

Social Trust in Opportunistic Networks

Bernhard Plattner, ETH Zurich

Based on work by Sacha Trifunovic, Franck Legendre, Bernhard Distl
and Carlos Anastasiades (Univ. Bern)



Opportunistic networks

- § Mobiles carried by humans
- § Communication via direct neighbors, no infrastructure needed
- § DTN-like
- § Applications
 - § Content distribution
 - § Mobile micro-blogs
 - § Opportunistic dating
 - § Uncensored communication
 - § Organization of (political) campaigns

Problems

§ Applications should be high-quality, trustable

§ No centralized authority

- § Authenticity of identity difficult to achieve

- § Sybil users

§ Privacy is important:

- § Pseudonymity may be broken – users may run into each other

- § Easy to infer about user locations, possible at every one-to-one encounter

§ Privacy vs. trust trade-off

Research questions

- § How much privacy does one have to give up in such a set-up?
 - § How much privacy can one retain?
 - § Is it possible to leverage social bindings for increasing trust while retaining privacy?
 - § What kind of social bindings?
 - § How to learn about them
 - § How to use them
- without giving up too much privacy

Explicit social trust

- § Consciously established „friend“ ties of paired users
- § Robust tree-like graph representing trust
- § Trust values are function of
 - § Hop distance from tree root
 - § Connection density
- § High trust values \rightarrow trust in user identity

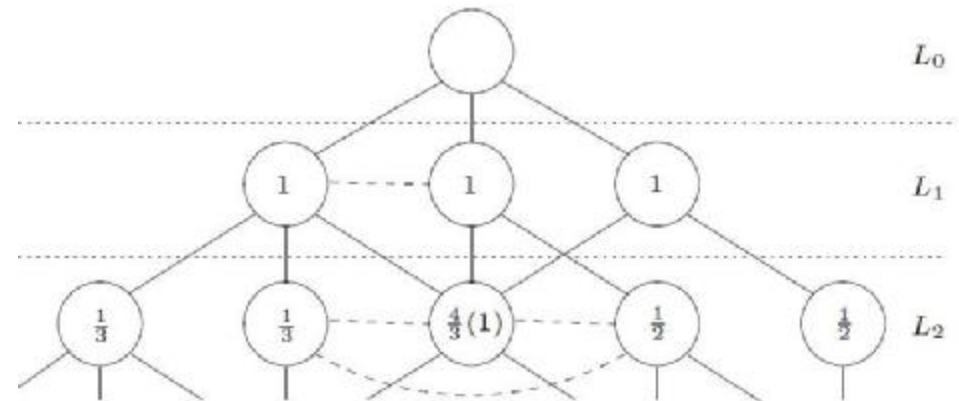


Fig. 1. Friendship Graph G_F

Implicit social trust

- § Based on mobility properties
- § Graph with limited diameter, representing familiarity with neighbors
 - § Trust increases with proximity time
- § Trust values based on the persistency of the identities in the graph
 - § Goes against sybil users switching their identities