Using Predictable Mobility Patterns to Support Scalable and Secure MANETs of Handheld Devices

David R. Bild[†], Yue Liu[†], Robert P. Dick[†], Z. Morley Mao[†], and Dan S. Wallach[‡]

[†]EECS Department
University of Michigan
Ann Arbor, MI 48109, USA

[‡]Department of Computer Science
Rice University
Houston, TX 77005, USA

MobiArch
June 28, 2011

Proposed System

A MANET architecture for censorship-resistant and secure text-based personal communication among friends and family.

Proposed System

Introduction should answer Why...

A MANET architecture for censorship-resistant and secure text-based personal communication among friends and family.

Proposed System

Introduction should answer Why...

A MANET architecture for censorship-resistant and secure text-based personal communication among friends and family.

Proposed System

Introduction should answer Why...

A MANET architecture for censorship-resistant and secure text-based personal communication among friends and family.

Proposed System

A MANET architecture for censorship-resistant and secure text-based personal communication among friends and family.

Caveats

Requires connectivity, so we're targeting densely populated areas (cities, towns, etc.) for local communication.

Proposed System

A MANET architecture for censorship-resistant and secure text-based personal communication among friends and family.

Caveats

Requires connectivity, so we're targeting densely populated areas (cities, towns, etc.) for local communication.

Interesting Technical Aspects

- Use the predictability of human motion to reduce routing costs.
- Adapt mix-nets to provide location privacy in MANETs using location-aided routing.

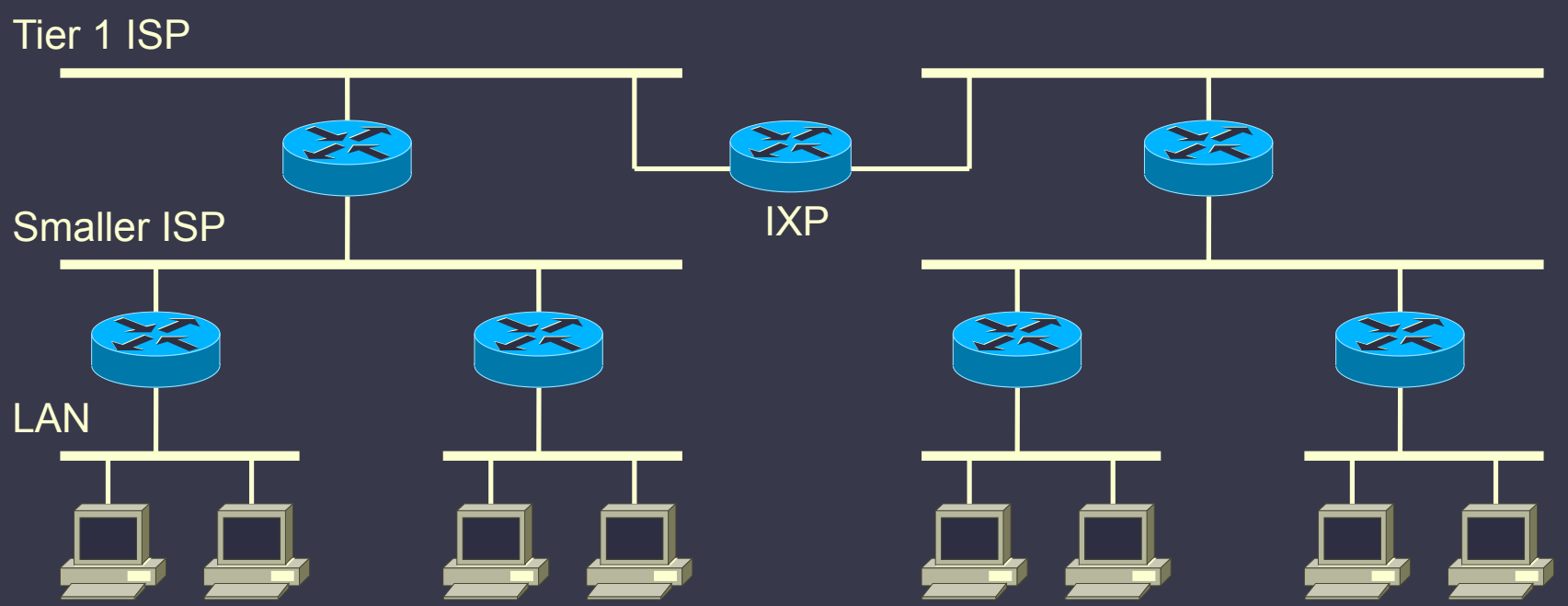
Internet Hierarchy Facilitates Censorship

Old Wisdom

"The Net interprets censorship as damage and routes around it."

—John Gilmore, 1993

Reality



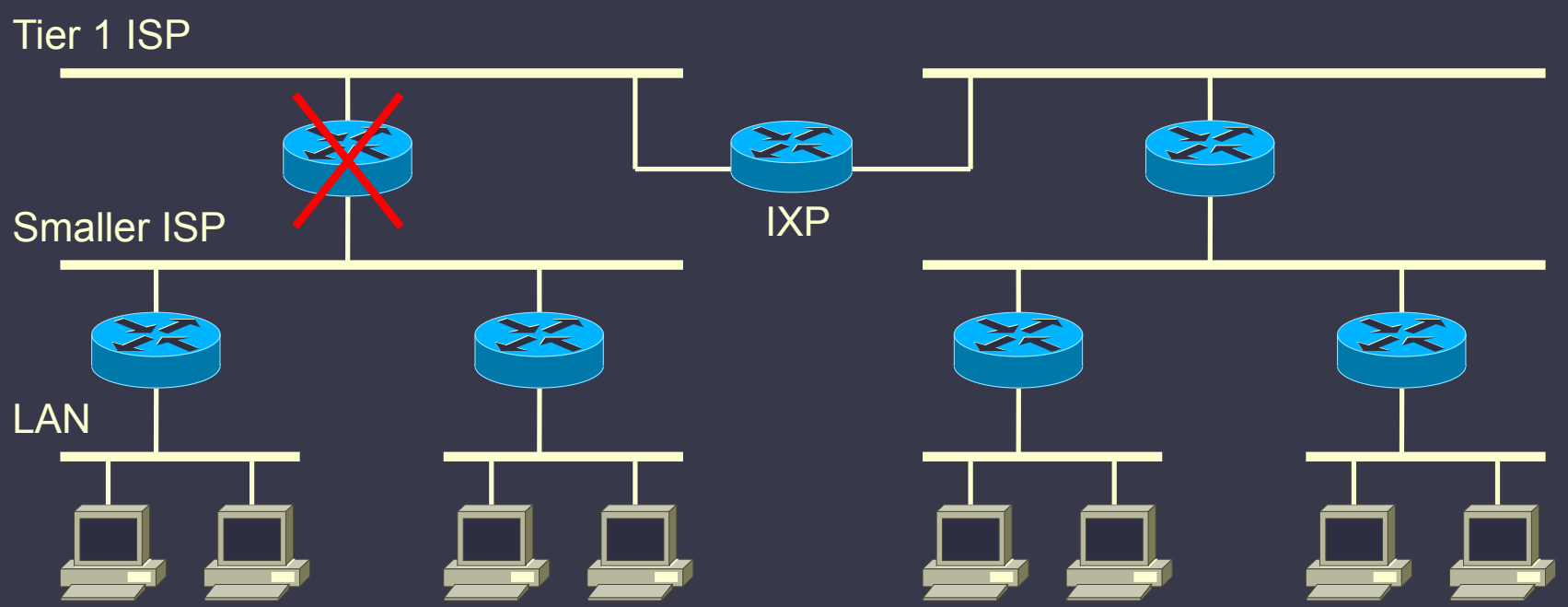
Internet Hierarchy Facilitates Censorship

Old Wisdom

"The Net interprets censorship as damage and routes around it."

—John Gilmore, 1993

Reality



Not Just a Hypothetical Concern

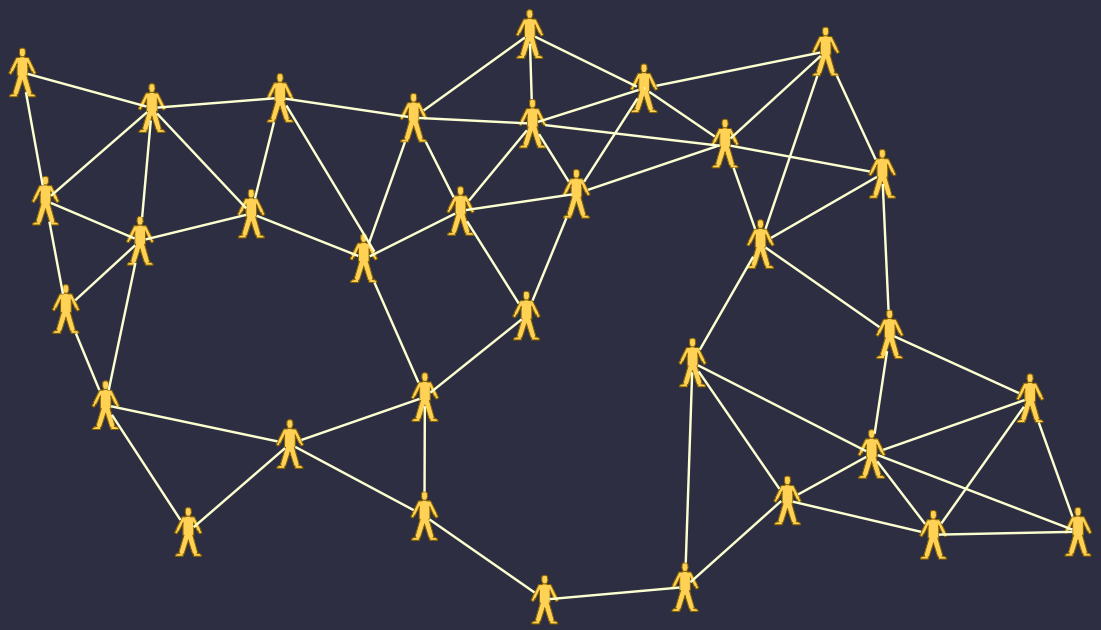
These hierarchy-induced choke-points have been used to take censorship to the extreme.

Recent Shutdowns

- Jan. 2011 — Egypt
- March 2011 — Libya
- June 2011 — Syria

Lose the Hierarchy

We envision non-hierarchical MANETs as a more robust *supplement* to the Internet.

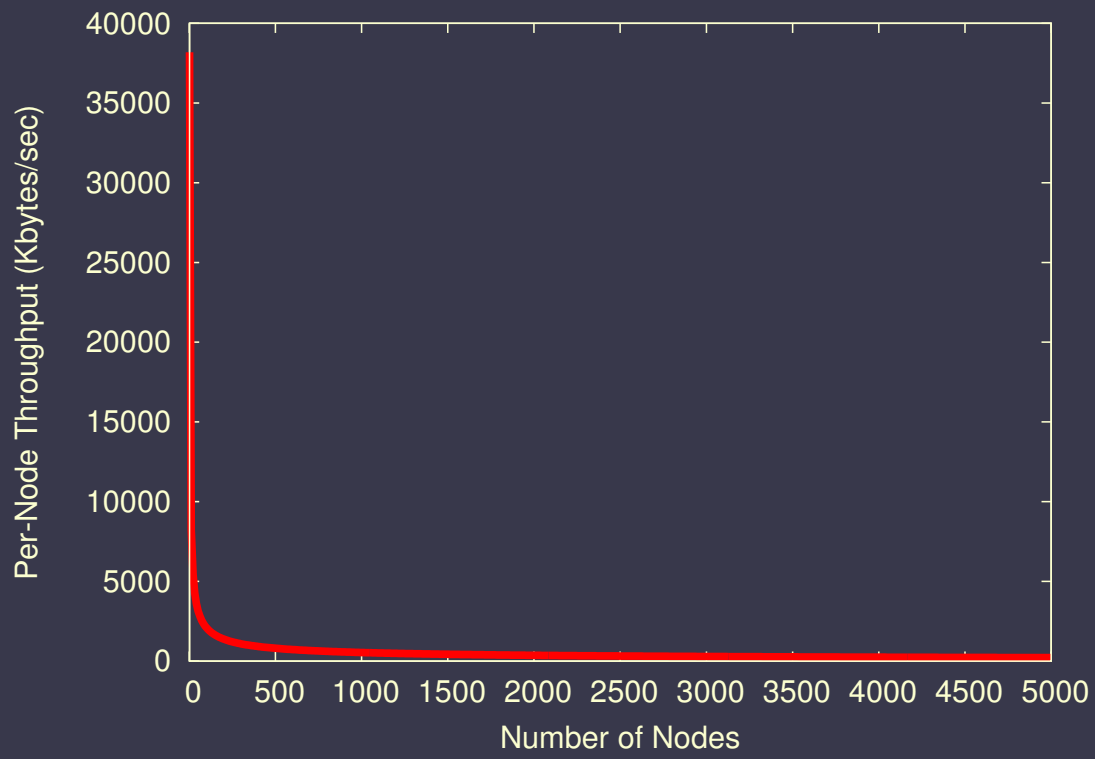


- Censorship would require controlling many nodes in the network.
- Mobility prevents long-term choke-points from arising.

Two Major Scalability Problems

Two scalability problems prevent a general-purpose MANET-based supplement.

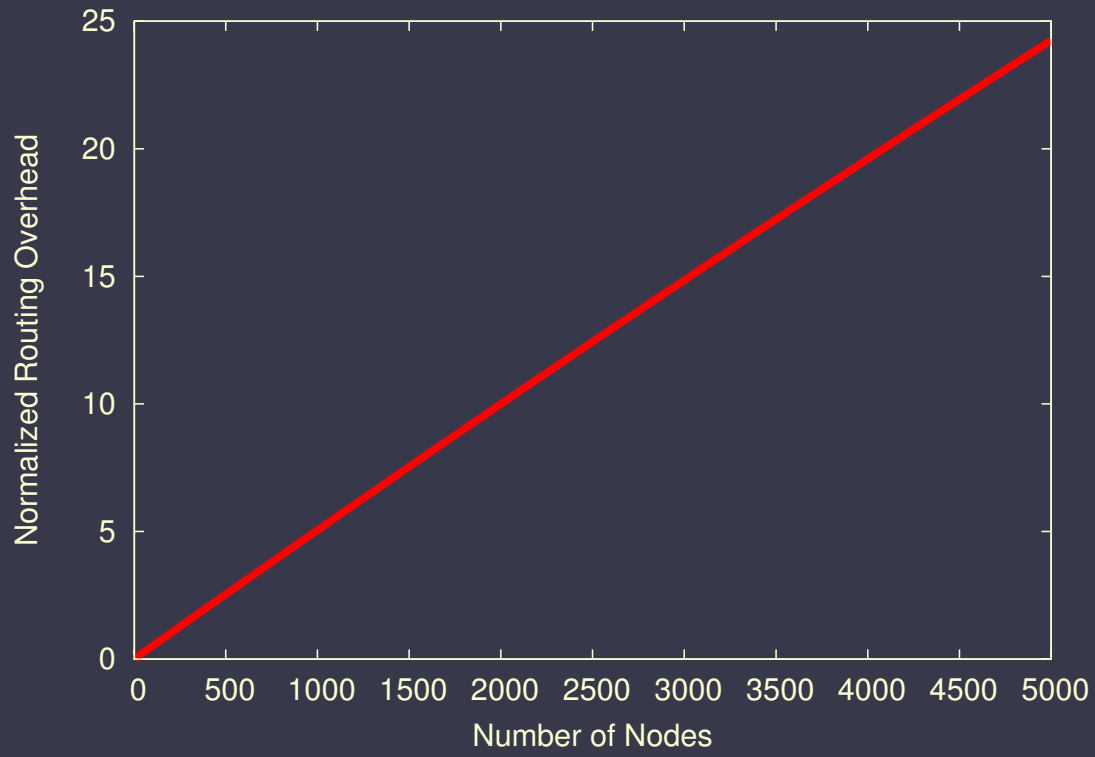
Per-node throughput decreases with network size



For unit-disc transmission model from F. Xue and P. Kumar, 2006.

Two Major Scalability Problems

Routing maintenance increases with network size



For XYLS Location Service. Data from S.M. Das, H. Pucha, and Y.C. Hu, 2005.

Implication: Tailor Architecture to Application

Throughput Scaling

Throughput and latency must be acceptable at desired network size.

Routing Overhead

Leverage properties of the application to improve routing efficiency.

Text-Based Personal Communication Application

Text-based personal communication is well-suited to a MANET.

Properties Helpful for Throughput

- Low per-node bandwidth (e.g., bps, not Kbps).
- High latency is acceptable (e.g., several seconds).
- Much communication is with nearby contacts.

Properties Helpful for Routing

- Human motion is highly predictable.
- Motion patterns change infrequently.
- Much communication is with few contacts.

Censorship-Resistance, not Shutdown-Resistance

Primary Goal

Censorship-resistant and secure (reprisal-resistant) communication for *day-to-day* use.

Handling Shutdowns Useful as Well

Our system will work to the extent that locations are still predictable.

System Features

Scalability: 10,000–20,000 nodes. A small town or university campus.

Confidentiality: Public key cryptography. Key distribution is done face-to-face.

Location Privacy: Prevent others from linking past, current, and future locations, even while employing location-based routing.

Social Network Privacy: Hide participants in conversations, not just contents of conversations. Necessary for reprisal-resistance, a part of censorship-resistance.

Distributed Location Services

Location-aided routing with a distributed location service is scalable, but not scalable enough.

Routing Algorithm

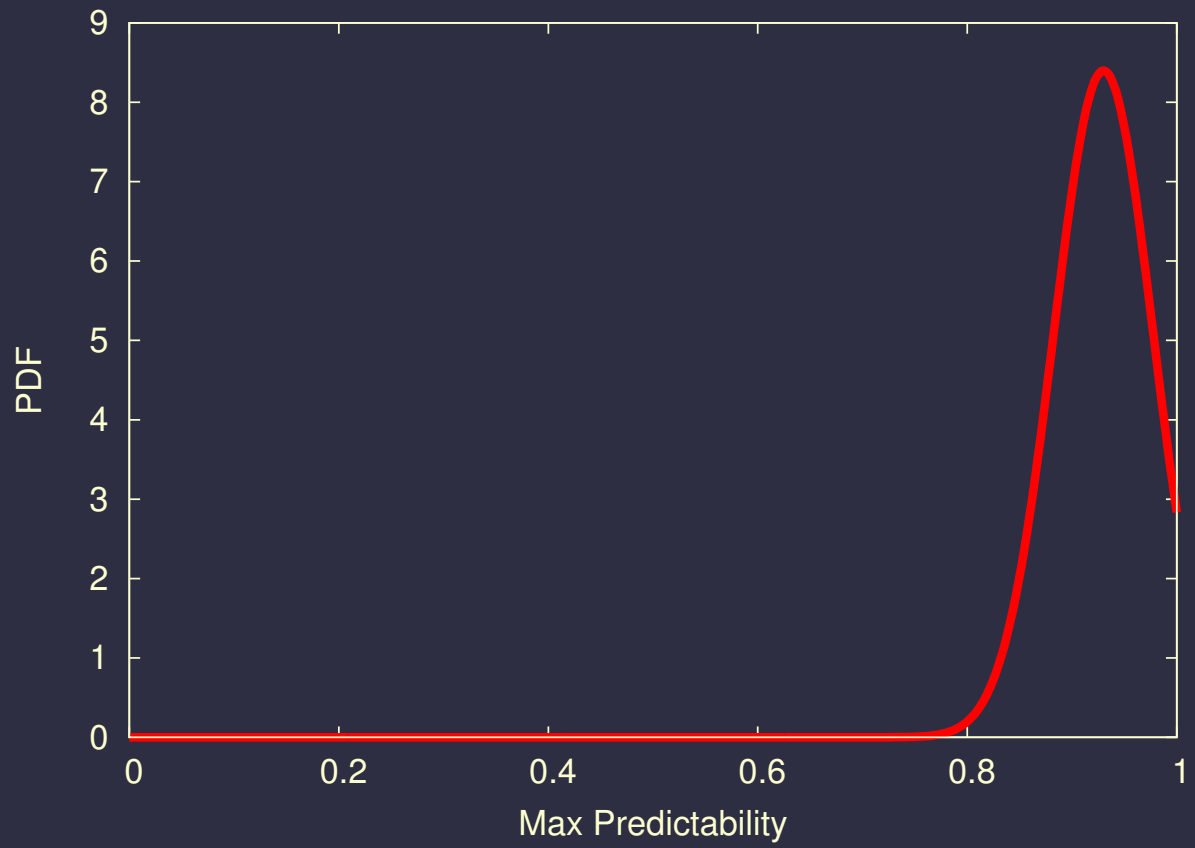
Location-Aided Routing (e.g., GPSR).

Problems with Distributed Location Services

- Update costs increase with network size and mobility.
- Query costs increase with network size and query frequency.
- Supporting anonymous queries is complex.

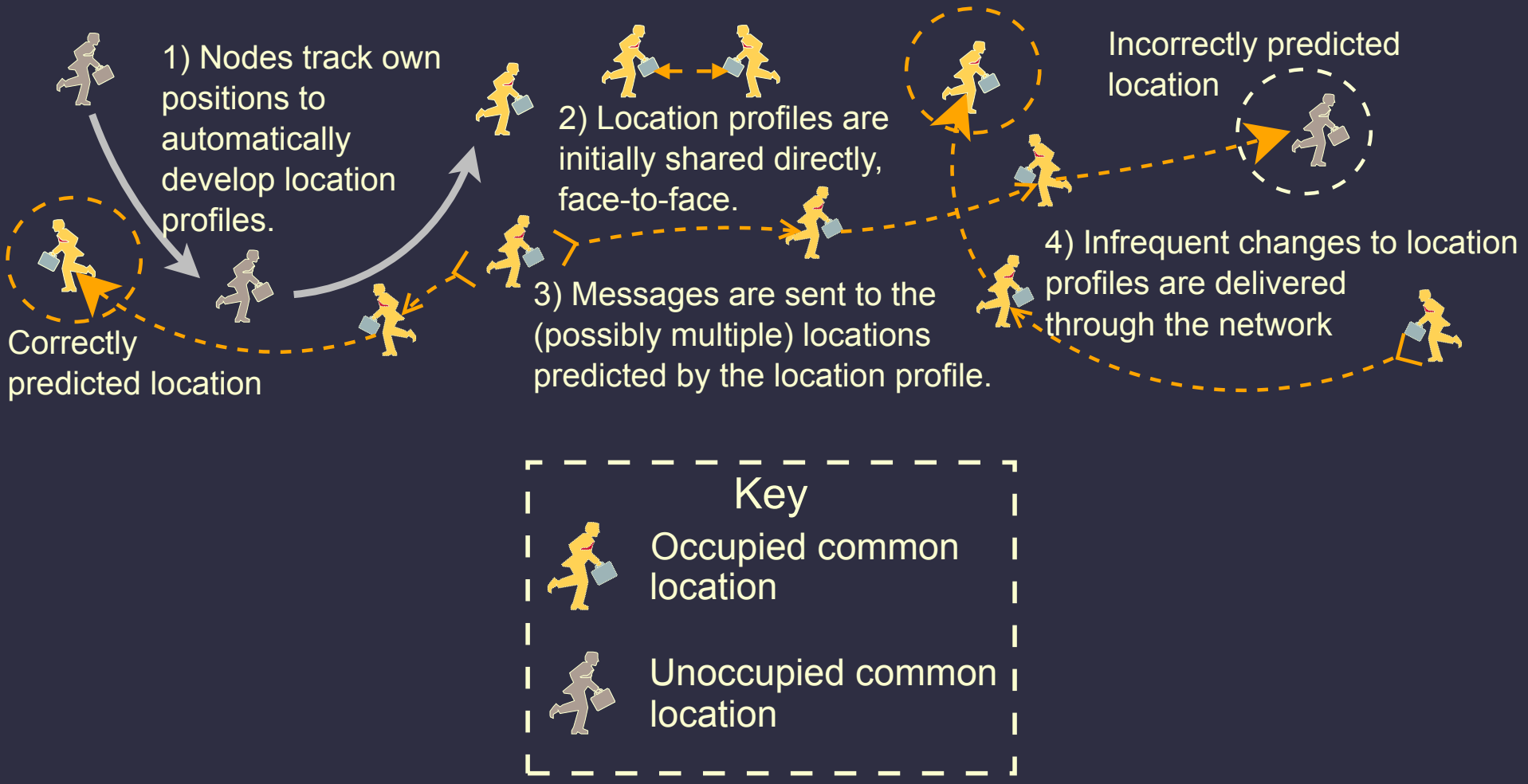
Predictability of Human Motion

For most users, location is predictable at least 80% of the time.



From C. Song, Z. Qu, N. Blumm, A.L. Barabasi, 2010.

Location Profiles



Components

Location Profiles

Specifies (location,confidence) tuples given some public information (e.g., time-of-day, day-of-week, etc.).

Profile Distribution Method

Face-to-face, initially. Updates face-to-face or through network.

Addressing Policy

Message delivery strategy. Affects energy-latency tradeoff.

Fallback Method

Not our focus, but delayed delivery and rendezvous delivery are options.

Pseudonyms

Location Profile Aided Routing has Poor Precision

Near the destination, route using AODV and per-location pseudonym addresses.

Privacy and Anonymity Motivation

MANETs are open to untrusted observation and participation.

Censorship-resistance implies reprisal-resistance.

Attacker Model

Attackers may...

- Participate in the network.
- Observe all links.
- Have large storage and processing capabilities.
- Triangulate positions of nodes.

Economics dictate that

Conforming nodes will outnumber attackers.

Desired Anonymity and Privacy

Prevent linking of multiple attributes of a node

- location–location *(location privacy)*
- identifier–identifier *(social network privacy)*
- action–location
- action–identifier
- action–action
- identifier–location

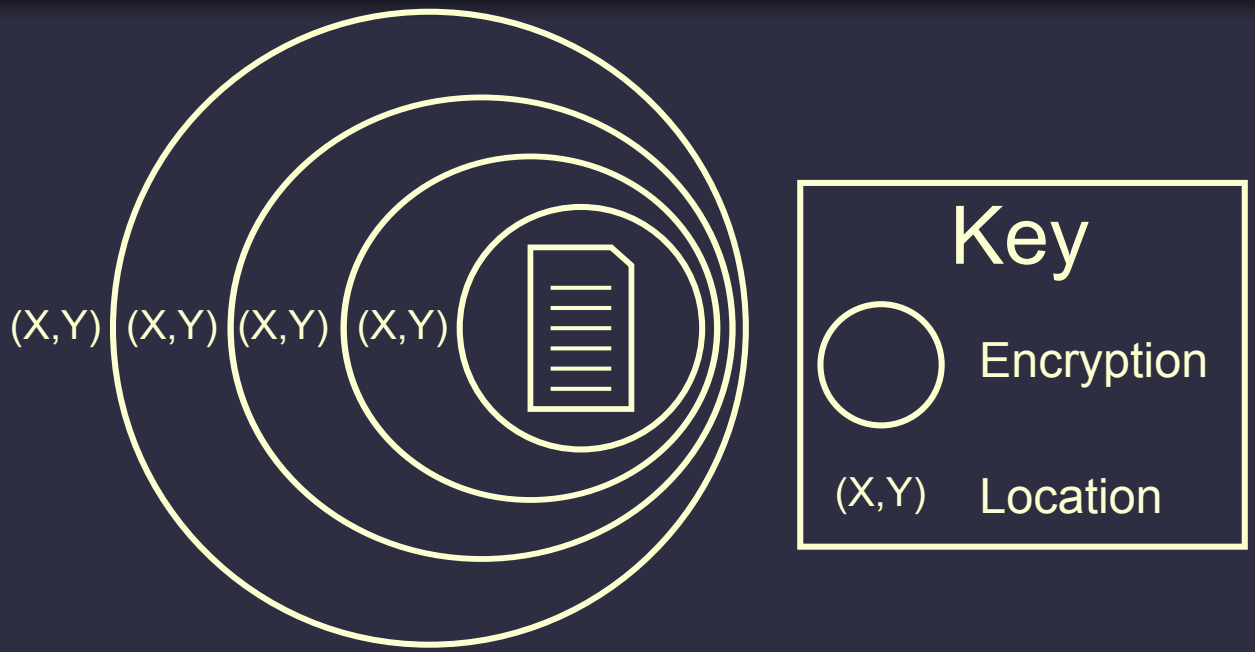
Protecting These Relationships

Two attributes are unlinkable if:

1. Both are never available in the same context.
2. Transitive application of known relationships cannot link them.

Reply Block

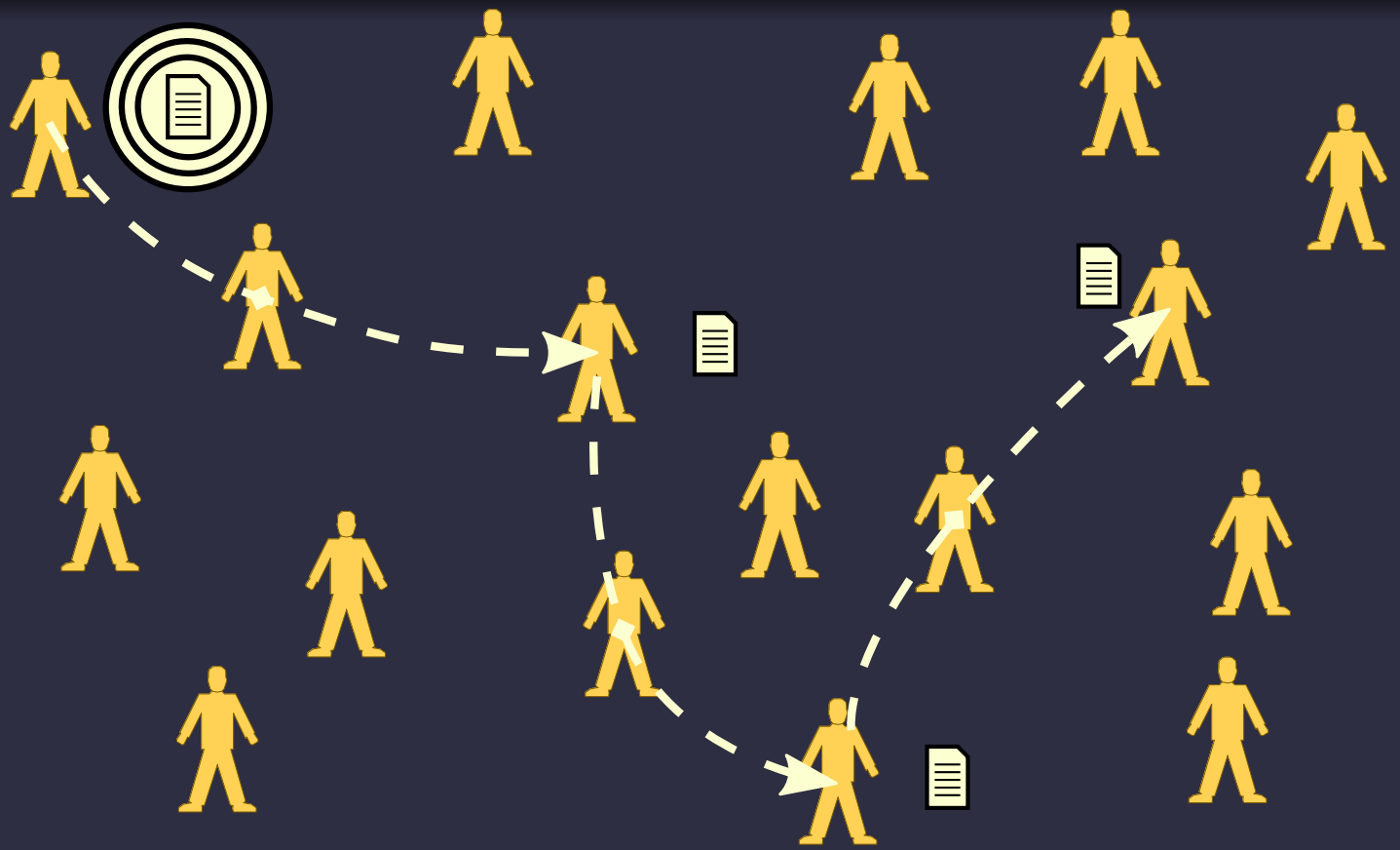
The destination contact layers encryption around its location before sharing with its contacts, preventing the sender from seeing the actual location.



D.L. Chaum, *Comm. ACM,* 1981

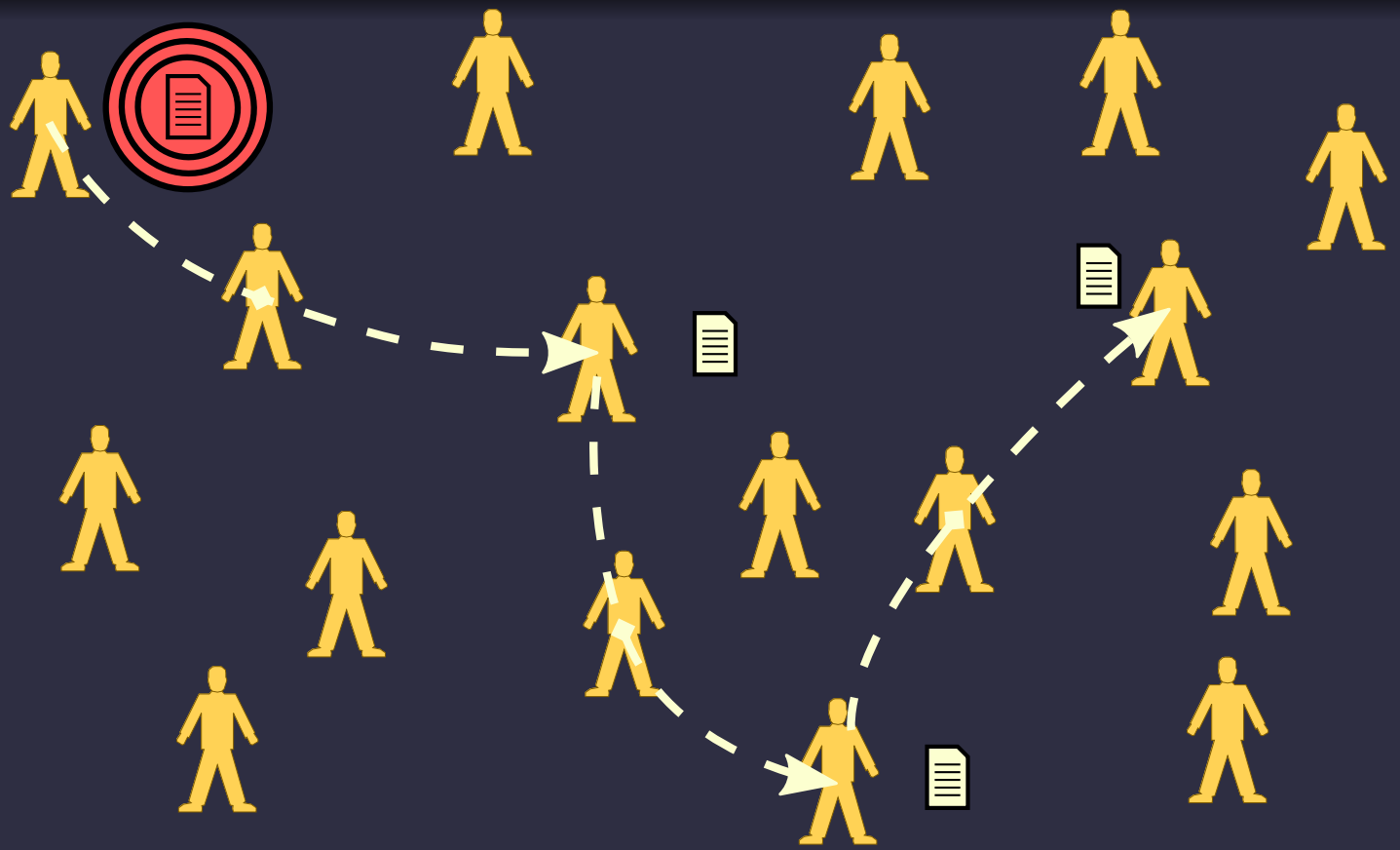
Mix-Chain

A message is routed to the locations specified in the reply block, a new location revealed at each hop, until finally reaching the destination.



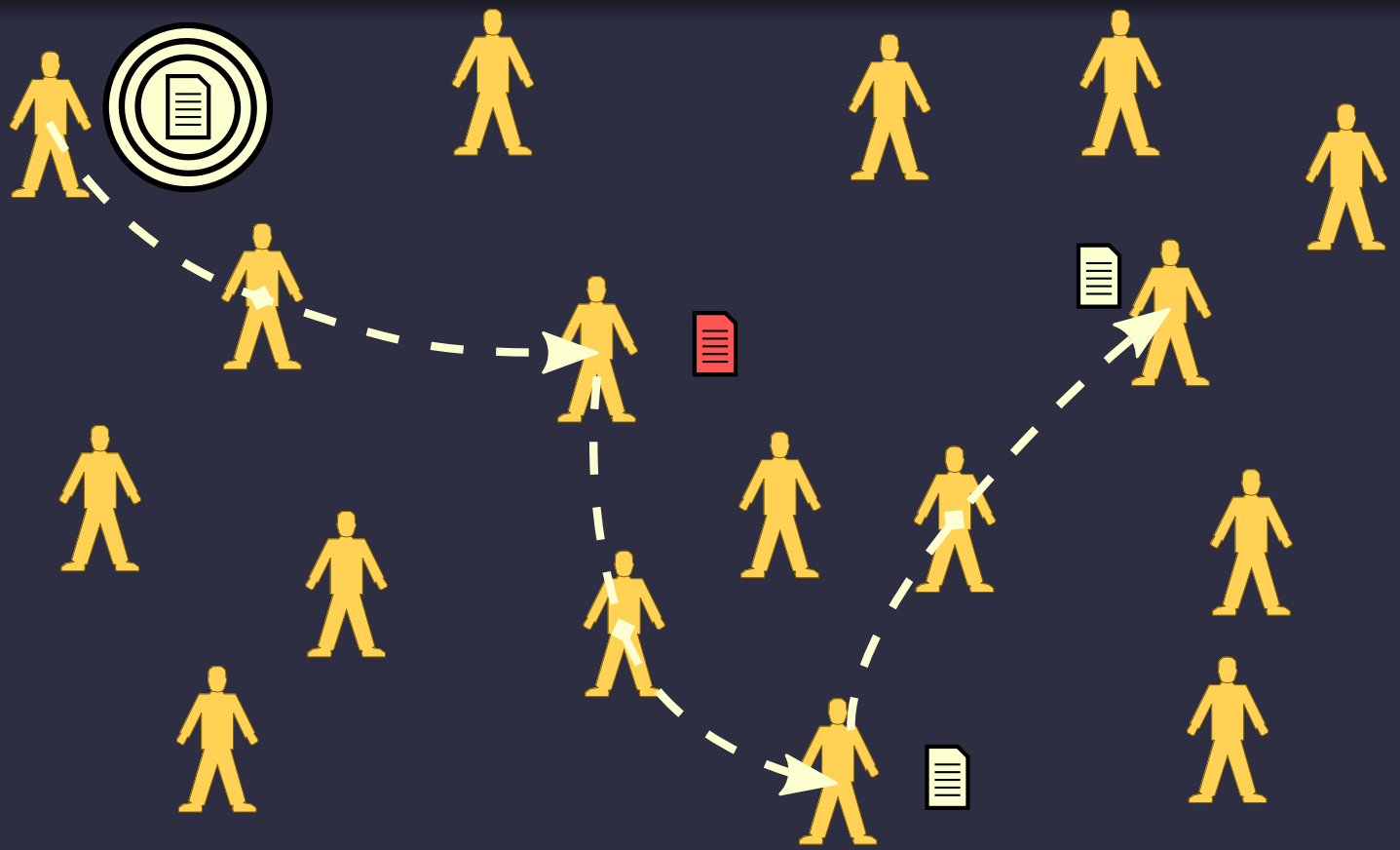
Mix-Chain

A message is routed to the locations specified in the reply block, a new location revealed at each hop, until finally reaching the destination.



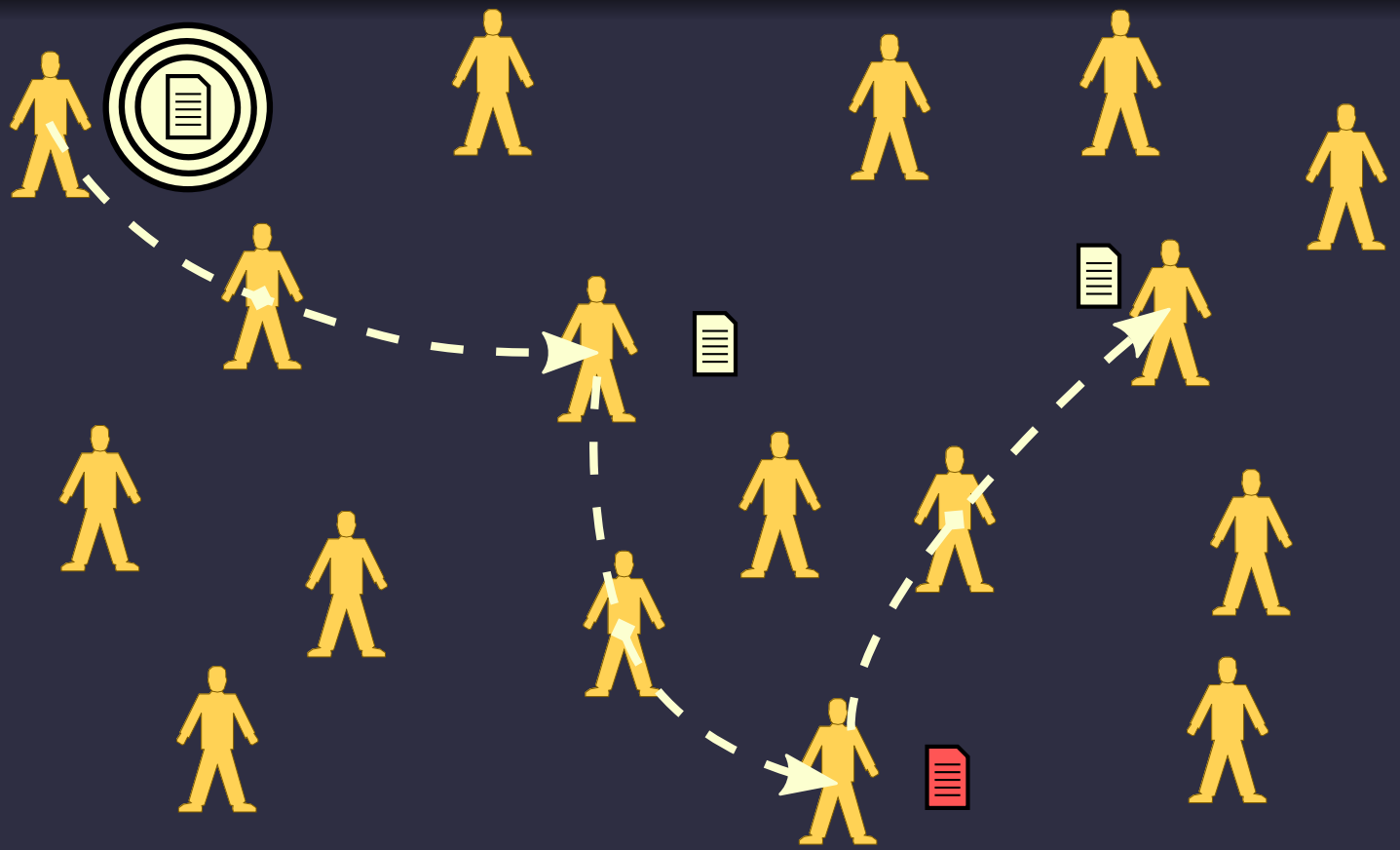
Mix-Chain

A message is routed to the locations specified in the reply block, a new location revealed at each hop, until finally reaching the destination.



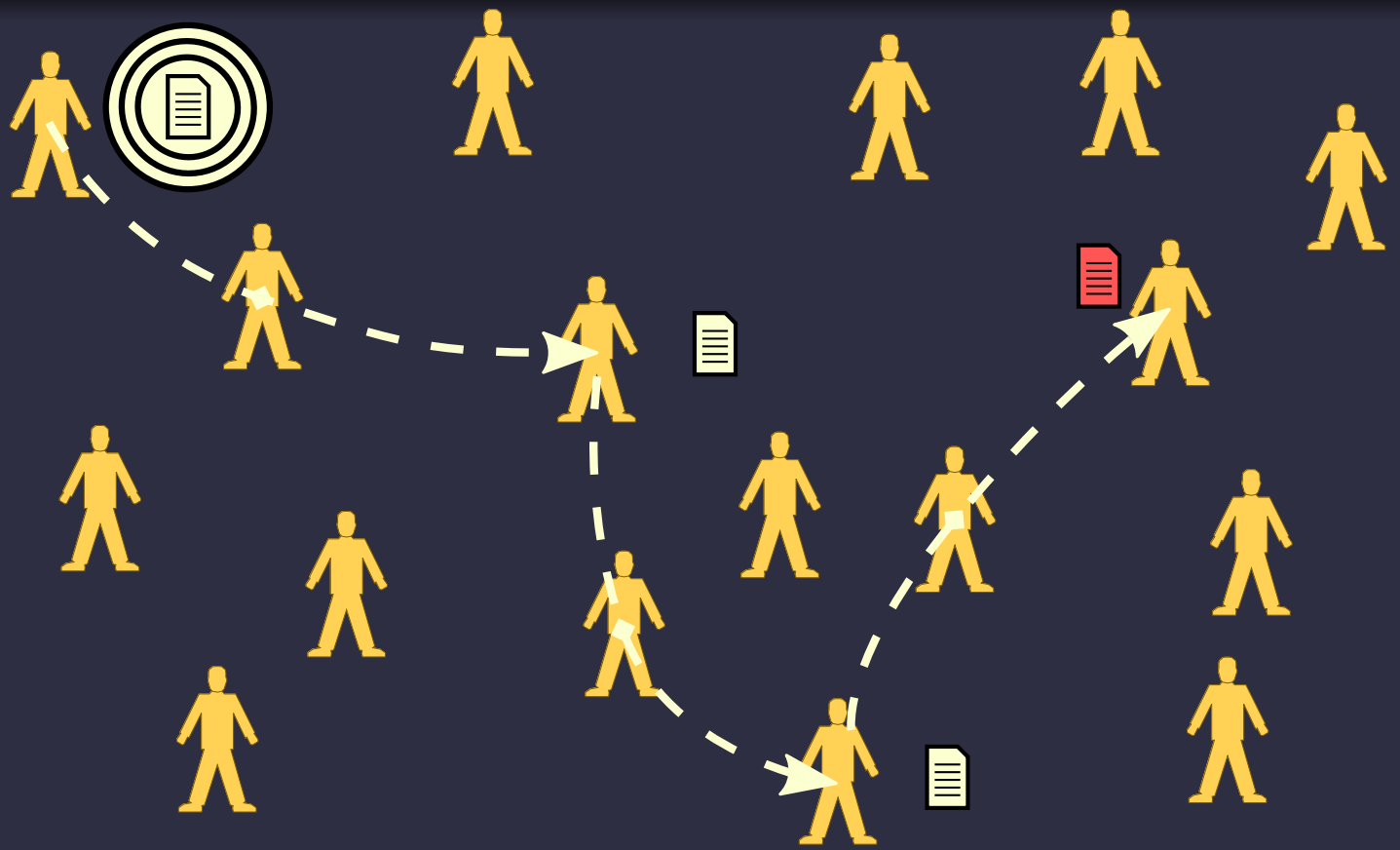
Mix-Chain

A message is routed to the locations specified in the reply block, a new location revealed at each hop, until finally reaching the destination.



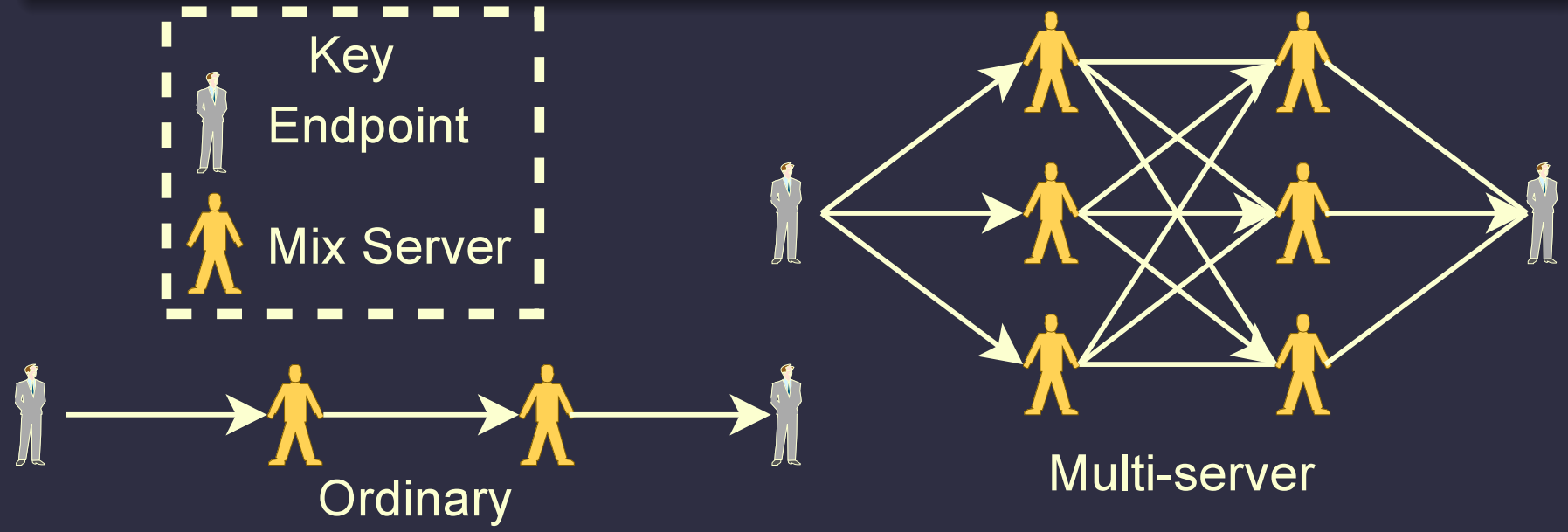
Mix-Chain

A message is routed to the locations specified in the reply block, a new location revealed at each hop, until finally reaching the destination.



Reply Block Operation

With significant probability, one of the intermediate nodes will not be in its predicted location. So we increase reliability by including redundant nodes at each level of the mix-chain.

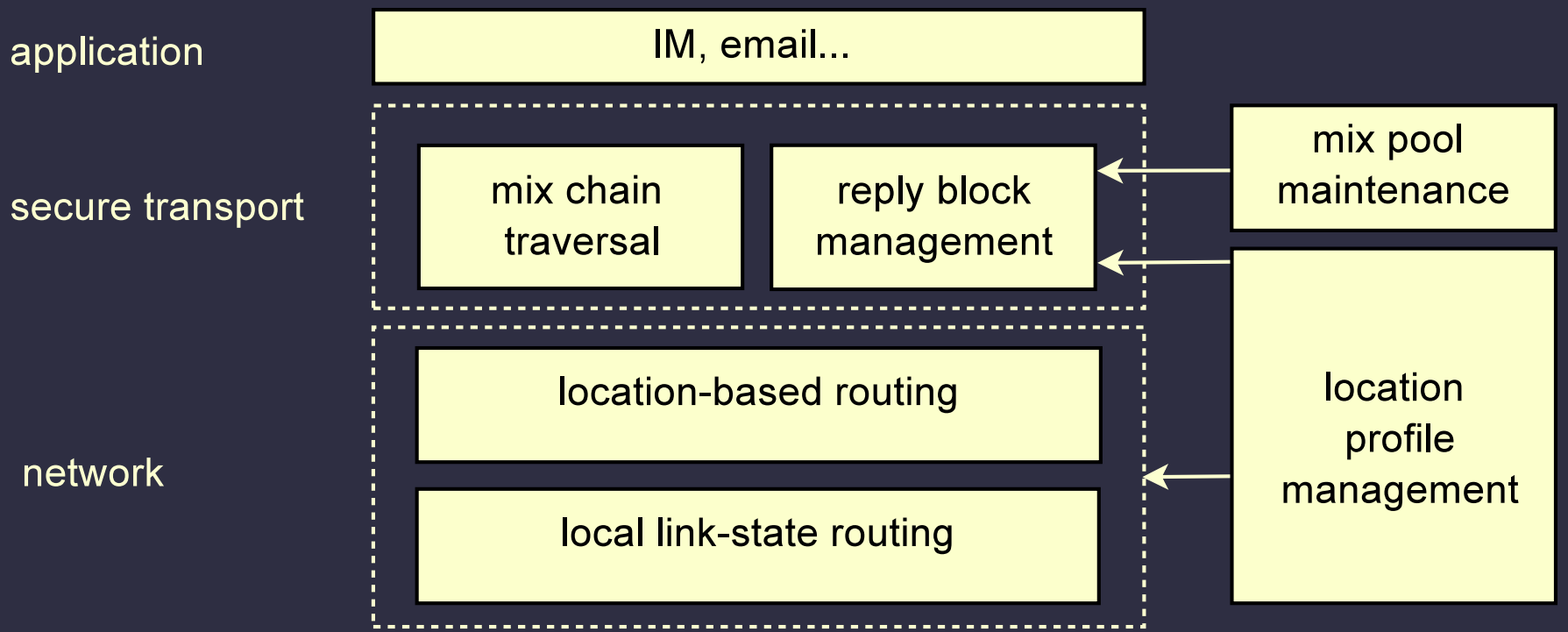


Mix Pool Management

Nodes randomly select one-hop neighbors for mix-pool inclusion.

As reply blocks age, they must be updated and redistributed.

Location-Centric Network



Summary

Goal

A MANET architecture for censorship-resistant and secure text-based personal communication among friends and family.

Architecture Takeaways

- Leverage the predictability of human motion to reduce routing overhead.
- Employ reply-blocks/mix-chains to get location privacy.

Thank You

Questions?