Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue

Daniele Quercia Stephen Hailes

By Xincen Yu

What is it about

- Propose a new decentralized defense for portable devices called MobID
- Every device manages two small networks where it stores information about the devices it meets: network of friends, network of foes
- Determine whether the unknown device is honest or not by reasoning these two networks

Existing Solutions

- Additional infrastructure that bind identities and cryptographic keys
- Bootstrap tree of the DHT. Sybil nodes will attach to the rest of the tree only at limited number of nodes [Danezis *et al.*]
- Sybil Guard. [Yu *et al.*] Nodes exchange keys with limited friends. After putting together, attacker would have limited number of friends(online Social Network)

Using mobility…

- The devices may be not always online
- The small social network may be not fast mixing as the large one.
- But people move, meet and exchange information.

Problem Statement

- MobID guarantees that an honest individual accepts, and is accepted by, most other honest people with high probability. The end result is that honest people successfully trade services with each other

Assumptions

- Assumption 1: People have off-line relationships (have "friends") with whom they share their identities
- Assumption 2: People identify themselves using public keys.
- **Assumption 3**: People do not meet at random. They meet their friends and their familiar strangers
- **Assumption 4**: Honest nodes are well-connected in social networks while sybil nodes sit in the periphery.

The basic

- *C and D which share encounters* are more likely than a pair of random individuals to be friends; that is, the link *C-D is likely to exist.*
- *Since links are* not random but preferentially exist among honest individuals, those individuals end up to be well-connected in the social network (Assumption 4). (or, the network will be sparse)
- Then, by measuring the network centrality of a stranger, one is able to determine whether the stranger is a sybil or not.

How it works

- A. Recording human-established relationships.
- B. & C. Reasoning not only on a network of friends but also on a network of foes.
- D. Deciding whether to accept or reject.
- E. Updating those two networks.

A. Recording Human-established Trust Relations

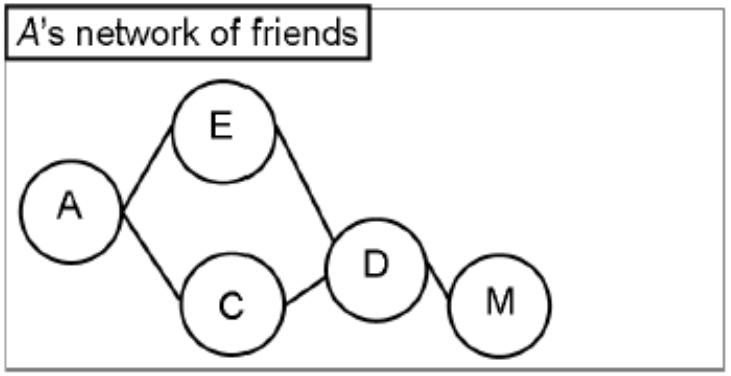
- To prevent B from lying his list of friends

  B's friends certify their relations using private keys

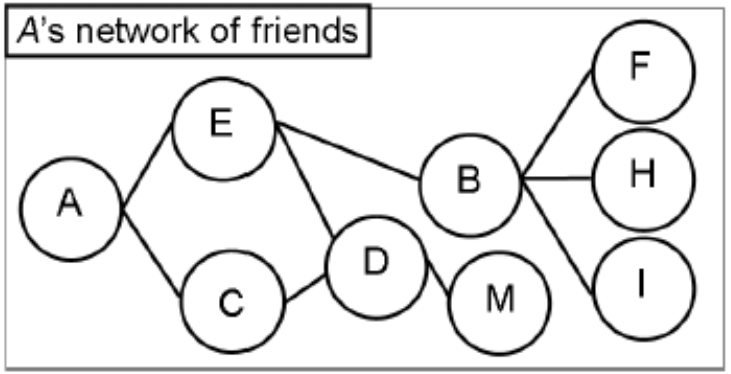
- B's friends are F, H, and I
- $S_F\ (PK_F\ ||PKB)$
- $S_H(PK_H||PKB)$
- $S_I\ (PK_I\ ||PKB)$

B. Reasoning on a Network of Friends

- Step 1. *A incorporates B's list into its network of friends.*



(a)



(b)

Step 2. *A ranks B on its network.*

- *B's rank reflects B's importance in the network.* The more central *B's role in the network, the higher its rank.*
- One common way of measuring centrality is to measure the network betweenness of B.
- **Definition**: The random-walk betweenness of *B* with prior *A is equal to the number of times a* random walk starting at *A and ending at any* node *X passes through B, averaged over all X.*

Step 3. *Depending on B's rank, A decides whether to accept or reject B.*

- The higher *B's rank, the* likelier *B is honest.*

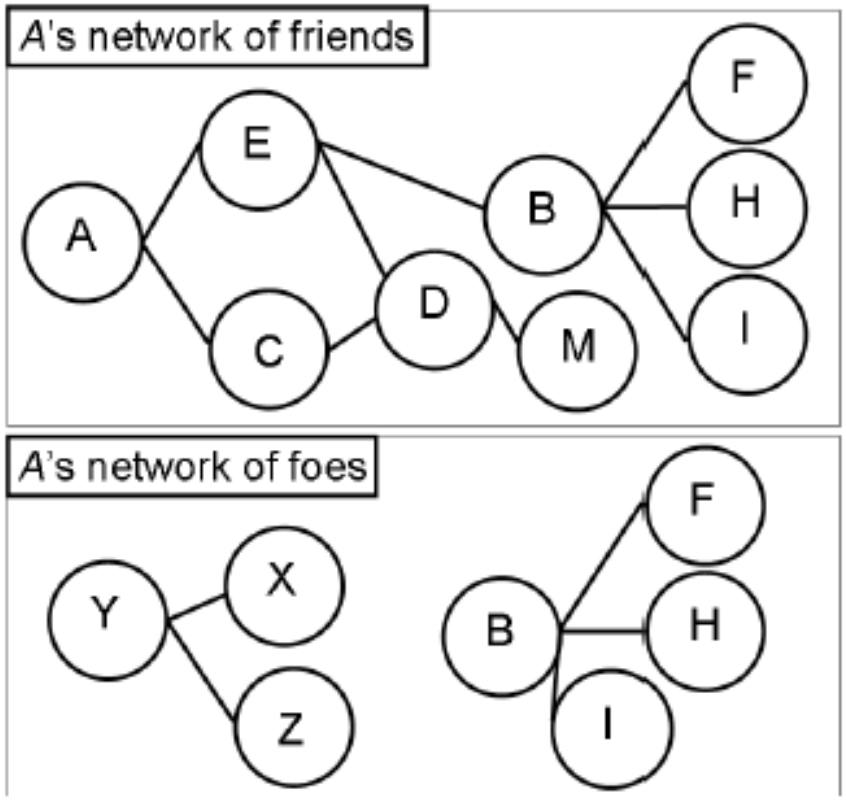
- *Since sybils do not have many* real friends, they sit in the periphery of the network and are rarely traversed by a random walk.

Not enough…

- *B can easily boost its rank in a tiny network. (fool some node, make sybils under control become multiple individuals)*
- *To fix this, introduce network of foes*

C. Reasoning Also on a Network of Foes

- Step 1. *A incorporates B's list of friends in both of its networks.*



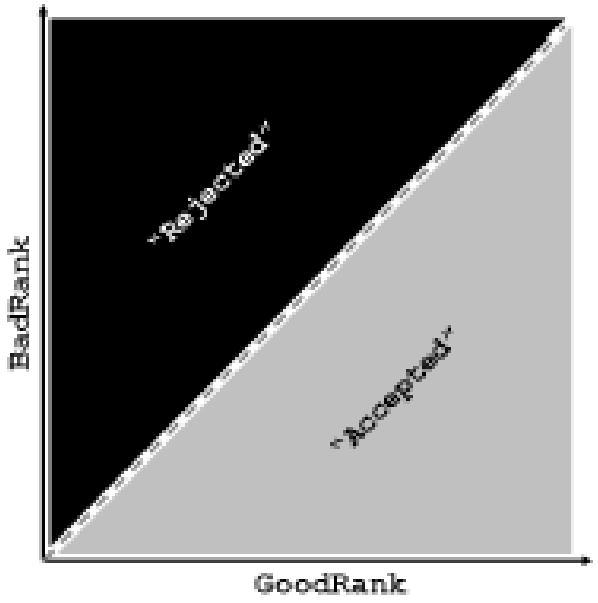
- Step 2. *A ranks B on its two networks.*
- *(good rank, bad rank)*

- Step 3. *Depending on both of B's ranks, A decides whether to accept or reject B. (linear way, clusters)*

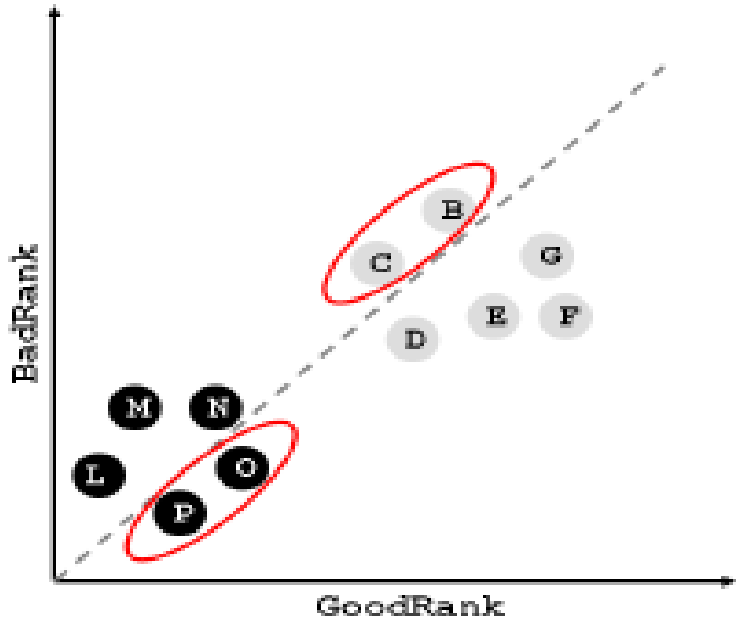
D. Deciding Whether to Accept or Reject

1. Comparing Ranks Linearly.

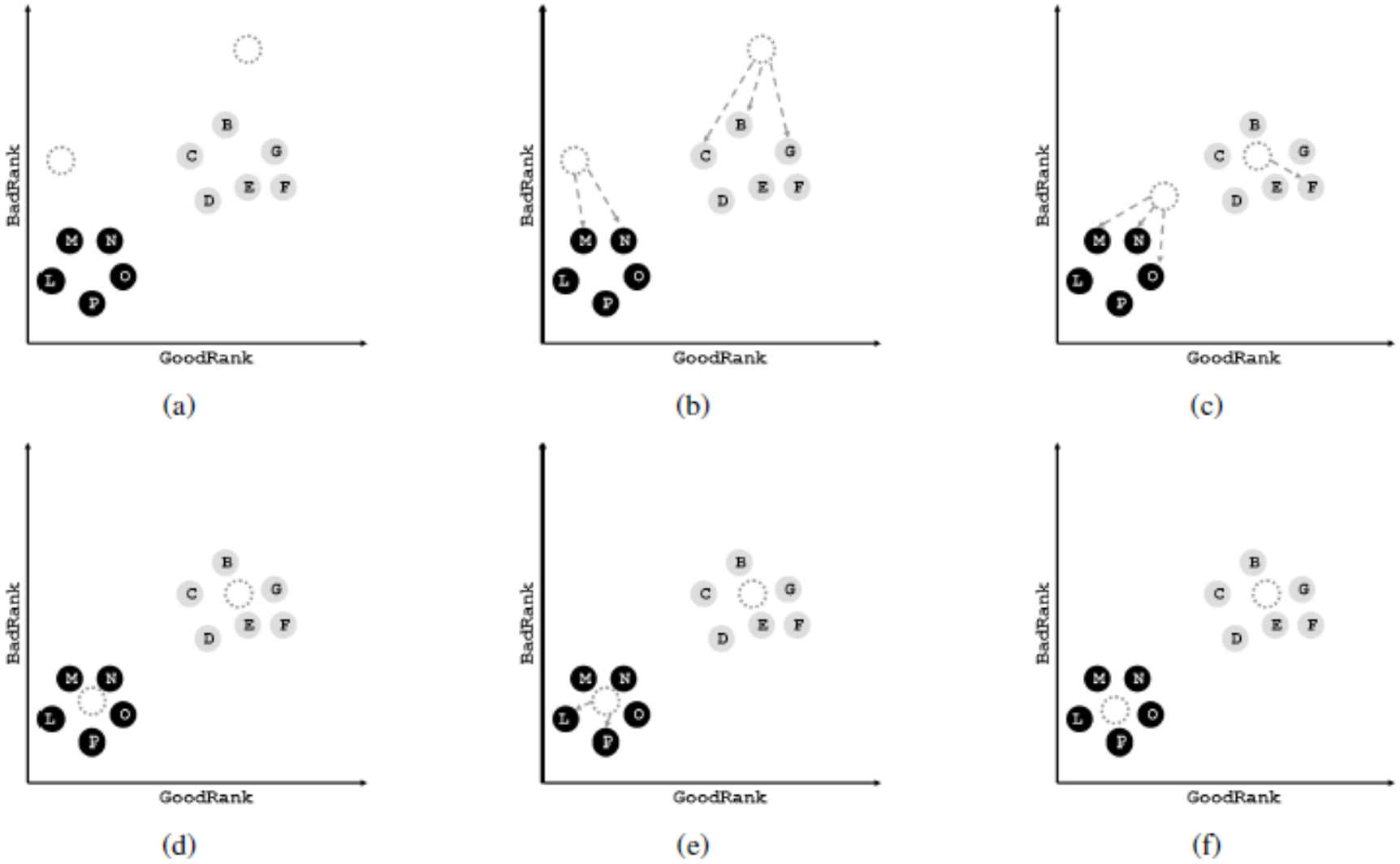
- *GoodRank > I *BadRank.*
- *If* that is the case, then *A accepts B; otherwise, it rejects B.*
- For example, if *I = 1*



2. a problem



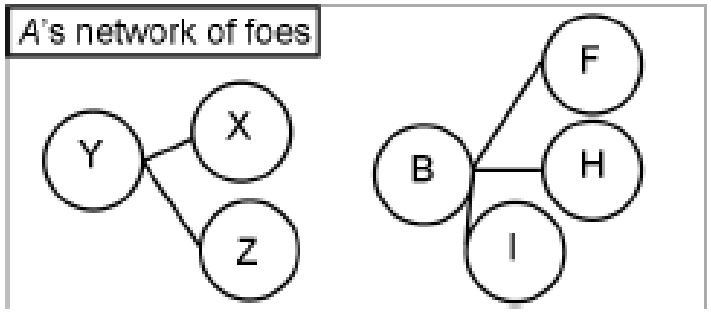
3. Clustering Ranks (k-means)



By Xincen Yu

The benefit of using two networks

- *B creates bogus identities, then it would artificially boost not* only its *GoodRank but also its BadRank.*
- *Help detect colluding attackers (Consider F and X to befriend)*



E. Updating the Two Networks

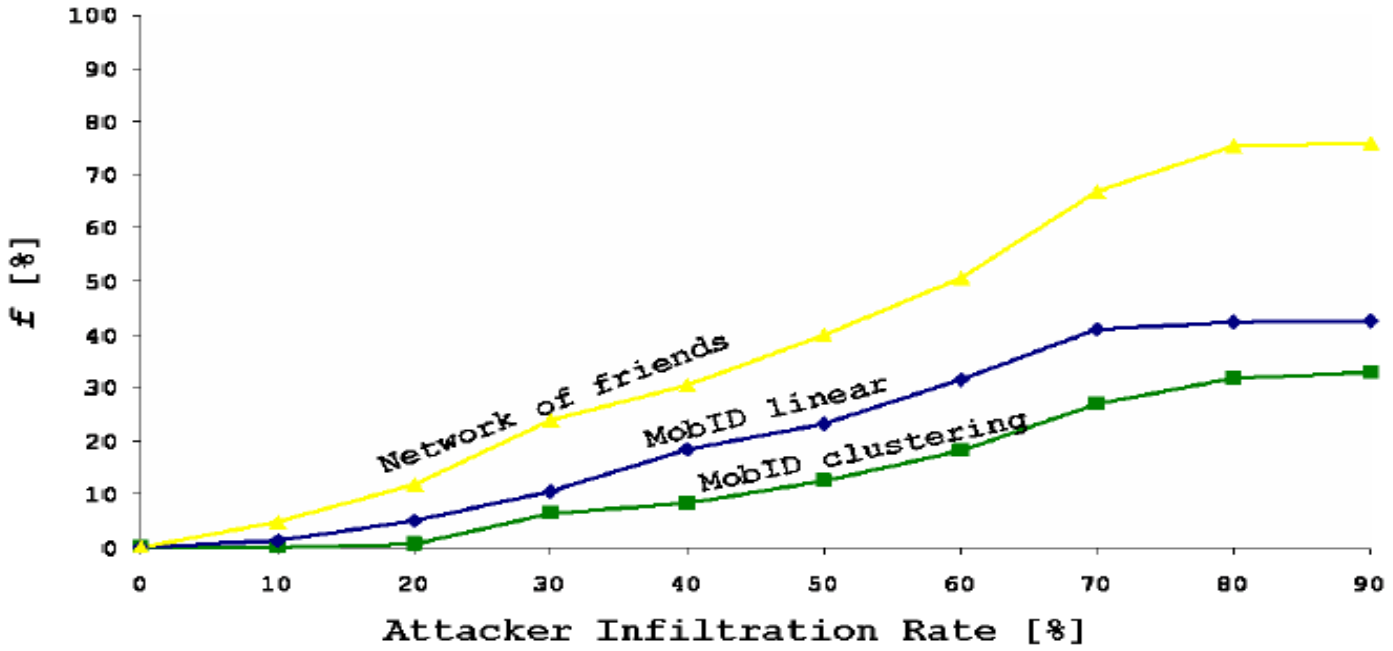
- *A does so by* removing *B and its friends from its network of foes, if A* accepts *B; or from its network of friends, if A rejects B.*

Evaluation

- we evaluate the robustness of MobID by keeping track of:
- 1) The fraction *f of fulfilled sybil interactions (i.e., interactions* that have been fulfilled by Sybils over those attempted);
- 2) The fraction *m of missed interactions (i.e., interactions* mistakenly refused over those attempted by honest people).
- By doing so, we assess to what extent MobID reduces both *f* and *m*.

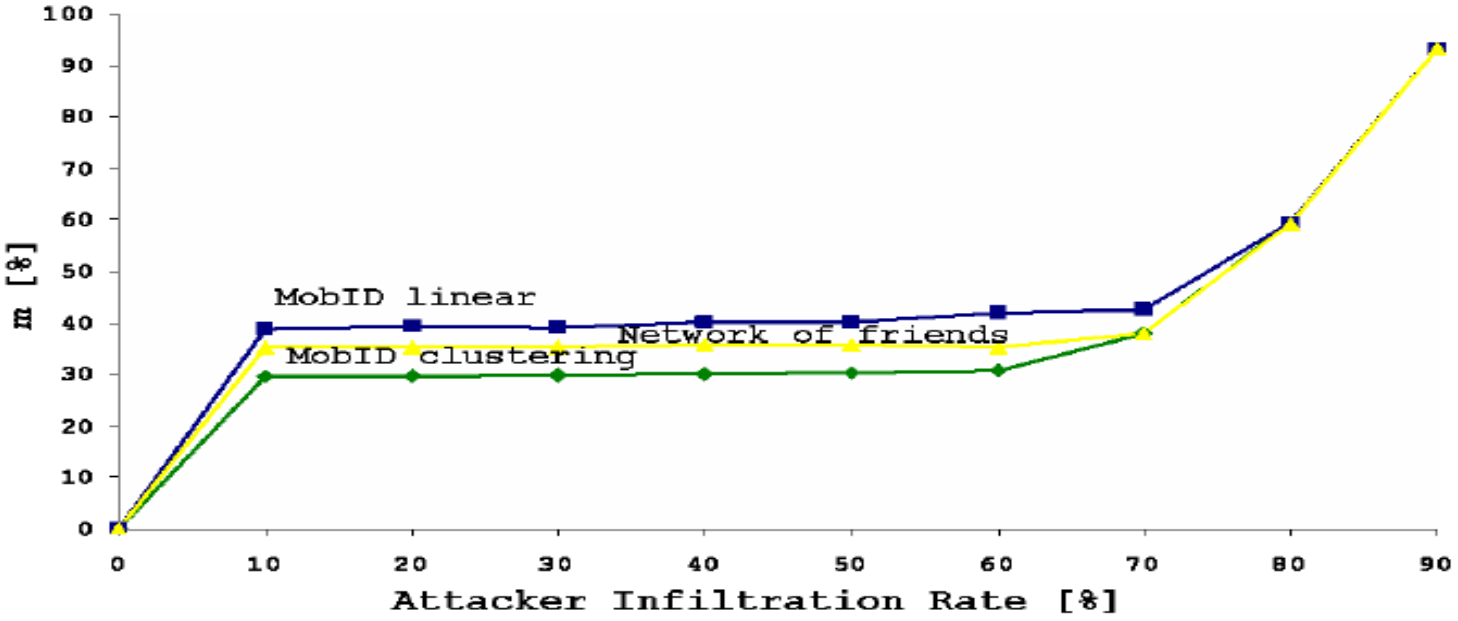
Reducing f

- the fraction of interactions that sybils fulfill (*f*) *mainly depends on* how diffusively sybils infiltrate the social network
- *l* = {*1/2*, *1*, ***2***}



Reducing(lost opportunities) m

- How much they mistakenly reject honest people
- l={**1/2**, 1, 2}
- If attackers manage to diffusely infiltrate the community (more than 70% of its members), most honest people are abruptly excluded from the system.
- networks become extremely sparse and they are unable to identify sybils.



Thank You!

By Xincen Yu