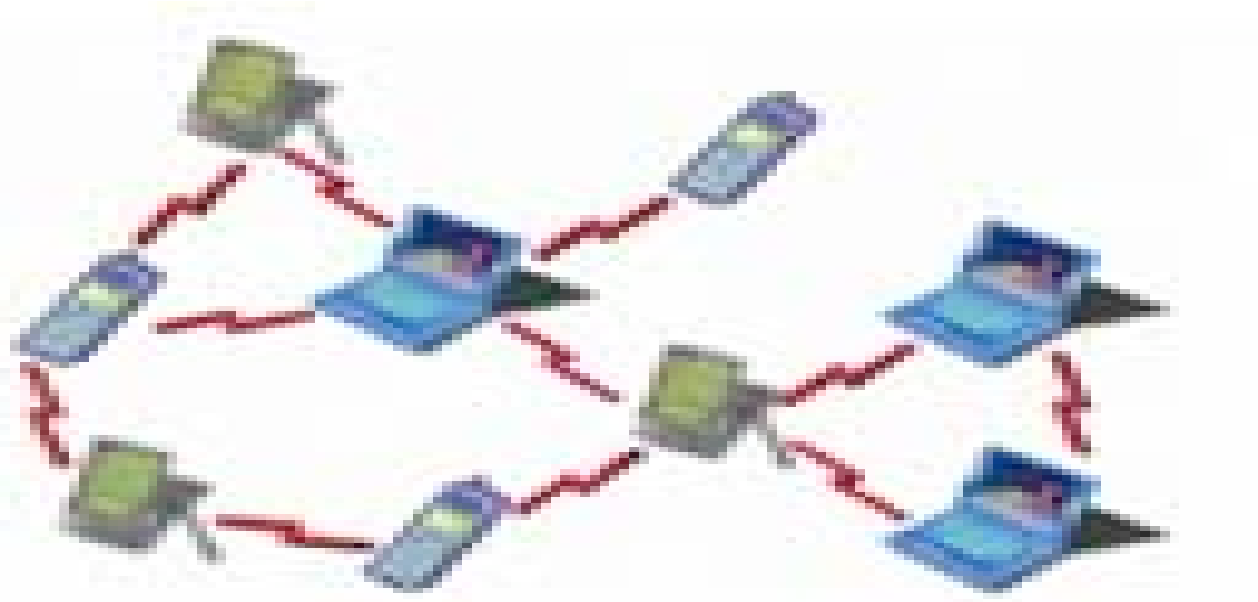
ALARM: Anonymous Location-Aided Routing in Suspicious MANETS

Gene Tsudik (joint work with Karim Eldefrawy)
UC Irvine
gene.tsudik @ uci.edu

IEEE ICNP'07, October 2007 (to appear).

In a “normal” MANET:

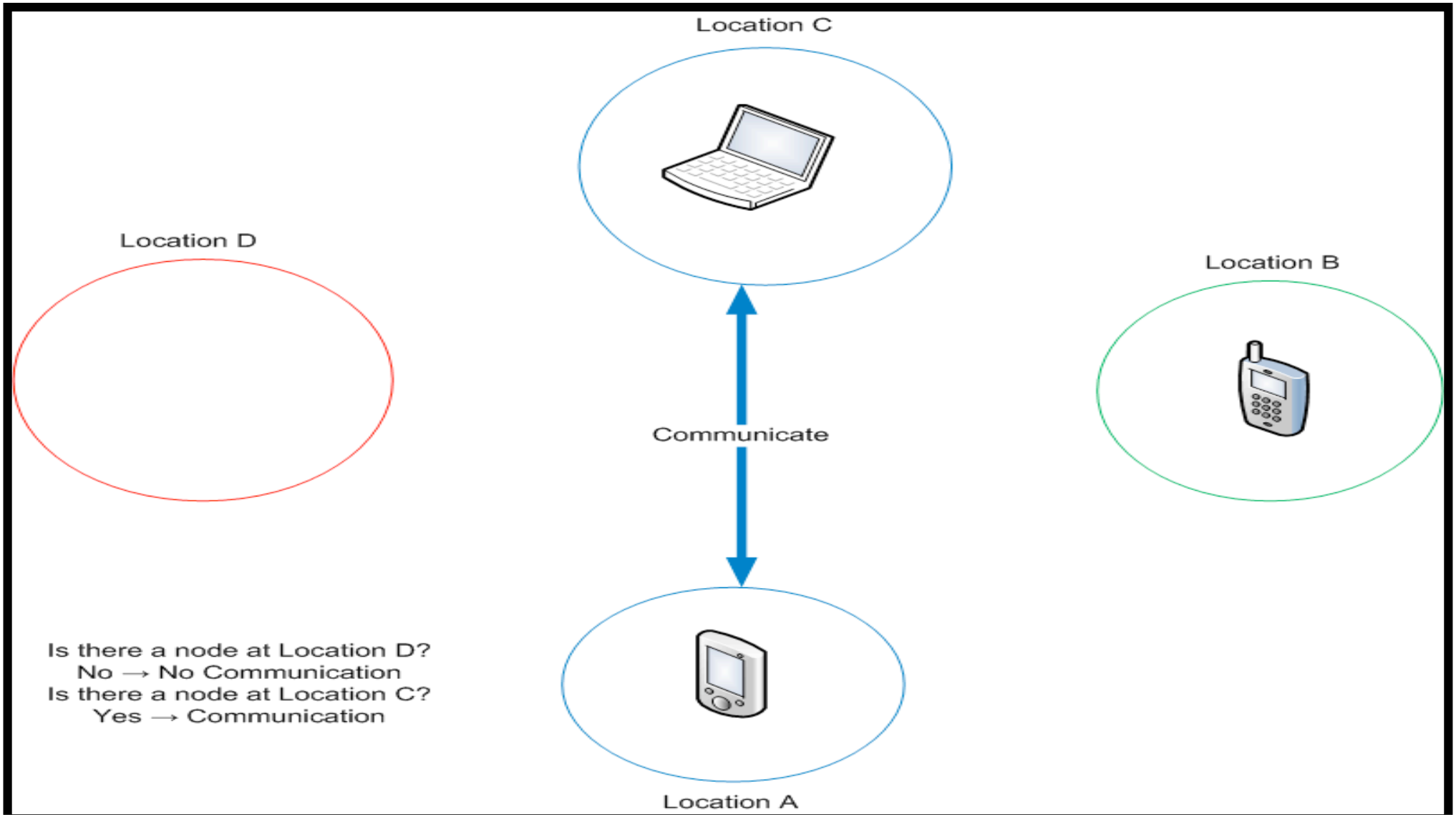
- Set of peer nodes
- Nodes move (but not too much)
- Nodes have unique names/addresses/IDs
- Routing protocols enable communication between a pair (or group) of explicitly named nodes



A different MANET setting:

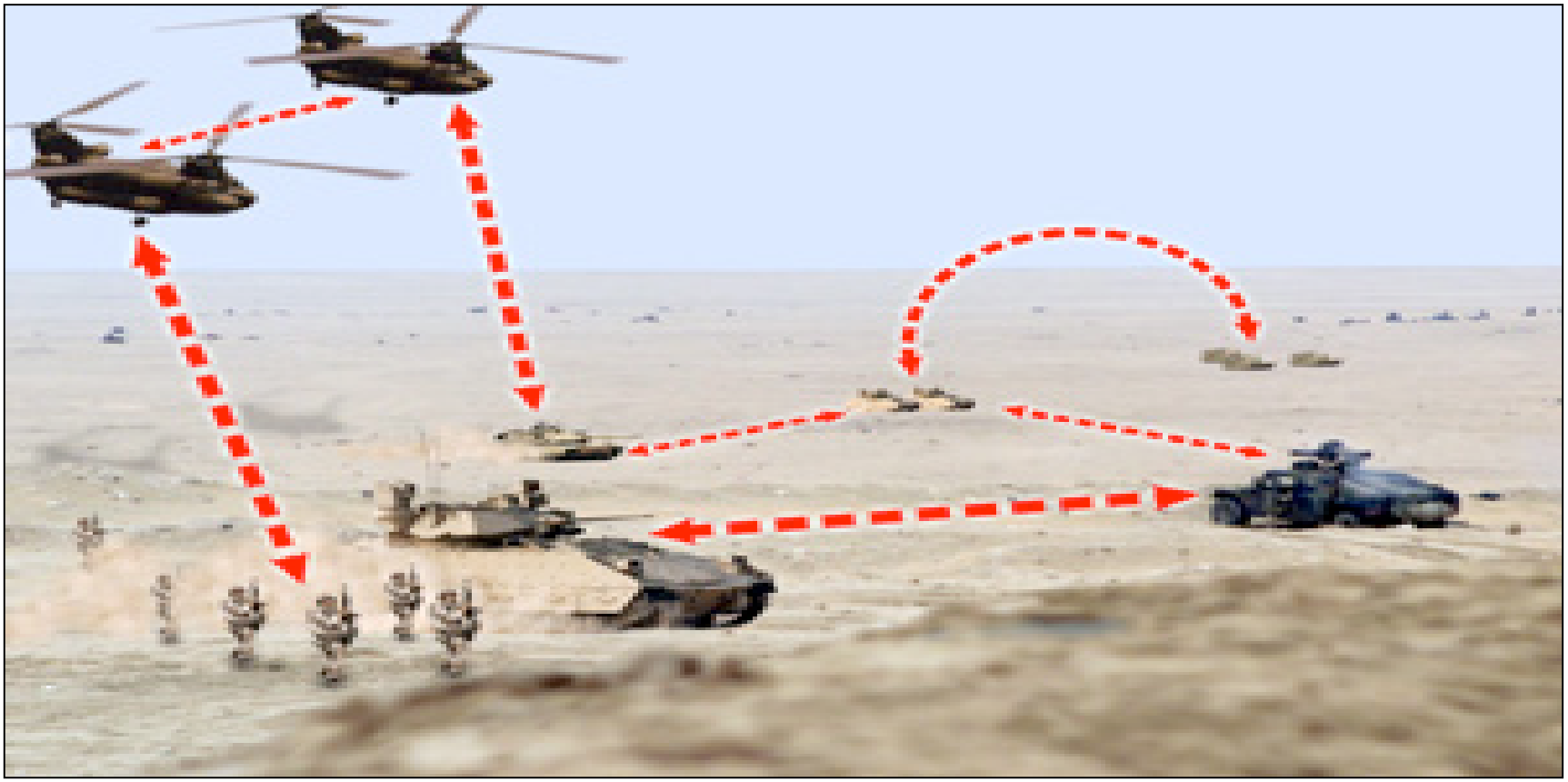
- Set of peer nodes
- Nodes move
- Communication between nodes is based on their locations (not on persistent identifiers)
- Node A makes a decision to communicate (or NOT) with node B based on the latter's current location
- Danger of insider/outsider attacks

Communication Decision



Examples:

- Military/battlefield: infantry, machinery, naval- and air-craft
- Law enforcement: sting operations, terror-attack/disaster aftermath



Basic Tenets

- [LOCATION] each node is equipped with a GPS or similar device
- [PRIVACY] no public node identity or address
- [MOBILITY] a certain minimum number of nodes move periodically $\Rightarrow$ tracking a node will require discerning it among a subset of nodes that moved
  - [SYNCHRONY]: common mobility followed by common rest
- [SECURITY]
  - all outsider attacks
  - passive (honest-but-curious) insiders

Whither reactive (on-demand) routing algorithms?

- Route discovery phase typically required in such protocols (e.g., AODV, DSR)
- No name or ID to send route discovery for…
- Can we do route discovery for a location?
- *Chicken-and-egg* problem: how can we initiate route discovery for a location, if we don't know whether any node(s) are there?

Distance Vector?

- How to build a DV table without IDs?
- Could build it based on location…
  - But need to prune it periodically (it'll get large!)
- Weak security: a single compromised node can poison everyone's DV table
- Slow convergence (folklore)

Link State?

- Let’s suppose that movement is “synchronized”, e.g. move-rest-move-…

- No need for route discovery: every node has the entire topology view
- Suitable for real-time communication
- Strong security: origin authentication and integrity can be easily achieved
- Scalability not the most pressing issue in many MANETS (100-s of nodes)

ALARM Framework

- Allows MANET nodes to communicate based on location
- Provides Anonymity, Authentication and Integrity
- Works with any location-aided routing scheme
- Group Signatures provide:
  - one-time pseudonyms
  - anonymous authentication of origin and data integrity
  - revocable anonymity
- Any group signature scheme can be used (unless protection against Sybil attack is needed)

Assumptions re-considered

- [LOCATION] node can securely and reliably obtain its present location (e.g. GPS)
- [TIME] nodes maintain loosely synchronized clocks
- [RANGE] nodes have uniform transmission range*
- [MOBILITY] at least *K nodes move at the same time*

** if nodes have different transmission range, an extra field will be needed in the messages, otherwise the framework is the same*

Group Signatures (GSIG)

- Any member in a potentially large and dynamic group can sign a message (produce a signature)
- Signature can be verified by anyone who has a constant-length group public key
- Valid signature implies that the signer is a *bona fide* group member
- Given two signatures, it is computationally infeasible to determine if they were signed by the same group member
- In the event of a dispute, a group signature can be opened to reveal actual signer

Group Signatures in ALARM

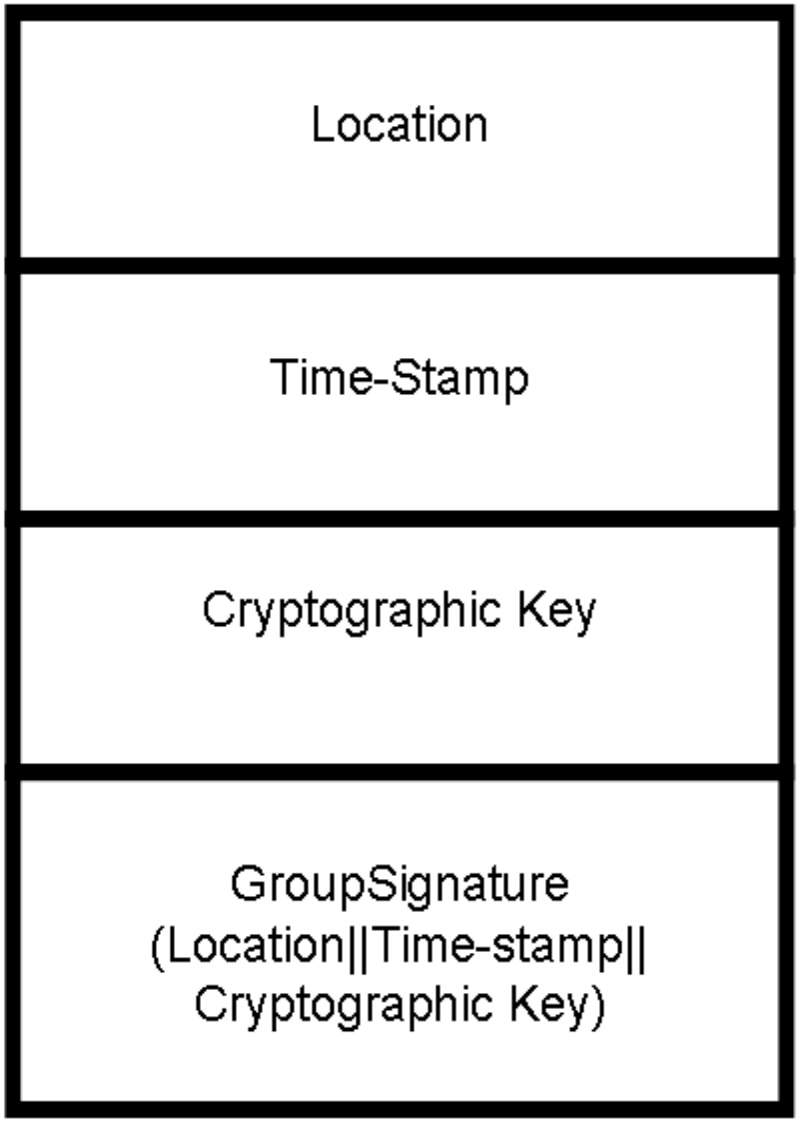
- A node generates a GSIG over its location update message
- Two location messages signed by same node can not be linked
- Anyone can verify that location message was produced by an authorized group member
- Assume an off-line (trusted) group manager who sets up the GSIG scheme

ALARM Sequence of Operation

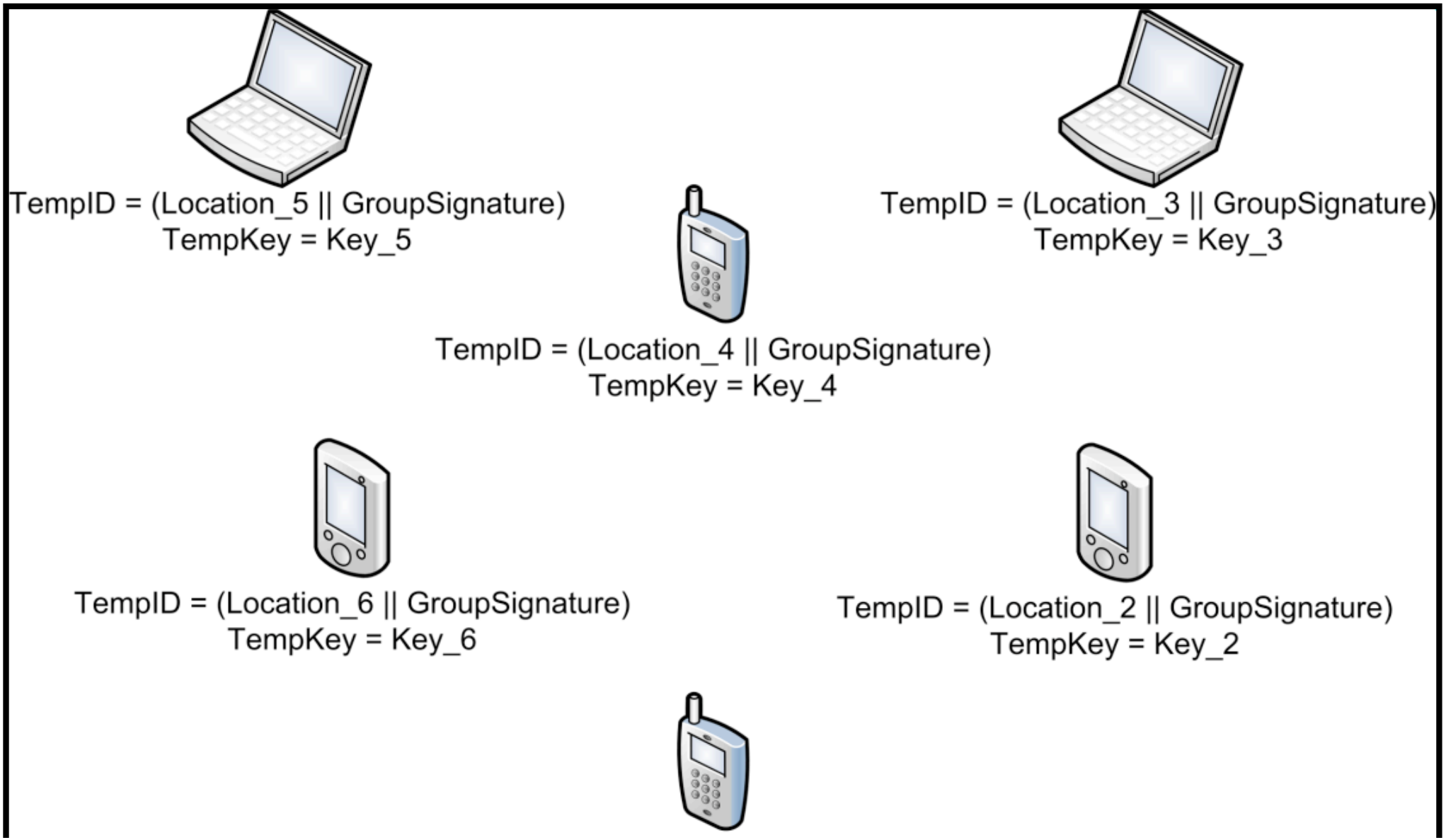
1. Each node periodically produces a location announcement message (LAM)
2. Broadcast LAM to immediate neighbours
3. LAMs flooded throughout the network
4. Each node receives all LAMs and constructs a map
5. A LAM GSIG serves as one-time identifier of the node at location specified in LAM
6. Ephemeral public key included in a LAM can be used to encrypt data to be transmitted later

Location Announcement Message (LAM)

- Location: current location of node
- Time-Stamp: current time-perid number (to prevent replays)
- Ephemeral Key: for encrypting data exchanged later (e.g., Diffie-Hellman half-key)
- Group Signature: provides authentication & integrity. Used as one-time pseudonym for node at that location.



Topology Example



Security (1)

Active/Passive Outsider:

- Records, replay messages or inject new messages
  - Replay attacks prevented due to LAM time-stamps
  - Injecting or modifying messages requires producing genuine GSIGs

Security (2)

Passive Insider (Honest-but-Curious):

- Eavesdrops on messages, wants to track peers nodes
  - Can't link two messages to same node (computationally infeasible to link two GSIGs)
  - Can track movement of node by monitoring likely trajectories
    - if node movement is random and *K nodes move within same period, attack not effective (simulation)*

Security (3)

Active Insider:

- Lies about other locations = creates phantom nodes with signed LAMs (Sybil attack)
  - Need to modify GSIG scheme to allow self-distinction
  - Has been done (FC'98, PET'06)
- Lies about own location
  - Need secure hardware…
  - Must contain GSIG Sign and GPS components

Average Node Privacy

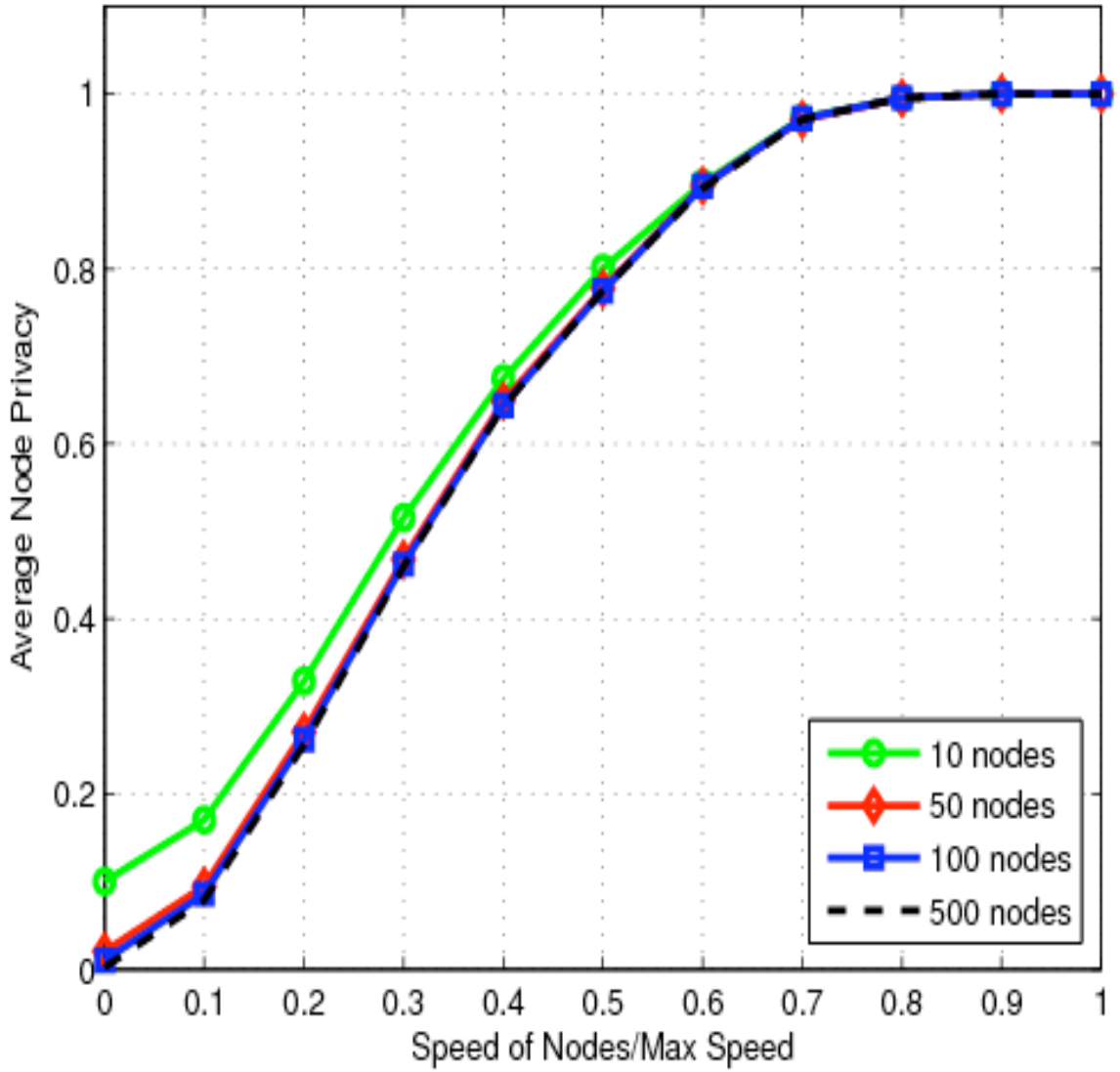
- One possible metric capturing node privacy
- Determines node fraction to which a node can be mapped between two successive topology snapshots

$$AverageNodePrivacy = \sum_{i=0}^{i=K} (K - K_i^{'})/K^2$$

- *K = total number of nodes*
- $K_i^{'}$ *= number of nodes to which i can't be mapped*

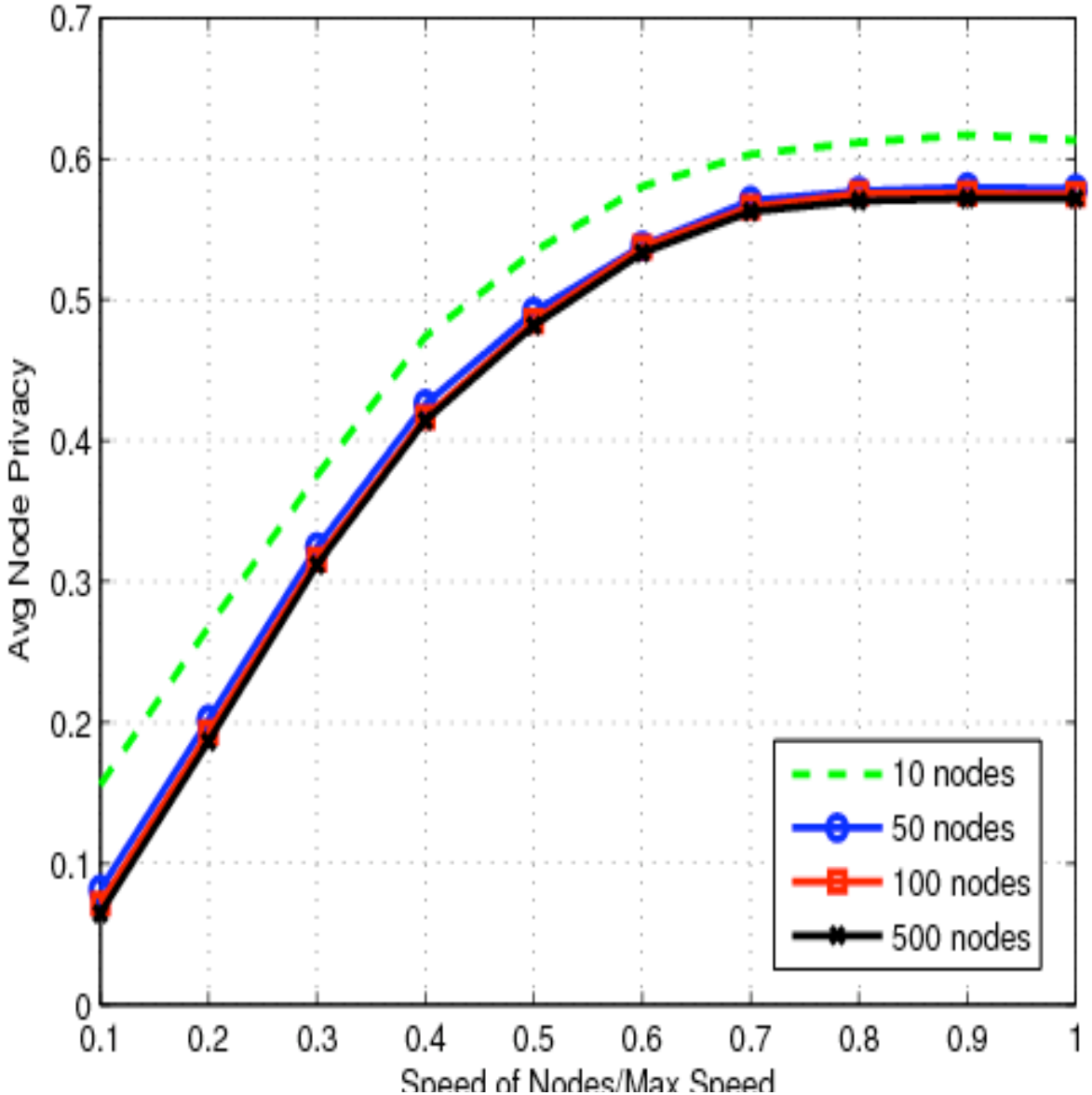
Simulation Results

- All nodes move
- Random Walk Mobility
- 1km*1km area
- Max speed = 1.4km/ period between 2 LAMs



Simulation Results

- All nodes move
- Random Way Point
- Nodes stop with probability (0.5) for duration of 2 LAMs
- 1km*1km area
- Max speed = 1.4 km/ period between 2 LAMs



Future Work

- Analytical Model for Privacy
- Adapting to path vector?
- Evaluation with “real” MANET traces
  - unsurprisingly, military traces hard to come by…