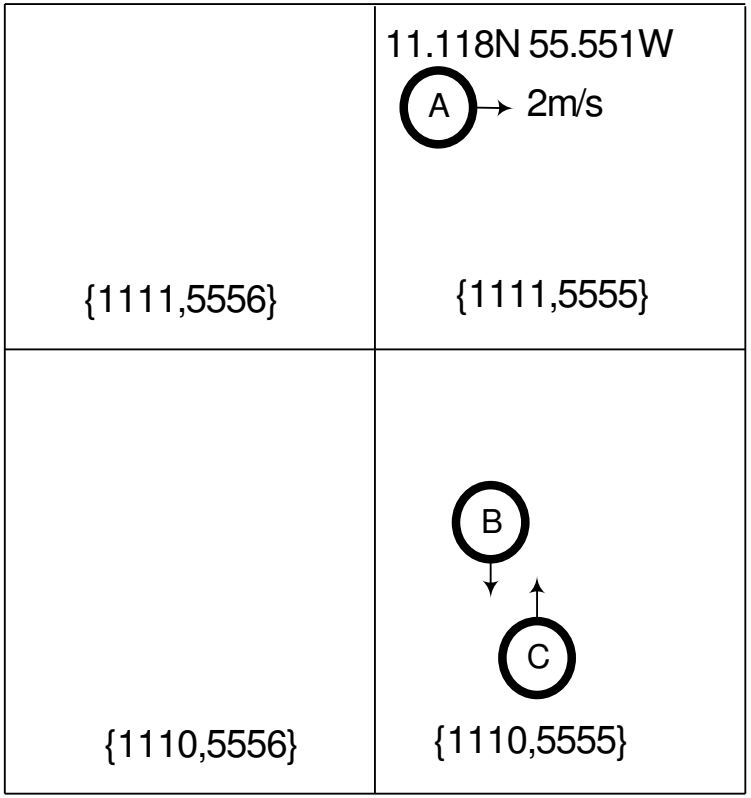
- Use case from Karp & Kung
  - Find location of the node of interest
  - Geographic routing finds route to location
- Vulnerabilities
  - Location errors and attacks
  - Location privacy

Our Solution

- Geographical secure path routing
- Resilient to malicious nodes
  - False location attack
  - Other malicious behavior like dropping packets etc.
- Infrastructure free authentication
  - Public key of destination
  - Location of destination
  - Path taken by a routed message

Geographical Authentication Model

- Nodes are anonymous
  - Use temporary pseudonyms
  - Generate their own key pairs
  - All messages are signed
- Locations mapped to integer vector space
  - Application dependent global constant for mapping

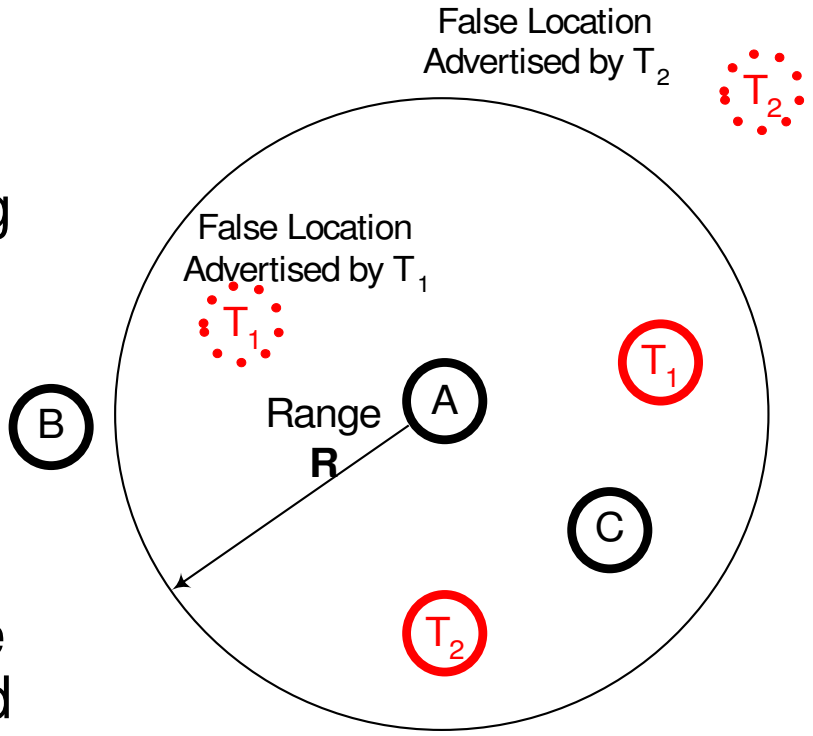


Assumptions

- Wireless network
  - Bi-directional links
    - 802.11 MAC
  - Physical layer defense against Jamming
    - Spread spectrum techniques
  - Global range limitation
  - Overhear transmissions of neighbors
- Adversaries can not affect honest nodes
  - Reception or transmission

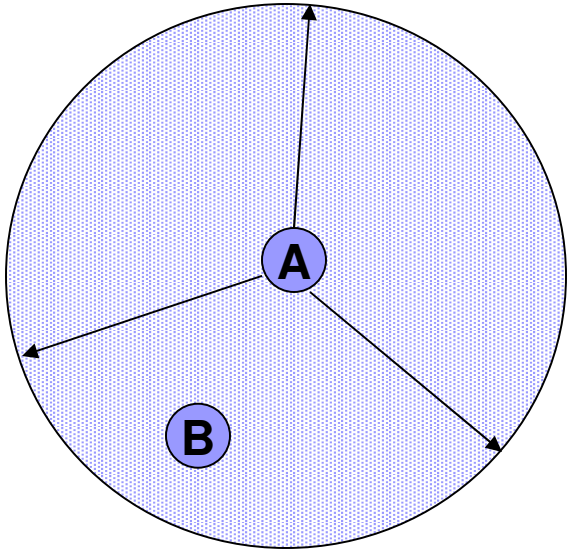
Detecting Malicious Neighbors

- Each node detects malicious neighbors
  - Range constraint violation
  - Overhear malicious forwarding behavior
- Takes corrective action
  - Ignore malicious node for routing
  - Malicious actions are provable because messages are signed



One-hop Public-key Authentication

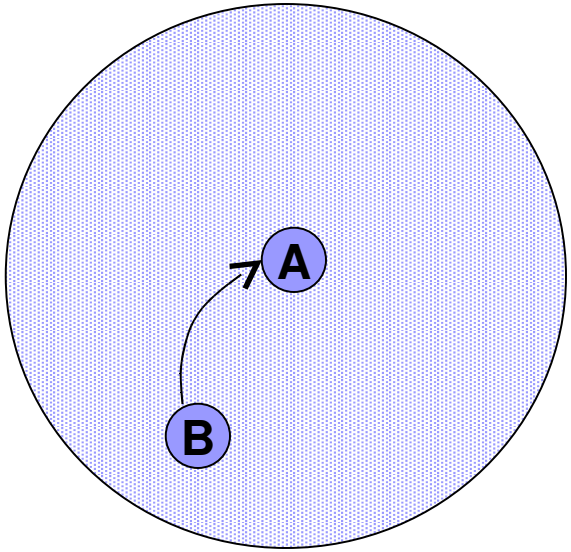
- Nodes generate their own key pairs
- Beacon includes public key
  - Public keys are well known locally
- One hop authentication through challenge response
  - Man in the middle attack is impossible in wireless network



Beacon	Time	Location	Public Key

One-hop Public-key Authentication

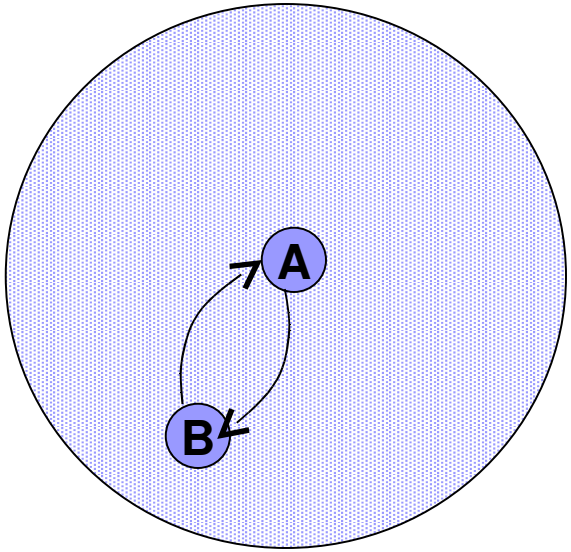
- Nodes generate their own key pairs
- Beacon includes public key
  - Public keys are well known locally
- One hop authentication through challenge response
  - Man in the middle attack is impossible in wireless network



Challenge	Nonce

One-hop Public-key Authentication

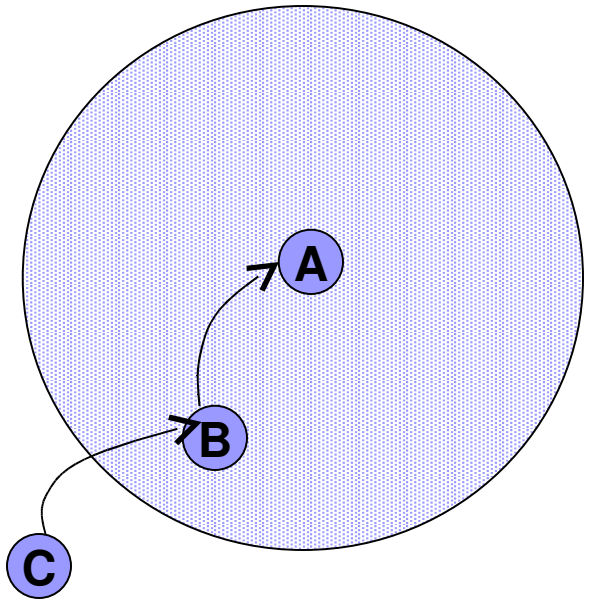
- Nodes generate their own key pairs
- Beacon includes public key
  - Public keys are well known locally
- One hop authentication through challenge response
  - Man in the middle attack is impossible in wireless network



Response	Nonce	Decrypted Nonce

Recursive Challenge Response

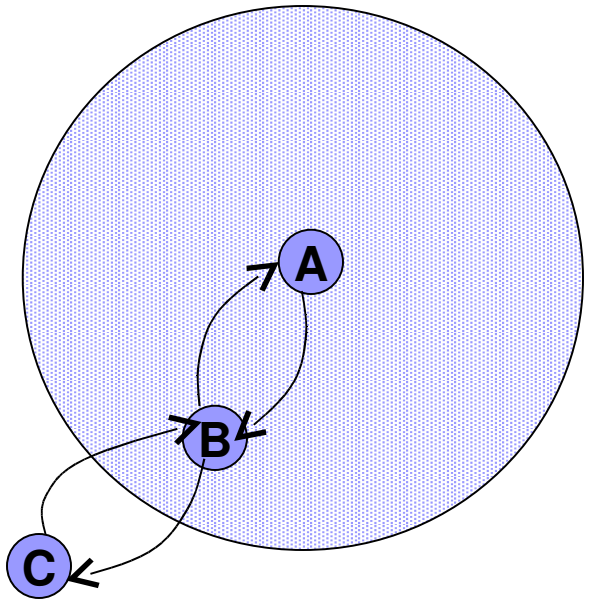
- Remote keys are recursively authenticated
  - From one hop to another
- Two-hop key is authentic
  - If one-hop is authentic
  - If B is honest



Challenge	Nonce

Recursive Challenge Response

- Remote keys are recursively authenticated
  - From one hop to another
- Two-hop key is authentic
  - If one-hop is authentic
  - If B is honest



Response	Nonce	Nonce decrypted with two keys

Pipelined Challenge Response

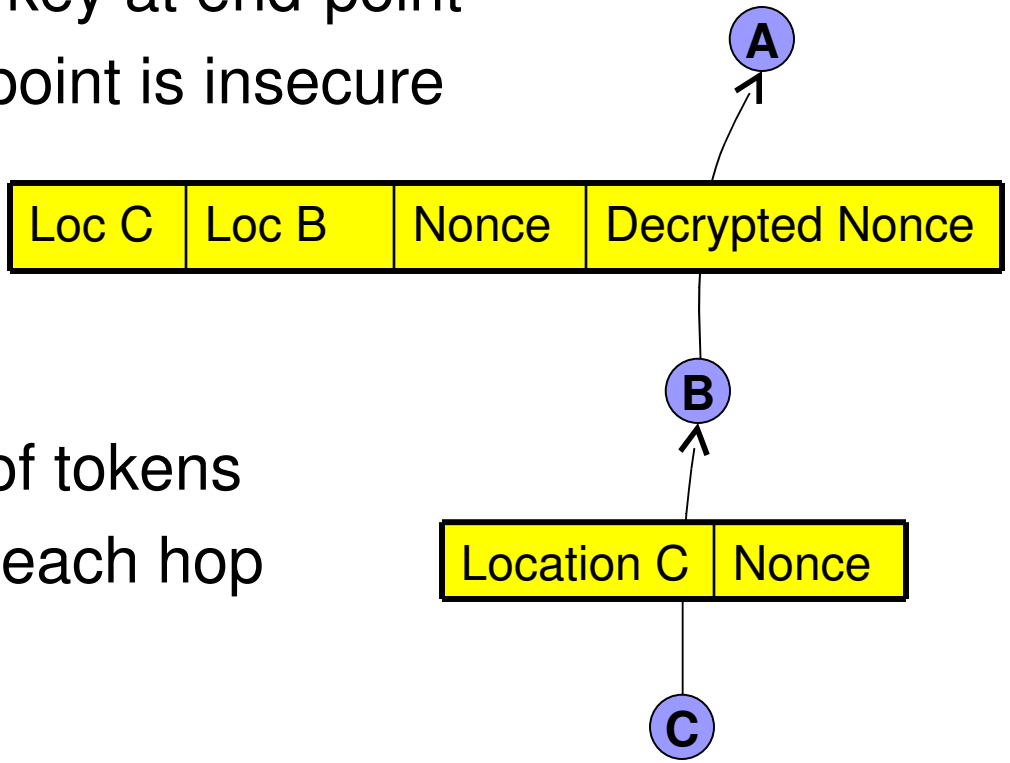
- Challenge response latency
  - Pipelining for performance

P_{i-1}	$\rightarrow$	P_i	$\{ \text{Challenge} , P_{i-1}, P_i, r_A \}_{P_{i-1}}$
P_i	$\rightarrow$	P_{i+1}	$\{ \text{Challenge} , P_i, P_{i+1}, r_A \}_{P_i}$
P_i	$\rightarrow$	P_{i-1}	$\{ \text{Local Response} , P_i, P_{i-1}, K_{P_i}^{-1}(r_A), K_{P_{i+1}}, P_{i+1} \}_{P_i}$
P_{i+1}	$\rightarrow$	P_i	$\{ \text{Local Response} , P_{i+1}, P_i, K_{P_{i+1}}^{-1}(r_A), K_{P_{i+2}}, P_{i+2} \}_{P_{i+1}}$
P_i	$\rightarrow$	P_{i-1}	$\{ \text{Recursive Response} , P_i, P_{i-1}, K_{P_i}^{-1} \circ K_{P_{i+1}}^{-1}(r_A), K_{P_{i+1}}, P_{i+1}, K_{P_{i+2}}, P_{i+2} \}_{P_i}$

- Remove latency
  - Get identical response

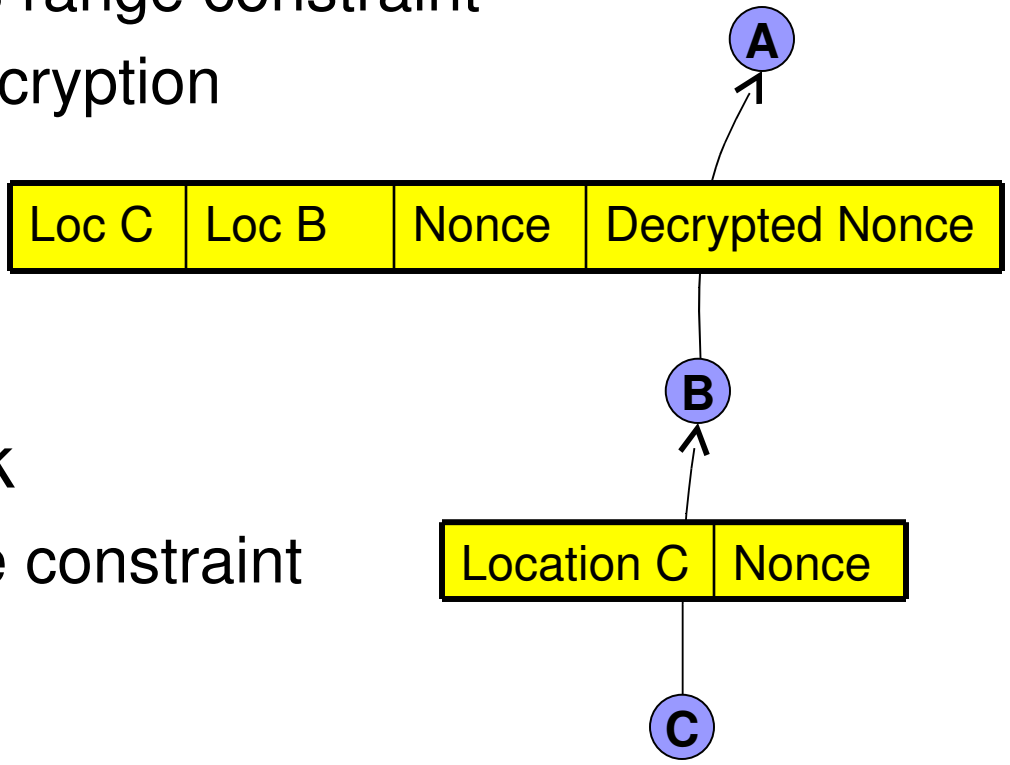
Proof of Path

- Recursive challenge response
  - Authenticates public key at end-point
  - Location of the end-point is insecure
- Proof of path
  - Packet contains list of tokens
  - Append to the list at each hop



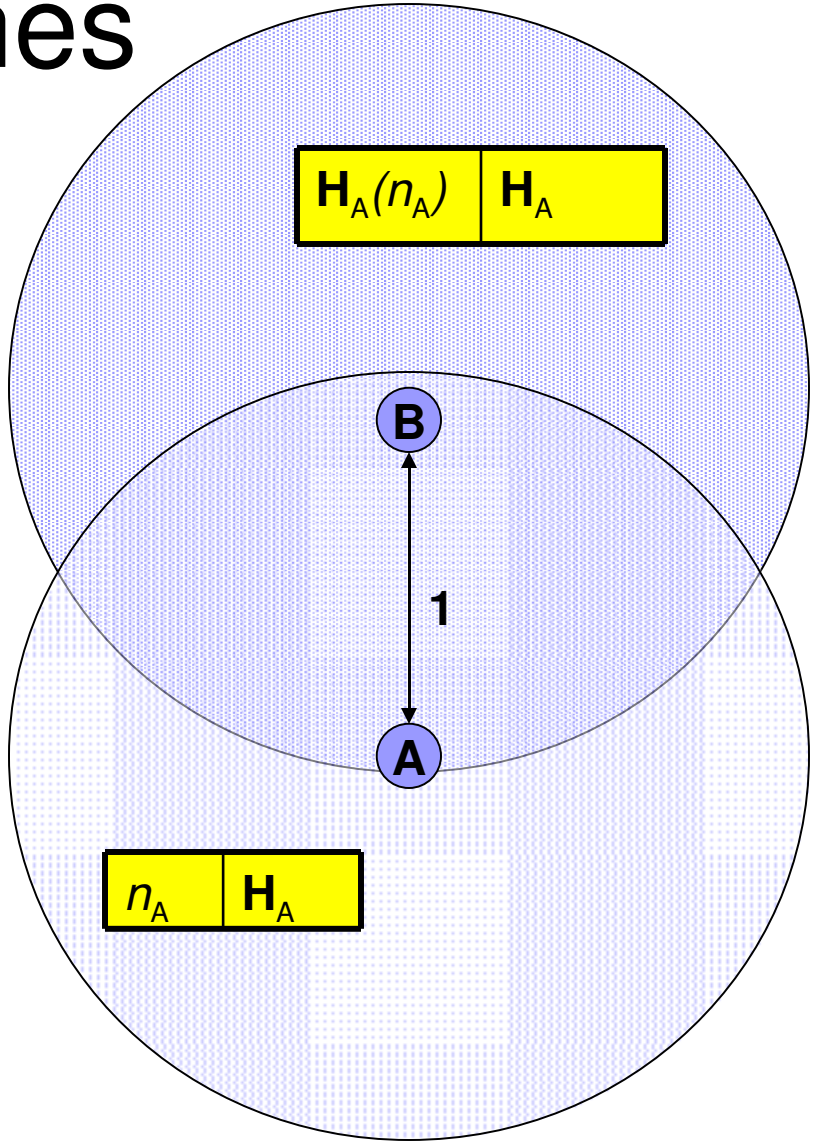
Proof of Path Mechanism

- Verification before forwarding
  - Location list satisfies range constraint
  - Integrity of nonce decryption
- False location attack
  - Must be within range constraint



Geographic Hashes

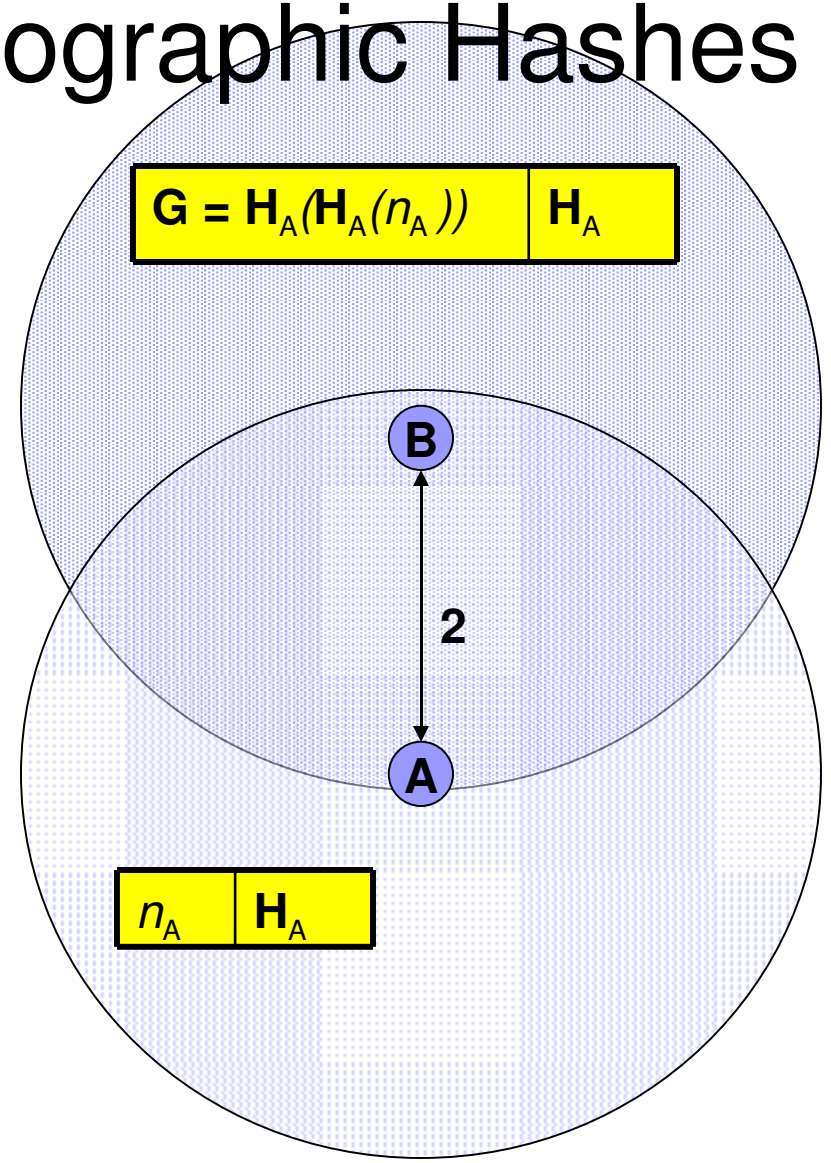
- Provide unforgeable positioning
  - Use associative one way hash functions
  - The geographic hash is with respect to a node
  - Its value depends on location



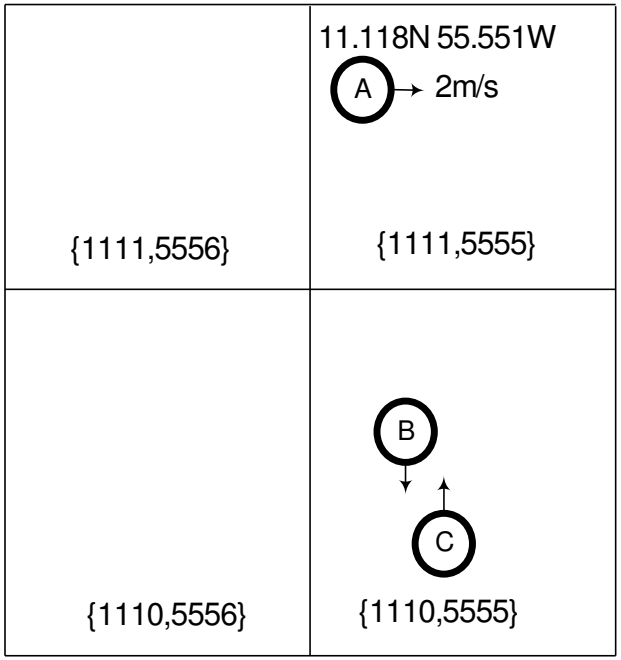
Construction of Geographic Hashes

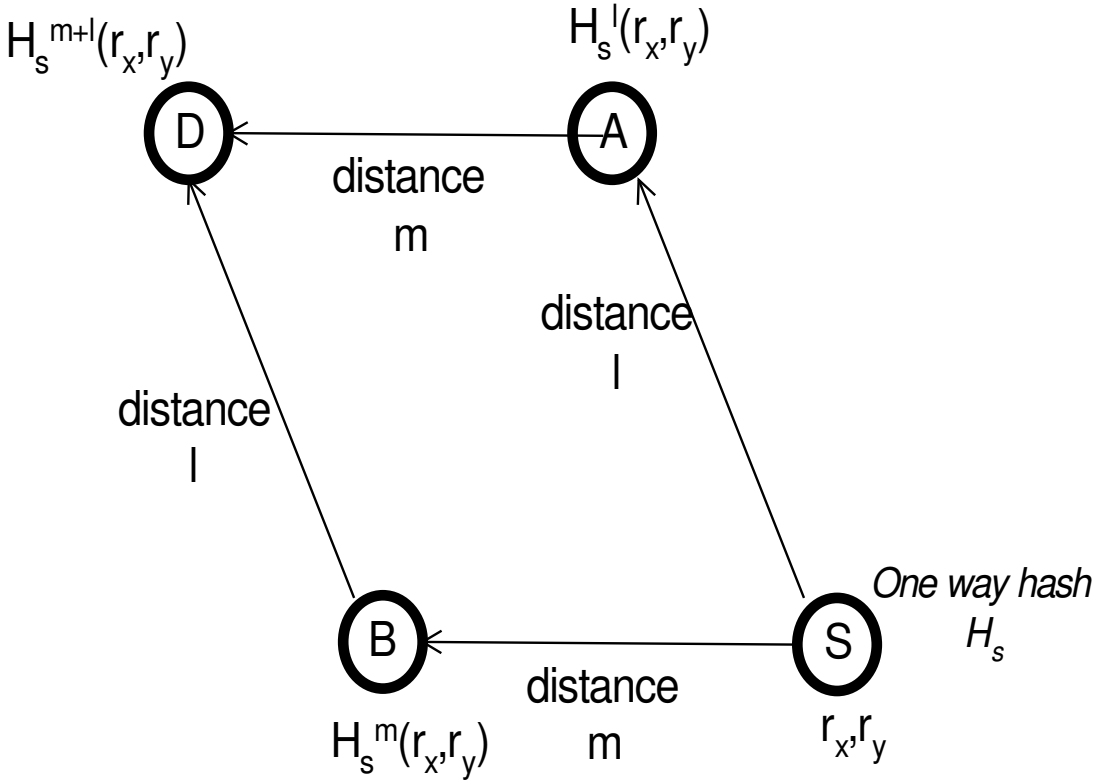
- Nodes publish one way hash functions
  - One for each dimension
  - Random nonce
- Receivers compute the local value based on integer co-ordinates

$$G_j(p) = H_j^{(y_j - p_j)}(r_p)$$



Geographic Hash Agreement





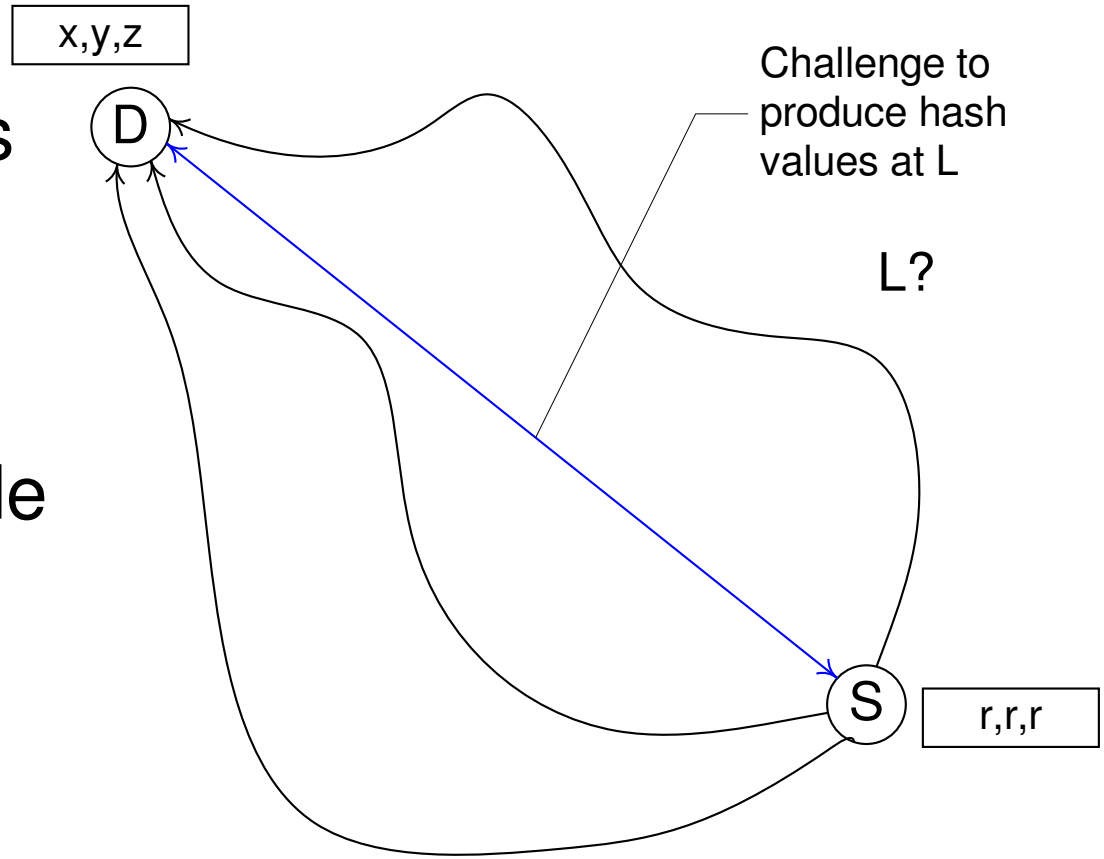
- Hash values must agree along all paths
  - Detect bad localities

Transient Geographic Hashes

- Short lived geographic hashes
  - Source publishes hash function for time
  - Every node applies it once per time period
- Associative hash functions
  - Preserve the hash value across space and time

Location Authentication

- Use multiple paths to authenticate geographic hash
- Challenge the node to prove it knows the secret without disclosing the secret



Secure Geographical Routing Sketch

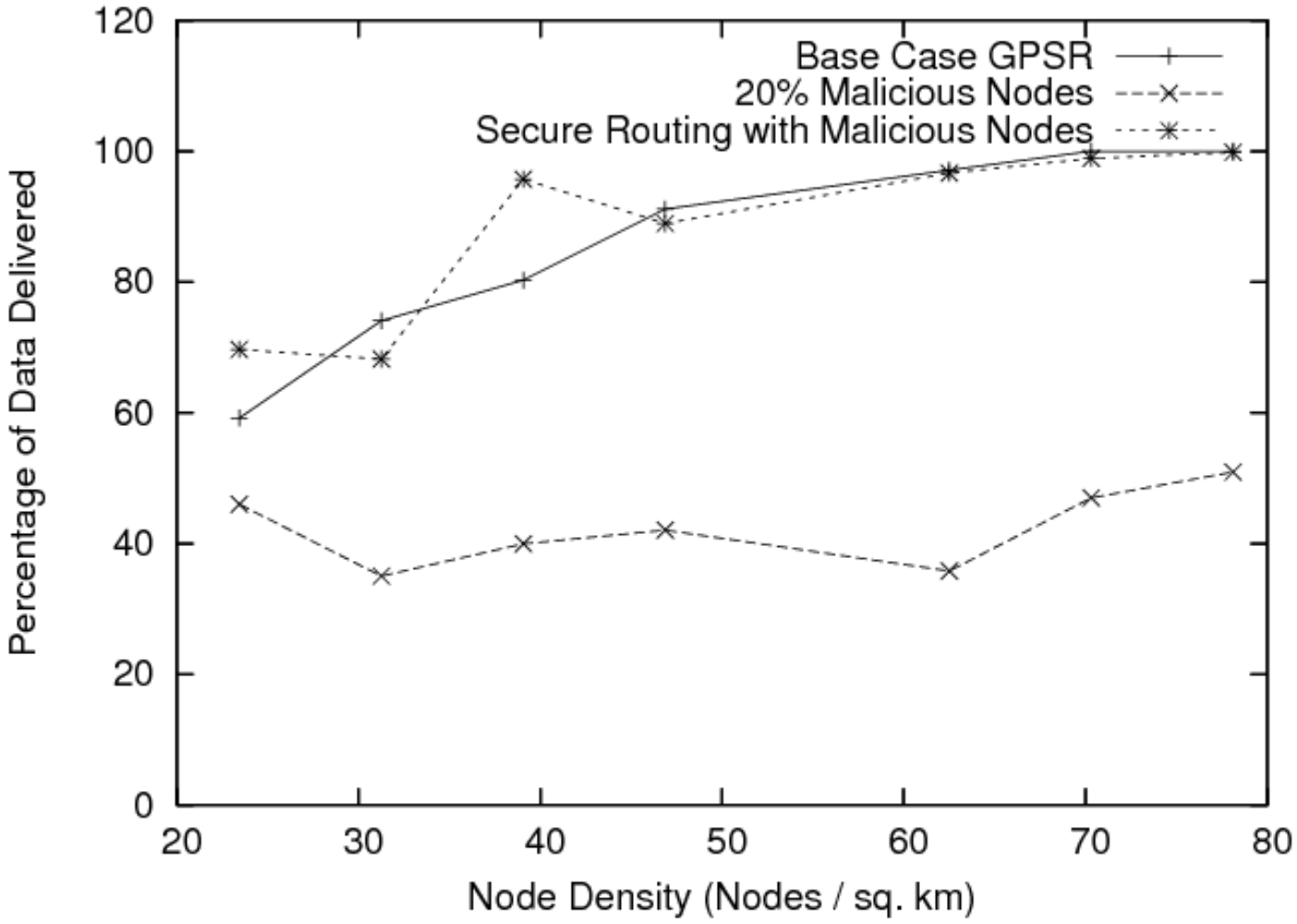
- Conduct challenge response with destination
  - Source authenticates public keys of all nodes on the path
- Attach proof of path tokens on the challenge and response messages
  - Receiver gets correct routing path from sender
  - Sender gets the correct routing path to receiver
- Destination publishes geographic hash
  - Source gets correct location of destination

Performance Analysis

- Compare with GPSR
  - Implement secure routing in NS2
  - Modify GPSR routing implementation to allow malicious nodes
- Effectiveness of secure geographical routing
  - Node density
  - Malicious nodes
  - Mobility

Effect of Node Density on Delivery Rate

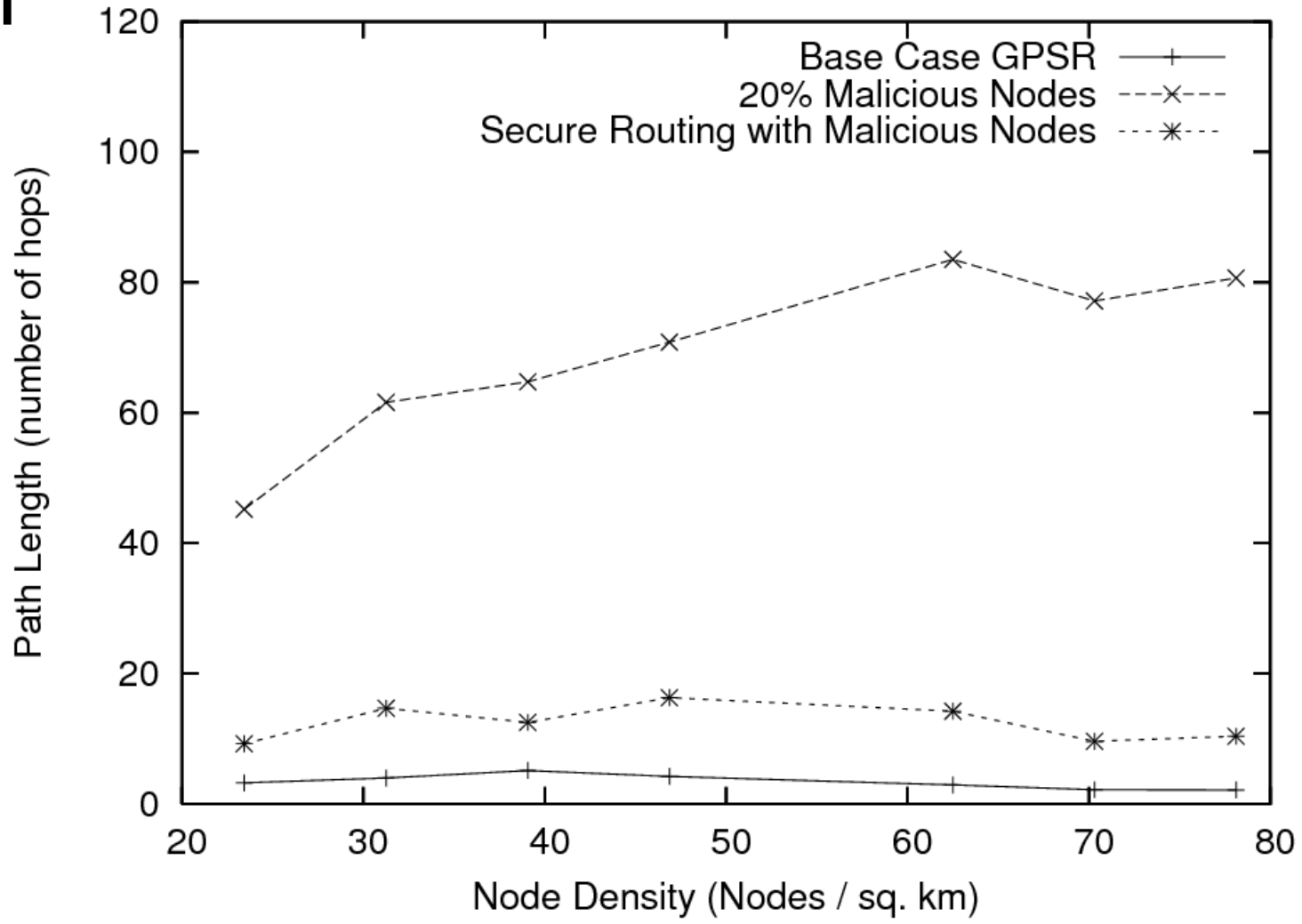
- GPSR is susceptible to malicious nodes
- Node density does not help
- Compare with secure geographical routing



- Take advantage of node density to resist routing errors introduced by malicious nodes

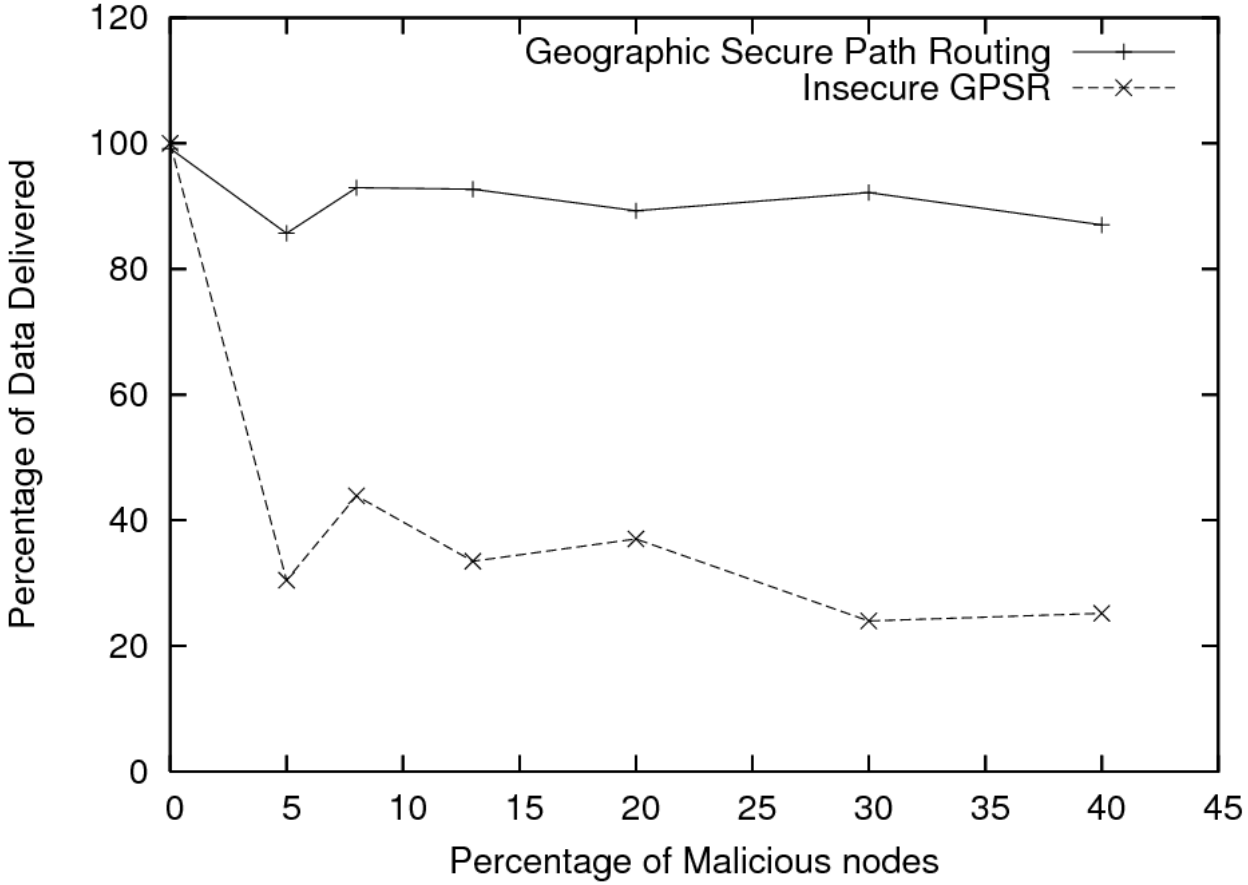
Effect of Node Density on Path Length

- Malicious nodes can not force extreme path lengths
- Resilience with large proportion of malicious nodes



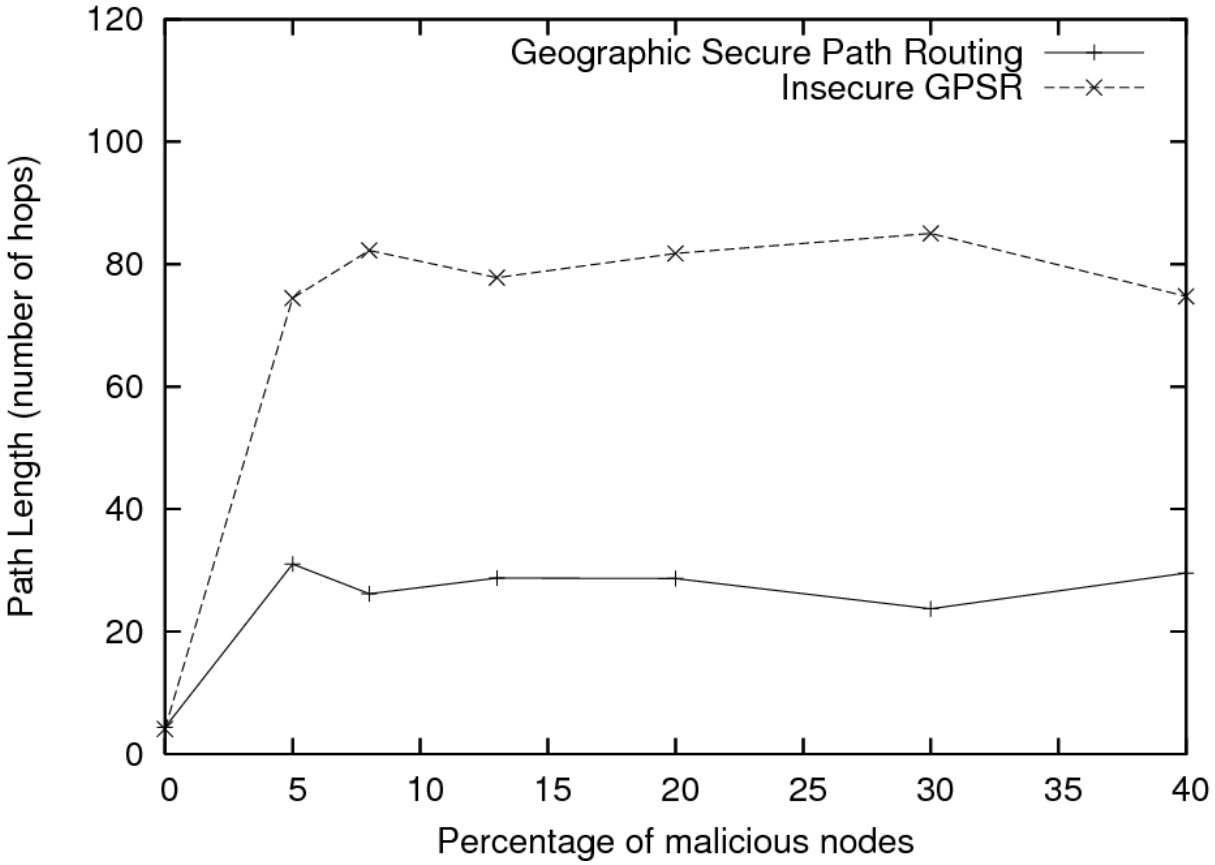
Effect of Malicious Nodes on Delivery Rate

- GPSR breaks down with malicious nodes
- Resilience to large fraction of malicious nodes



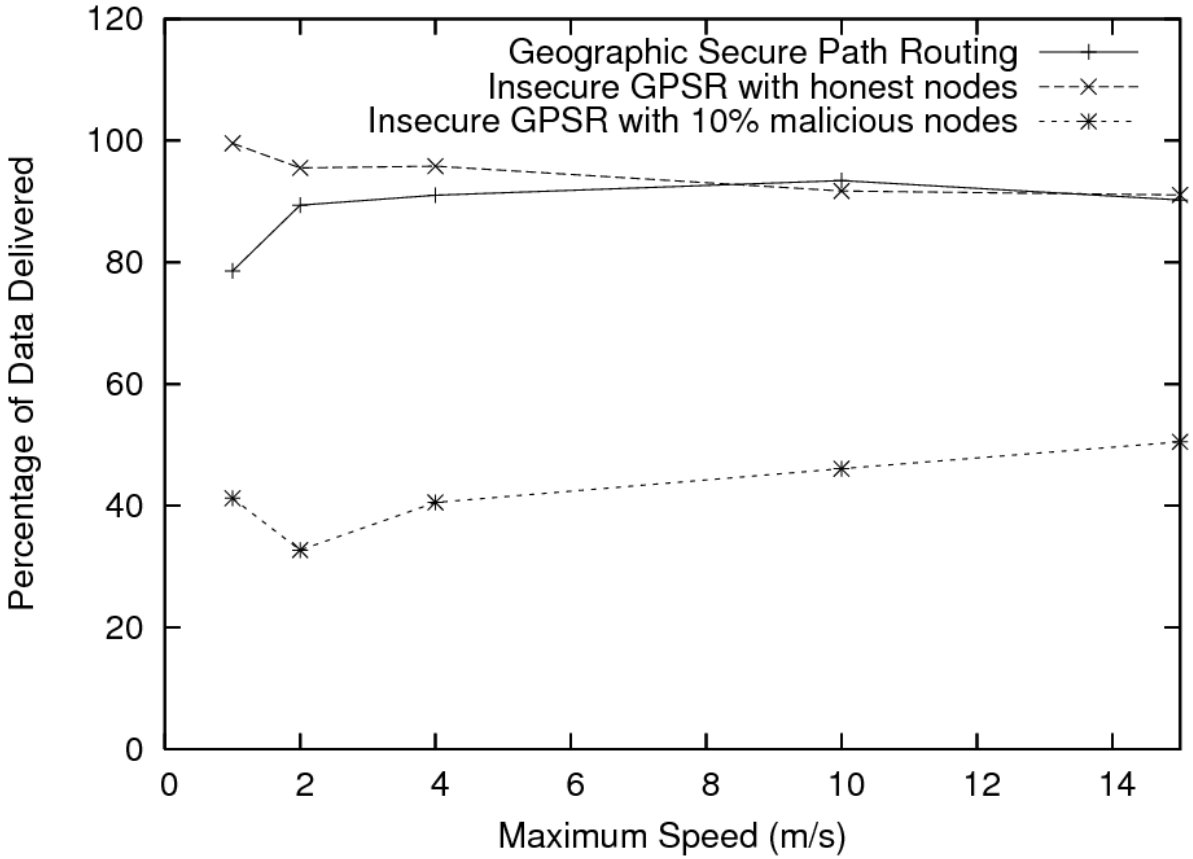
Effect of Malicious Nodes on Path Length

- Increase in path length along with low delivery rate
- Achieve high delivery rate with constant path length overhead



Mobility & Malicious Nodes

- Mobility does not help GPSR significantly
- Secure geographical routing improves delivery rate with mobile nodes



- Take advantage of mobility by finding new non-malicious nodes

Conclusion

- Secure geographical routing
  - Resist malicious nodes
  - Reasonable performance
- Authenticate location of anonymous nodes
  - Using short lived verifiable geographic hashes
- Authenticate public key of node at given location

Future Work

- Applications
  - Localized Cab fare negotiation
  - Private communication for highway conditions
- Geographical security policies

Future Work

- Applications
  - Localized Cab fare negotiation
  - Private communication for highway conditions
- Geographical security policies