Persistent Personal Names for Globally Connected Mobile Devices (UIA)

Bryan Ford, Jacob Strauss, Chris Lesniewski-Laas, Sean Rhea, Frans Kaashoek, Robert Morris
Massachusetts Institute of Technology

Presented by: Linguang Zhang

COS518

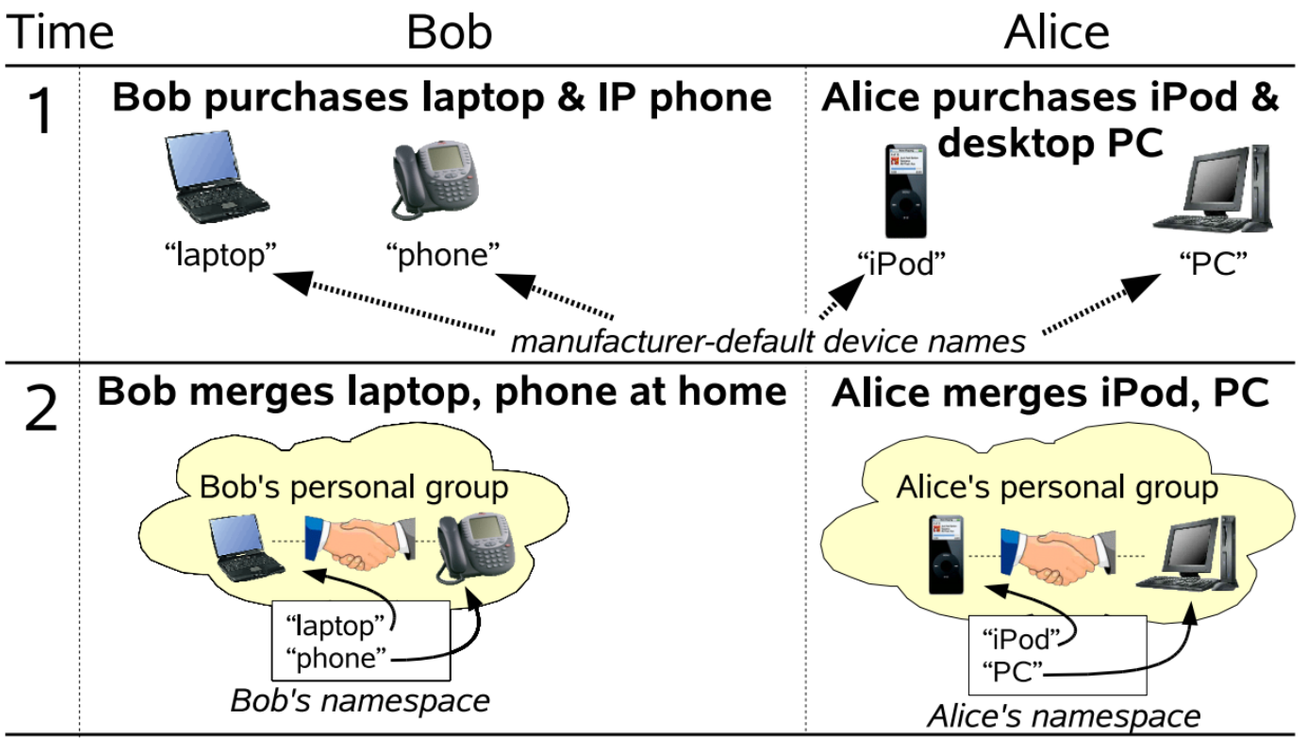
Motivation

- Global communication usually requires the target device to have:
  - a global name
    - *but* users need to register with central authorities.
  - static, public IP address
    - *but* mobile devices often have dynamic IP addresses

Central Ideas

- Unmanaged Internet Architecture
  - UIA provides zero-configuration connectivity via personal names.
  - Simple and intuitive usages.
  - Devices can be arbitrarily named and merged into personal groups.
  - Routing exploits user’s social network.

User Experience



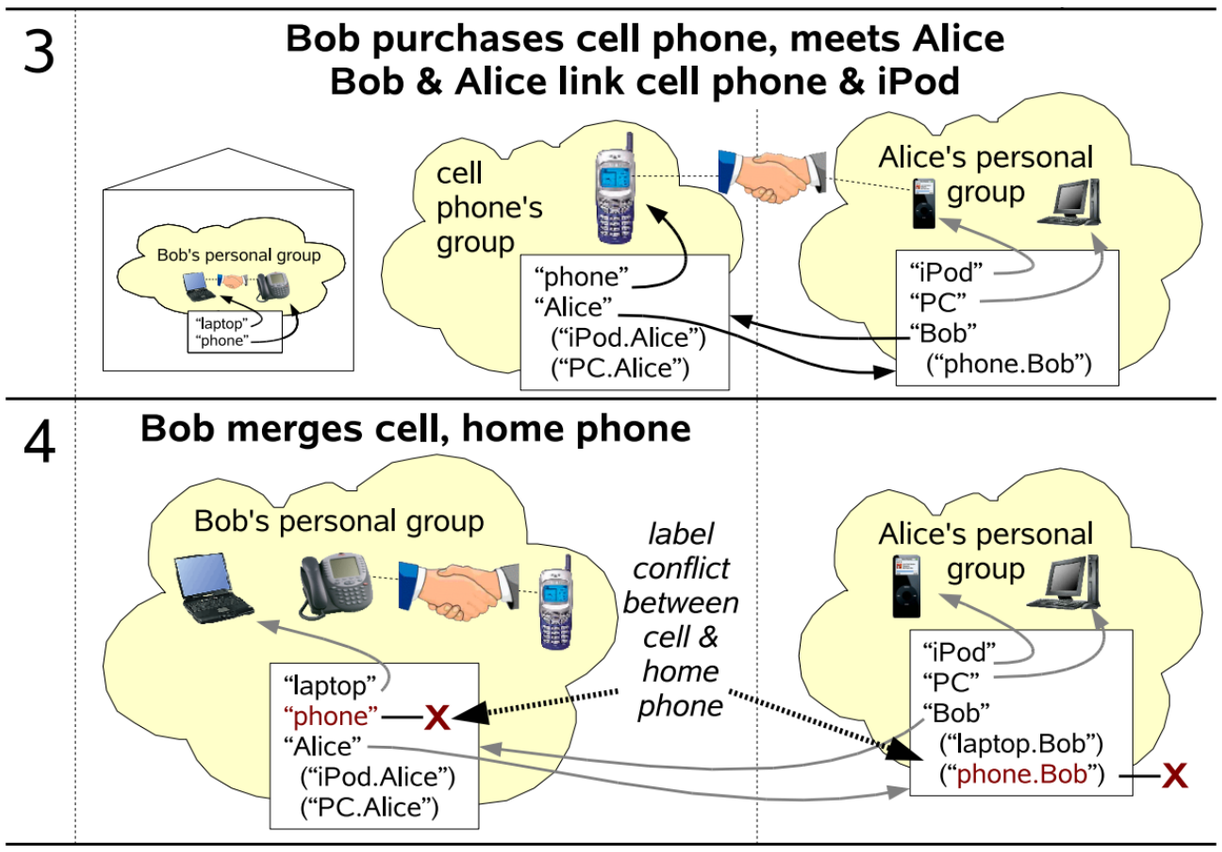
Device initialization

Time 1: Devices are manufactured with default names.

Merging into the personal group

Time 2: The new devices are introduced to personal groups.

User Experience



Social networking

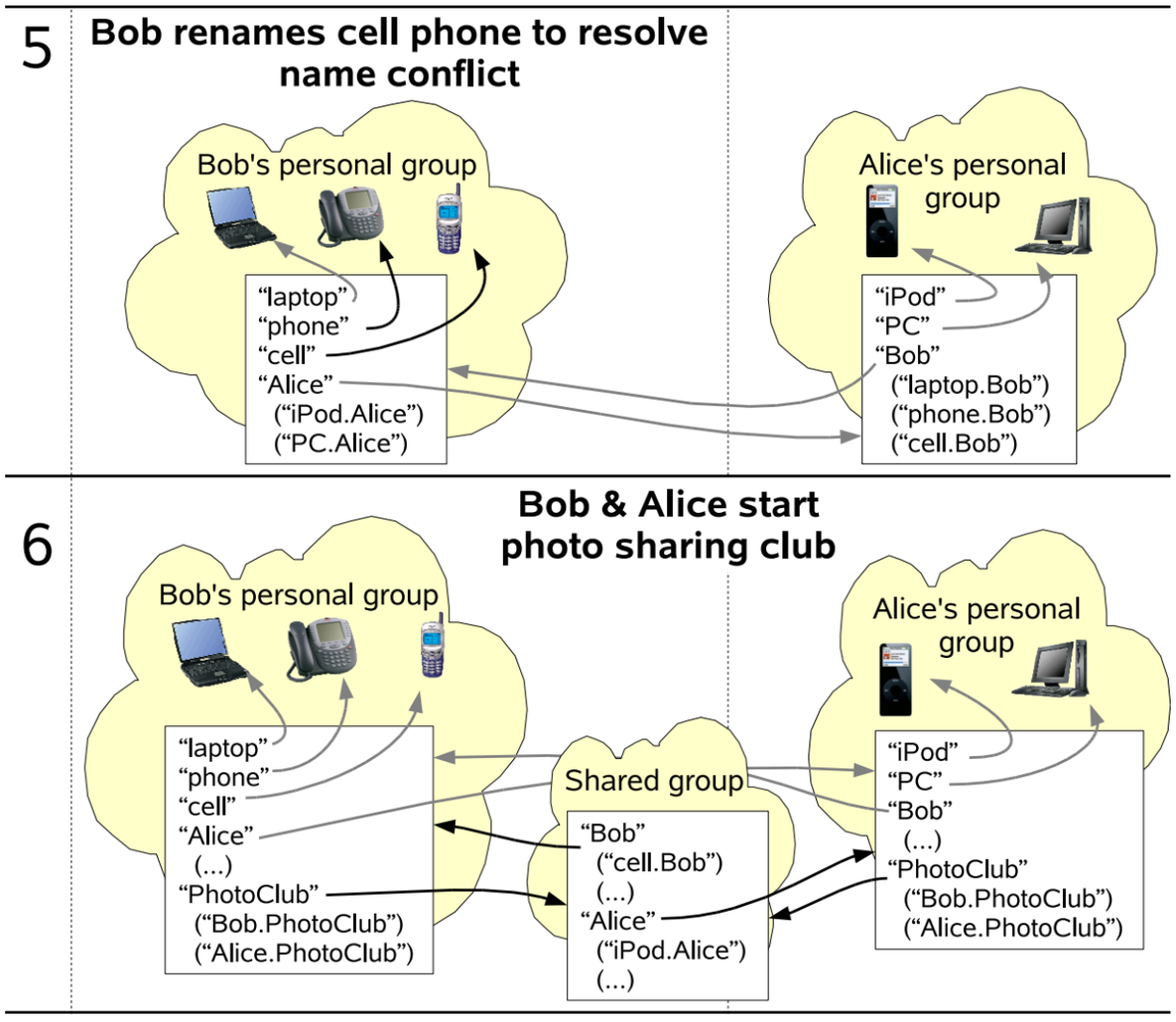
Time 3: Bob buys an new cell phone and introduces Alice's personal group as a new contact by finding Alice's iPod, and Alice does likewise. *(the new phone is not a part of Bob's personal group)*

Transitive merging

Time 4: Bob merges the new cell phone with his home phone. Devices gossip memberships.

`iPod.Alice`

User Experience



Privacy issue (not sure): Bob's photos are stored on the laptop, but others can view the contents on his phone.

Resolving naming conflicts

Time 5: Bob renames his cell phone to "Cell". *(otherwise both of the two phones won't work)*

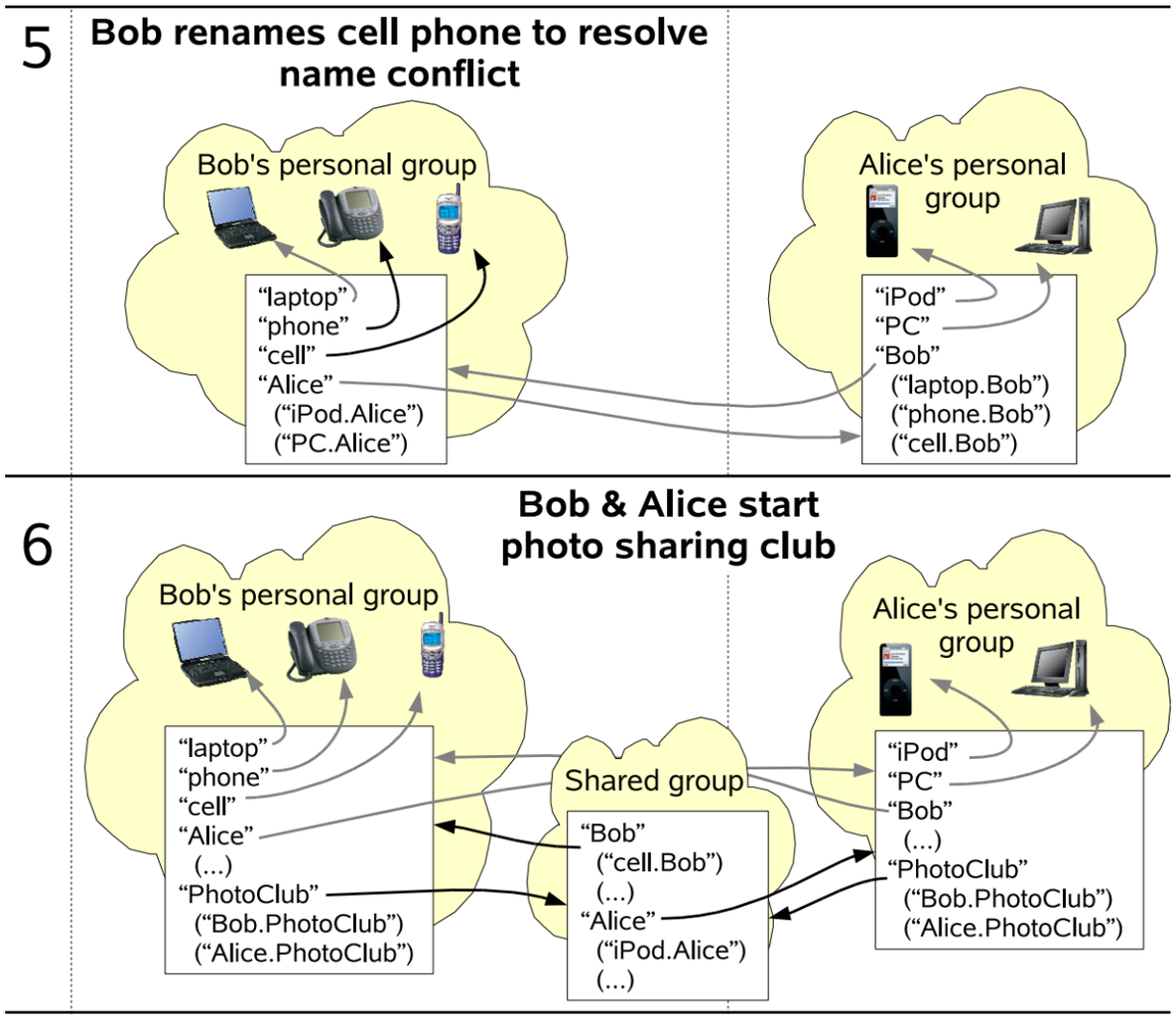
Creating shared groups

Time 6: Bob creates a shared group "PhotoClub" under his personal group and adds Alice to the group. Bob can also add others to the group, say "Charlie".

Group Ownership

Bob creates and owns the group. The group can be edited from any of his devices. Bob can also grant permissions to Alice. Other users can only browse the names.

User Experience



Privacy issue (not sure): Bob's photos are stored on the laptop, but others can view the contents on his phone.

Resolving naming conflicts

Time 5: Bob renames his cell phone to "Cell". *(otherwise both of the two phones won't work)*

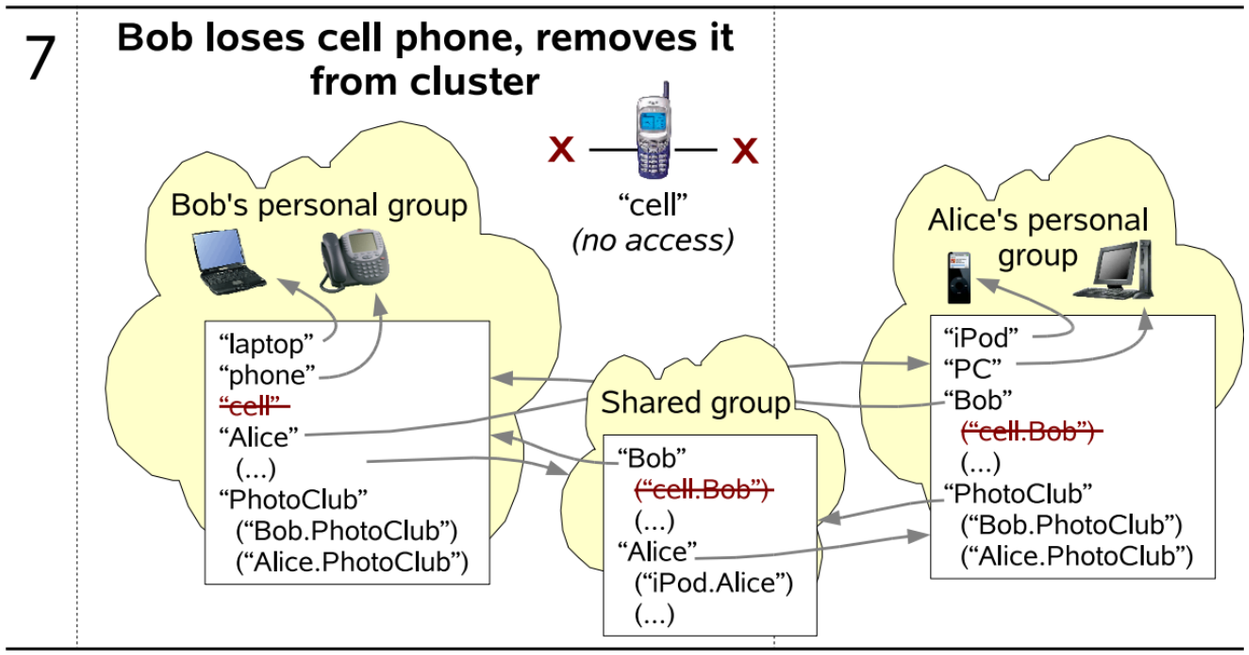
Creating shared groups

Time 6: Bob creates a shared group "PhotoClub" under his personal group and adds Alice to the group. Bob can also add others to the group, say "Charlie".

Group Ownership

Bob creates and owns the group. The group can be edited from any of his devices. Bob can also grant permissions to Alice. Other users can only browse the names.

User Experience



Revoking ownership

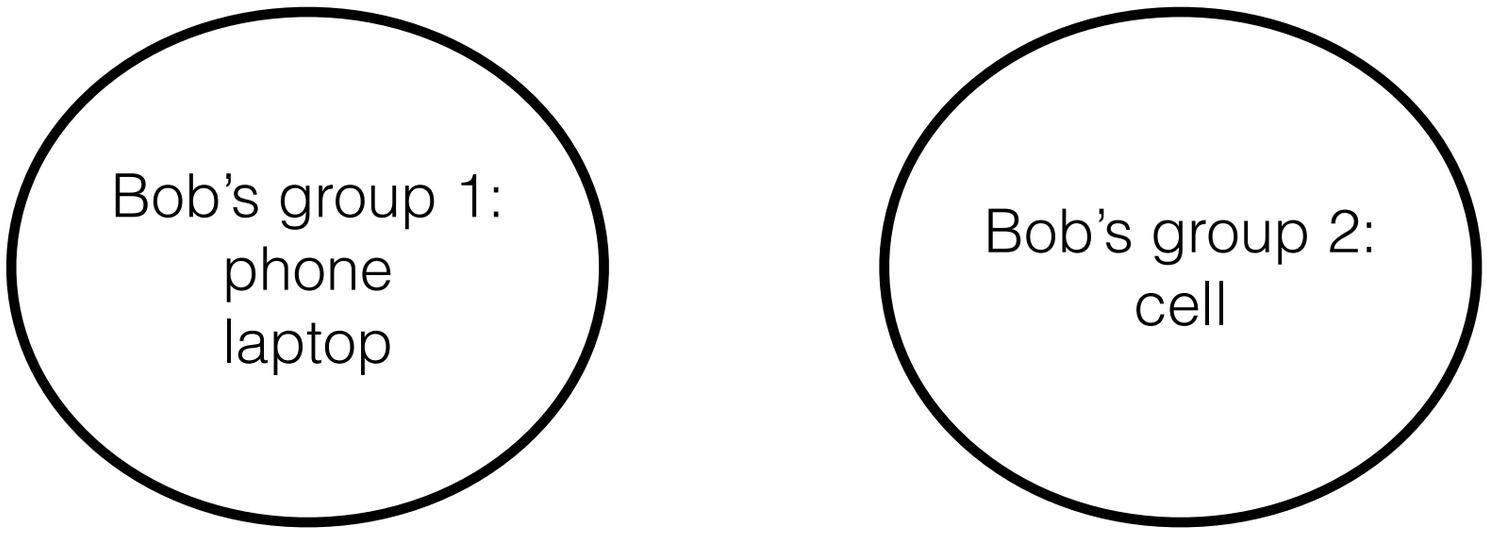
Time 7: Bob's cell phone is missing and he revokes cell phone's ownership of the personal group.

(can undo)

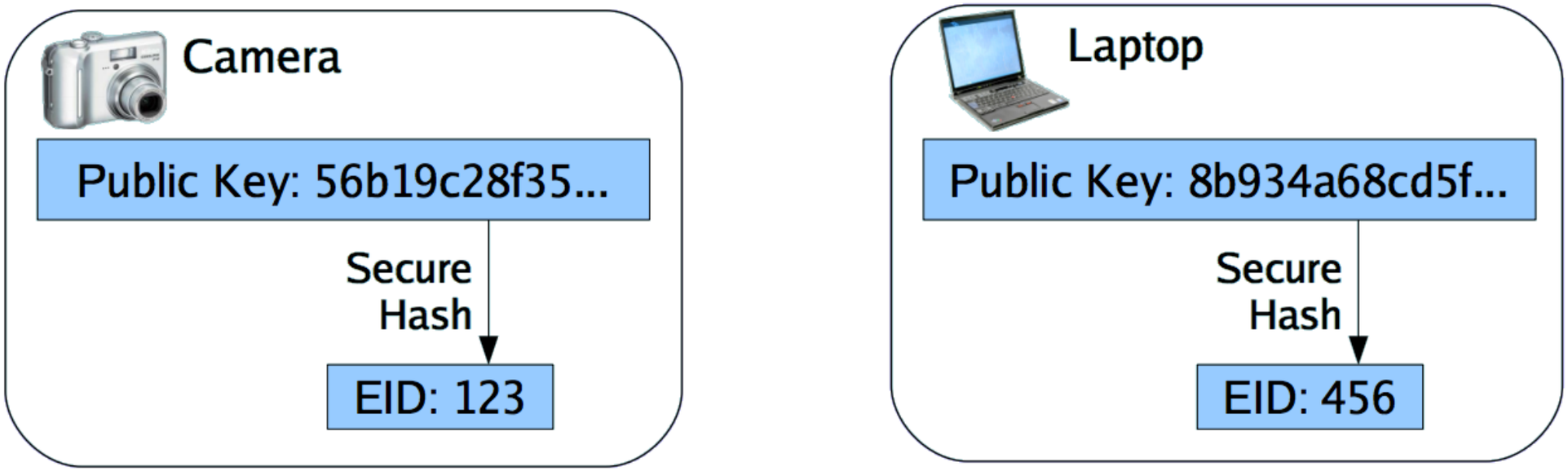
User Experience

What if the thief revoke the ownership of Bob's other devices first?

- UIA allows any device to dispute the revocation.
- Mutual revocation splits the group.
  - Alice needs to re-introduce Bob.
  - Can be merged again.



Personal Endpoint Identities

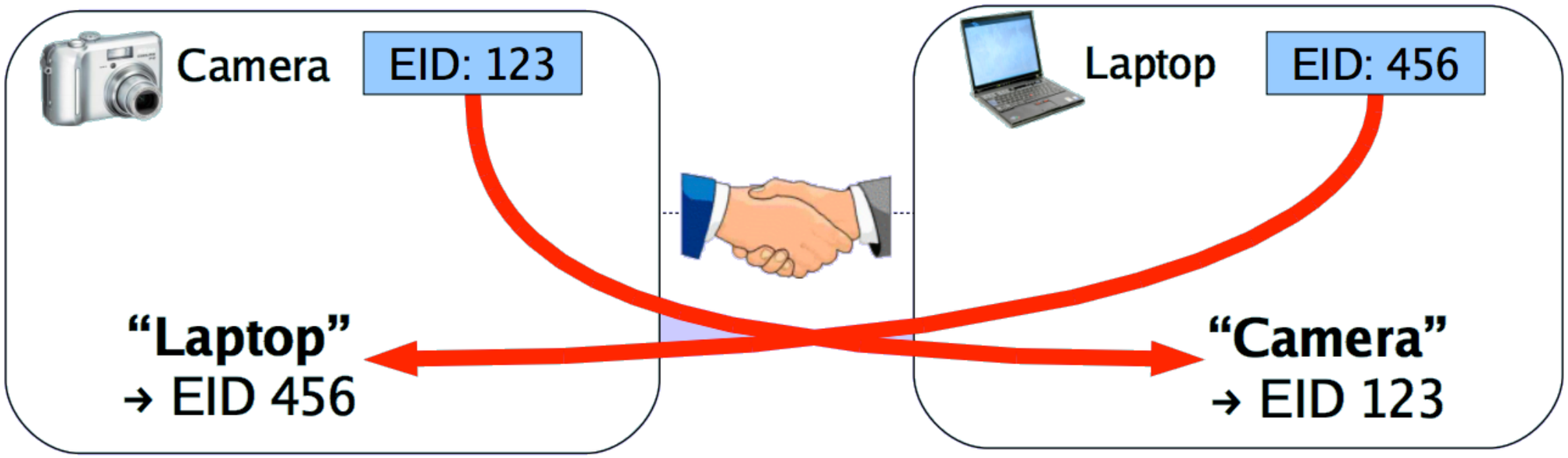


Endpoint Identities (EIDs)

1. *Stable*: do not change.
2. *Personal*: shared device creates a separate EID for each user.
3. UIA-aware network uses EIDs instead of IP addresses to identify communication endpoints.
4. The user can bind any name to the EID.

figure taken from "https://pdos.csail.mit.edu/papers/uia:osdi06-slides.pdf"

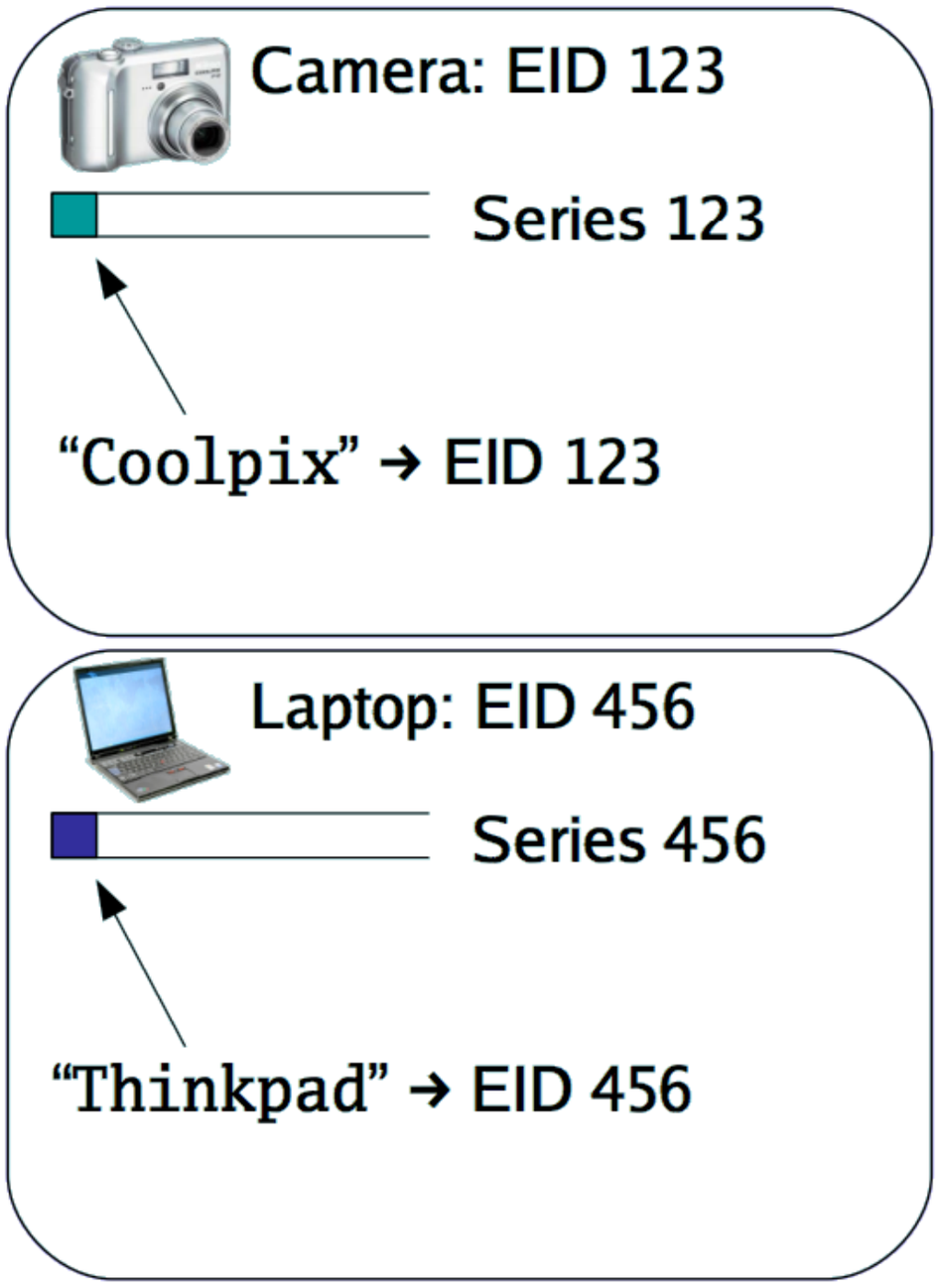
Device Introduction



Devices exchange EIDs on introduction

figure taken from “https://pdos.csail.mit.edu/papers/uia:osdi06-slides.pdf"

Series



Each device maintains a series

1. keeps track of the changes caused by the device.
2. series ID: uniquely identifies the series.
3. record ID: uniquely identifies the record.
4. four types of records: *create*, *link*, *merge*, *cancel*

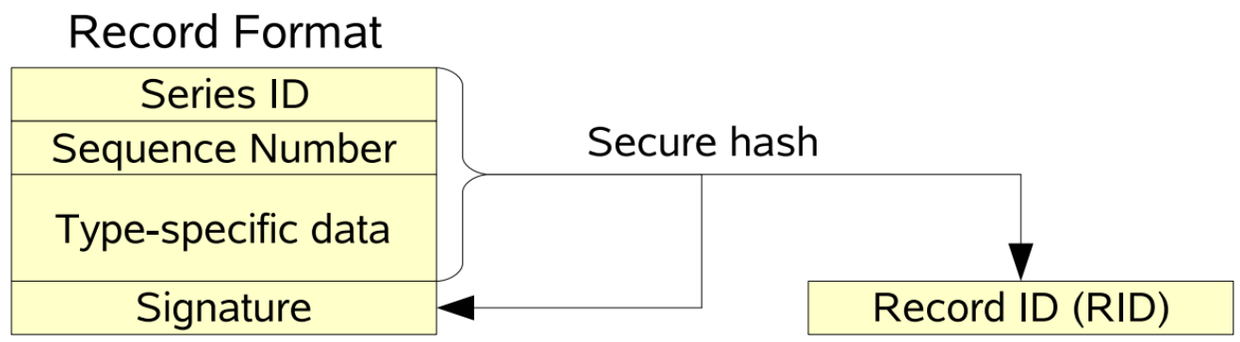


figure taken from "https://pdos.csail.mit.edu/papers/uia:osdi06-slides.pdf"

Records

- Create
  - initializes a new series.
  - record ID becomes the series ID.
  - signed using the owner’s private key.
- Link
  - binds label to an endpoint ID or series ID.
  - owner flag: grants ownership to the target.

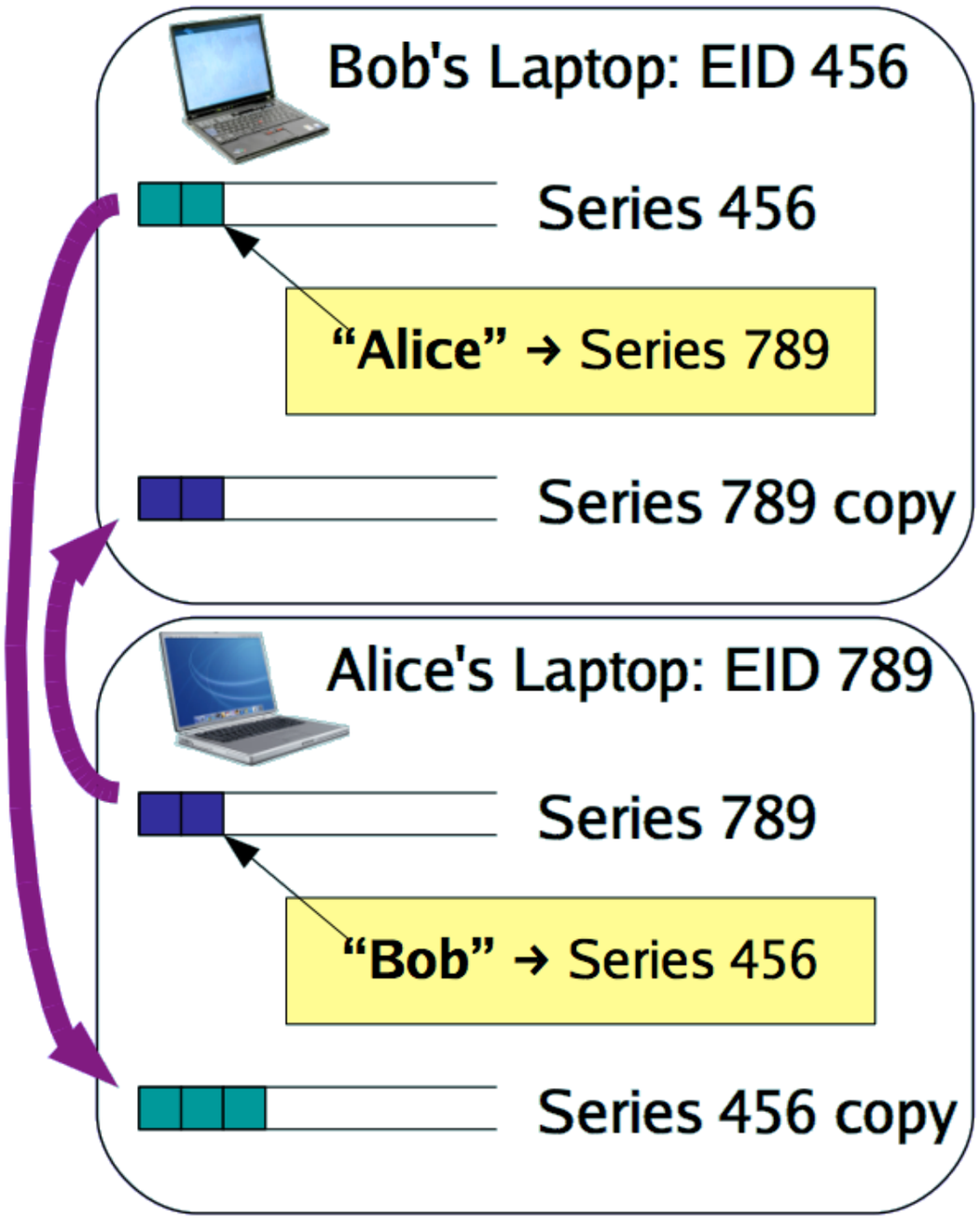
Records

- Merge
  - joins two series to form a single UIA group.
  - union of all links and cancel in all merged series determines the set of names being displayed.
- combines *transitively*.
- takes effect when:
  - device owns the target group.
  - mutual merge records.

Records

- Cancel
  - nullifies the effect of a previous record.
  - delete or rename group members.

Meet Others



During introduction:

1. Exchange series IDs.
2. Write new link records pointing to the other device's root series.
3. Gossip contents.

figure taken from "https://pdos.csail.mit.edu/papers/uia:osdi06-slides.pdf"

Routing and Forwarding

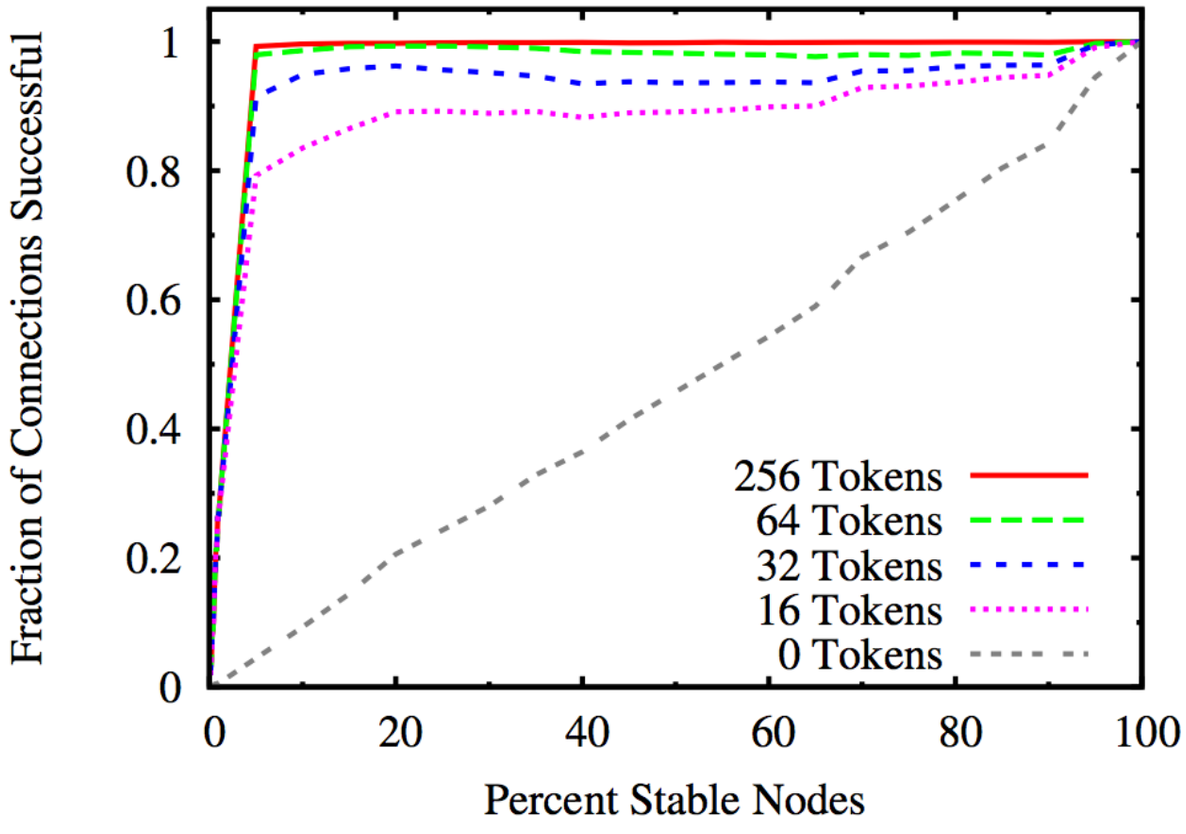
- Task:
  - finding the target's current IP address
  - forwarding traffic to it directly or indirectly.
- *Social neighborhood*: user's own devices, friends' devices, "friends of friends".
- IP address of the target is unknown
  - flooding location request through the overlay network between devices in its social neighborhood.

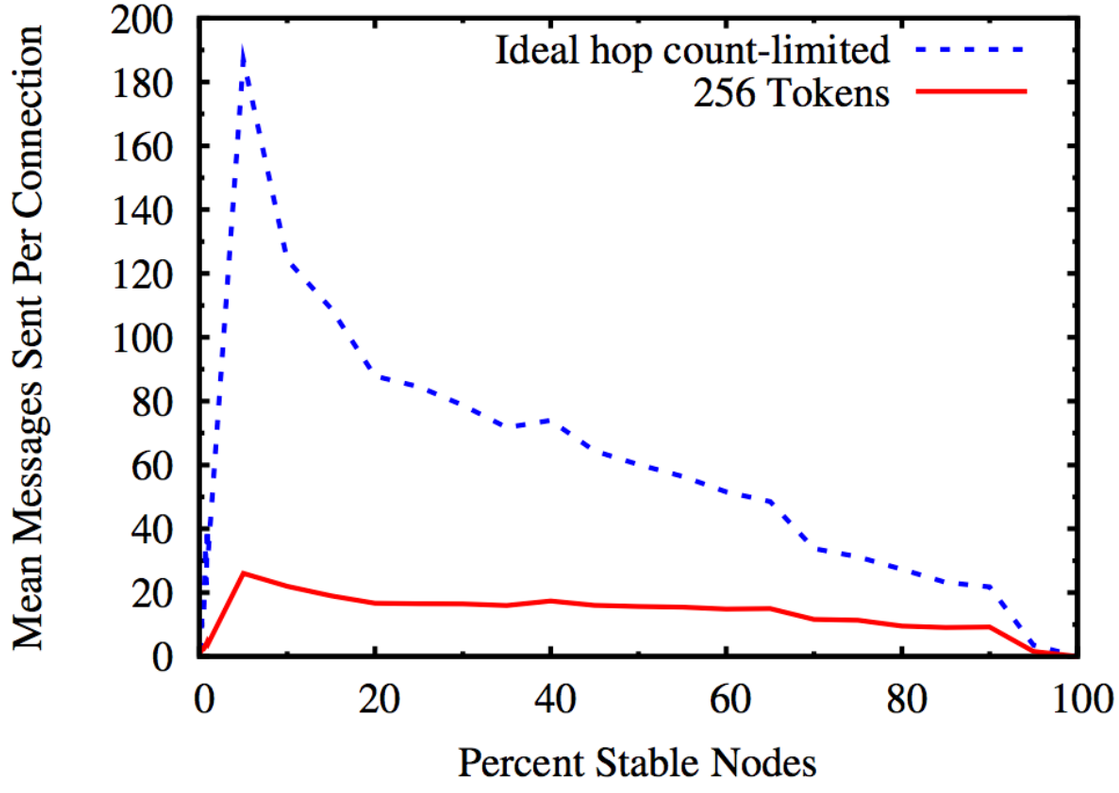
Overlay Construction and Maintenance

- Each UIA device maintains an open TCP connection with some overlay *peers*.
  - stable (90% available at the same public IP in the last week)
  - closest to it in *friendship distance*.
    - dist(user's devices) = 1
    - dist(direct peer) = 1
    - dist(direct peer of a direct peer) = 2
    - …
- Flooding is token limited rather than hop count limited.

Experimental Evaluation

1. Simulate network using social network site Orkut.
2. Stable devices are chosen randomly
3. “Ideal hop count-limited” knows the minimum number of hops needed in advance.





Future Work

- Privacy: no read restrictions.
  - users may want to hide some contacts.
- Assuming groups are small and change infrequently
  - can always gossip the entire group.
  - store change records forever.
- Assuming groups are owned by one person / a few people managing by consensus.
- Better digital signature algorithm.

Related Work

- Decentralized security:
  - SDSI and UIA both allow users to define local names.
  - SDSI associates public keys to users rather than devices.
- Connectivity:
  - existing internet protocols require configuration effort and technical expertise.
  - Dynamic DNS, Mobile IP, VPNs.

Related Work

- Systems replying on globally unique names with centralized registration and management: Uniform Communication Identifiers, HINT.
- Bonjour:
  - users can choose names on local-area networks.
  - names become invalid when networks change.
- Host identity
  - inspired by SFS, HOP, JXTA, i3
  - EID is also *personal.*

Related Work

- Distributed hash tables (DHTs)
  - provide scalable lookup of arbitrary flat identifiers in large distributed address spaces, but tolerate limited asymmetry or non-transitivity (NAT).
    - UIA focuses on reliable routing to nearby devices
- Global connectivity
  - global names: DDNS, i3, CoDoNS, TRIAD.
  - UIA focuses global connectivity via *personal* names.

Related Work

- Optimistic replication:
  - file systems and databases: Ficus, Coda, Ivy, Bayou
  - mobile devices: Rumor, PGrid, Roma, Footloose
  - UIA: data content and *set of participants.*
- Social data sharing: Turtle, SPROUT, F2F, Tribler

Strengths and Weaknesses

- Strengths
  - usage is intuitive to non-technical users.
  - no centralized management.
  - support offline operations.
- Weaknesses
  - in practice, very few devices are stable.
  - small social networks may fail.
  - revoking ownership is complicated.

Discussion