Fine-grained Encountering Information Collection under Neighbor Anonymity in Mobile Opportunistic Social Networks*

Kang Chen[1] and Haiying Shen[2]

[1]Dept. of ECE, Southern Illinois University, IL, USA

[2]Dept. of ECE, Clemson University, SC, USA

* Work was done when at Clemson

Outline

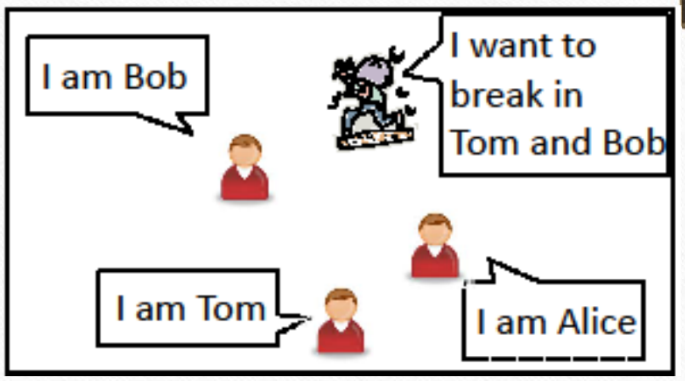
- Introduction
- System Design
- Performance Evaluation
- Conclusion

Introduction

- Mobile Opportunistic Social Networks (MOSNs)
  - Consisted of mobile devices carried by human
  - Rely on direct peer to peer short range communication, e.g., WiFi Ad hoc
    - Opportunistic communication sessions due to mobility
  - Special form of delay tolerant networks (DTNs)
  - Communication among devices reflect the encountering of human
  - Support proximity-based applications

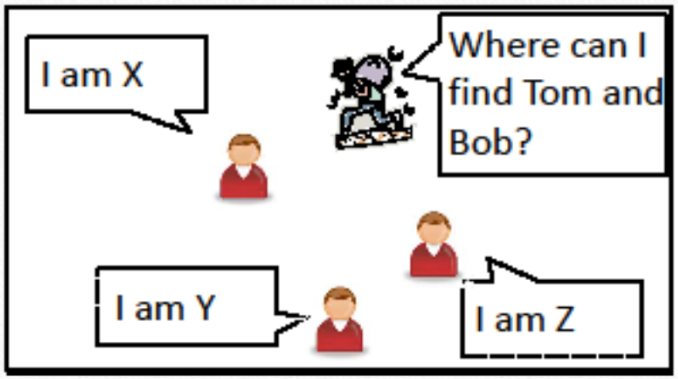
Introduction

- By default, in MOSNs
  - Each node has an ID in the network, denoted real ID
  - Nodes communicate with neighbor nodes using their real IDs
- We have a security and privacy concern
  - Easier for a malicious nodes to identity attack targets
  - Expose encountering information to others



Introduction

- Anonymity is a solution
  - Nodes use a constantly changing pseudonym
  - Can hide nodes from attackers
- But blocks proximity-based applications
  - Nodes need to know whom they have met for
    - Identifying social relationships
    - Deducing future encounter possibilities
    - Receiving files/messages



Introduction

- The problem we are facing
  - **Anonymity** is good to protect nodes
  - Anonymity is also not desired for **encountering information collection**
- Any solutions to get the situation reconciled?
  - Observation: Nodes communicate only when they meet, so do the attacks
  - Hint 1: Attackers cannot attack separated nodes in MOSNs
  - Hint 2: Anonymity is only necessary when nodes are in contact
  - Solution: Collecting the encountering information after two nodes separate