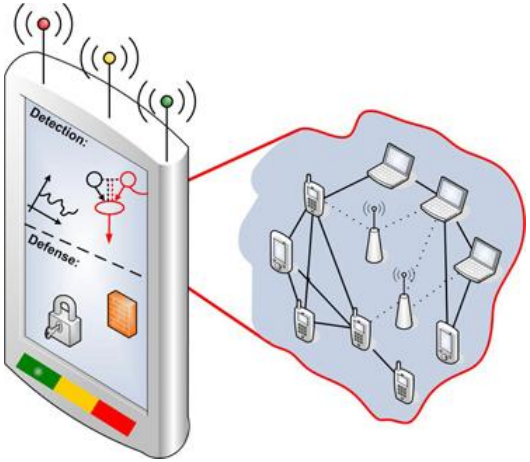


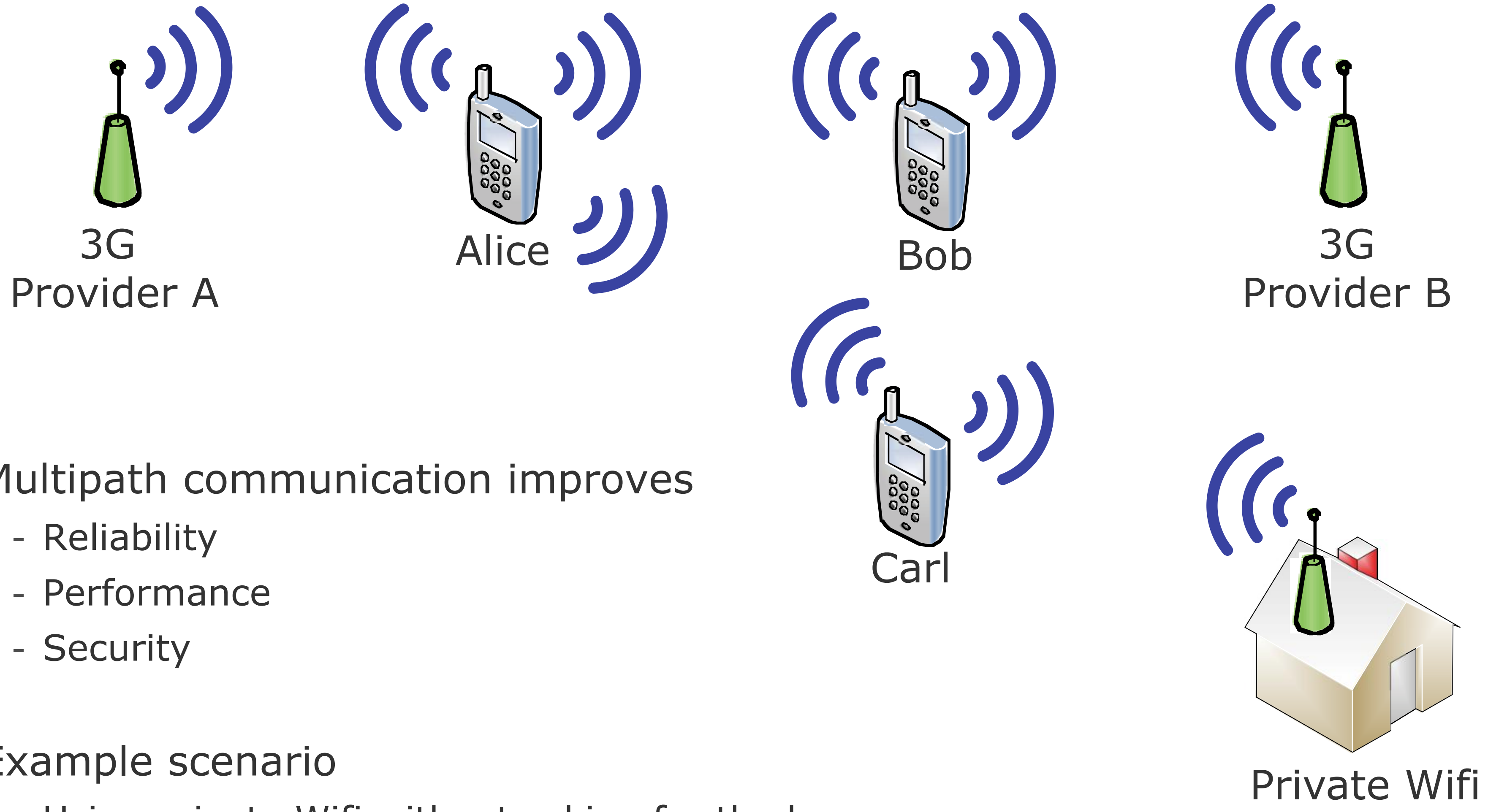
Can Your Phone Trust Your Friend Selection?

Trust establishment in mobile phone ad-hoc networks

Sebastian Trapp, Matthias Wählisch, Jochen Schiller
sebastian.trapp@fu-berlin.de

HAW Hamburg, 27.09.2011

Why ad-hoc communication with mobile phones



Multipath communication improves

- Reliability
- Performance
- Security

Example scenario

- Using private Wifi without asking for the key

Problem statement

- In ad-hoc communication all data is relayed via other devices
- Possible attacks
  1. Eavesdropping
  2. Data manipulation
  3. Packet dropping

- End-to-end encryption prevents (1) and (2)
- But: No prevention against (3)
  - Every relay can drop packets
  - Ad-hoc network will be unfeasible

→ Identifying trustworthy neighbors

Common approaches to assign trust

Through Authentication

- Idea: Derive trust from ID / group-ID
- Problem: Contradicts ad-hoc scenario
  - Central instance may not be available
  - Pre-shared secrets between all mobile phones unrealistic

Through Reputation

- Idea: Assign trust to well-behaving mobiles
- Problem: Slow and inaccurate prediction
  - Time consuming
  - Intention hiding problem
    - Phones can pretend to behave well until trust is established

Anything else?

A new way of trust establishment

Initial trust between mobiles has to be established…

…not using a central instance

…not relying on pre-shared secrets

…within a short timespan

Our idea – socially inspired trust

- Ad-hoc trust establishment based on local data
- Defining trust not technically but socially
- Using the user’s social network

→ **Finding phones of friends or friends of friends**

Towards sociological trust establishment

Finding phones of friends or friends of friends

Example: Sending someone to deposit money for you.

Who would you entrust with your cash?

- Family member?
- Acquaintance?
- Friend of trusted friend?
- Stranger?

Depends on relationship

Data about the user’s social network already inherent in phones

- Contact lists
  - Phone book, email directory, online social network (OSN) friends
- Interaction logs

How to find phones of friends?

Concept

1. Compare contact lists
   - Exchange and analyze contact lists between two nearby phones
   - Use of unique attributes of contacts
     - E.g.: phone numbers, email addresses, OSN IDs

2. Evaluate mutual contacts
   - Autonomous analysis on each phone
   - Mutual attributes indicate mutual contacts
   - Weight information based on
     - Quantity and
     - Quality of mutual contacts

Springfield

Montgomery Burns
+11 092 8476 234

Ms Krabappel
23425234

Ned Flanders
839 923 923

Patty Bouvier

Principal Skinner
30498753

Selma Bouvier
239872394

Waylon Smithers

Evaluating mutual contacts

Quantity

- How many mutual contacts are there?
  - (Weak) indication for closeness of two users
- Find out if users associate with the same groups of people

Quality

- Who are the mutual contacts?
  - Trusted friends can enhance trust towards the other user
- Assign a weight to mutual contacts

Tie Strength – Weighting interpersonal relationships

- Sociological concept introduced by Granovetter in 1973
- Range from weak ties (acquaintances) to strong ties (trusted friends, family)
- Classification based on
  - duration of relationship
  - intensity and intimacy of communication

Classification of mutual contacts

Classifiers

- Duration of relationship
  - Long lasting relationships → stronger tie
  - Indicator can be date of first contact
- Intensity and intimacy of communication
  - Vivid exchange of messages or calls → stronger tie
  - Time of last contact
- Type of entries
  - OSN friends → weaker tie
    - Becoming “friends” is typically effortless, no contact needed
  - Phone number or email address → stronger tie
    - More action required
    - If added automatically, initial contact has taken place
- Number of mutual entries per contact
  - different entries of the same kind → stronger tie
    - e.g., work, private mobile and landline phone number

Measurement-based analysis

Setup

- 12 contact lists of friends and colleagues (Android and iOS devices)
  - Subjects belong to 4 different social groups
- Phone numbers and email addresses
- No logs (quantitative analysis only)
- Comparison of contact lists
  - Mutual entries can be identified this way

Results

- Contact list sizes vary greatly
  - By one order of magnitude (48 to 496 entries)
- Social groups are represented in mutual contacts
  - Within one group high numbers of mutual contacts
  - Between groups hardly no mutual contacts
- About 11 kB traffic
  - Ø 240 contacts, 3 entries per contact and 128 bit hash function
  - Around 1 second transmission time on first generation Bluetooth

Technical implementation

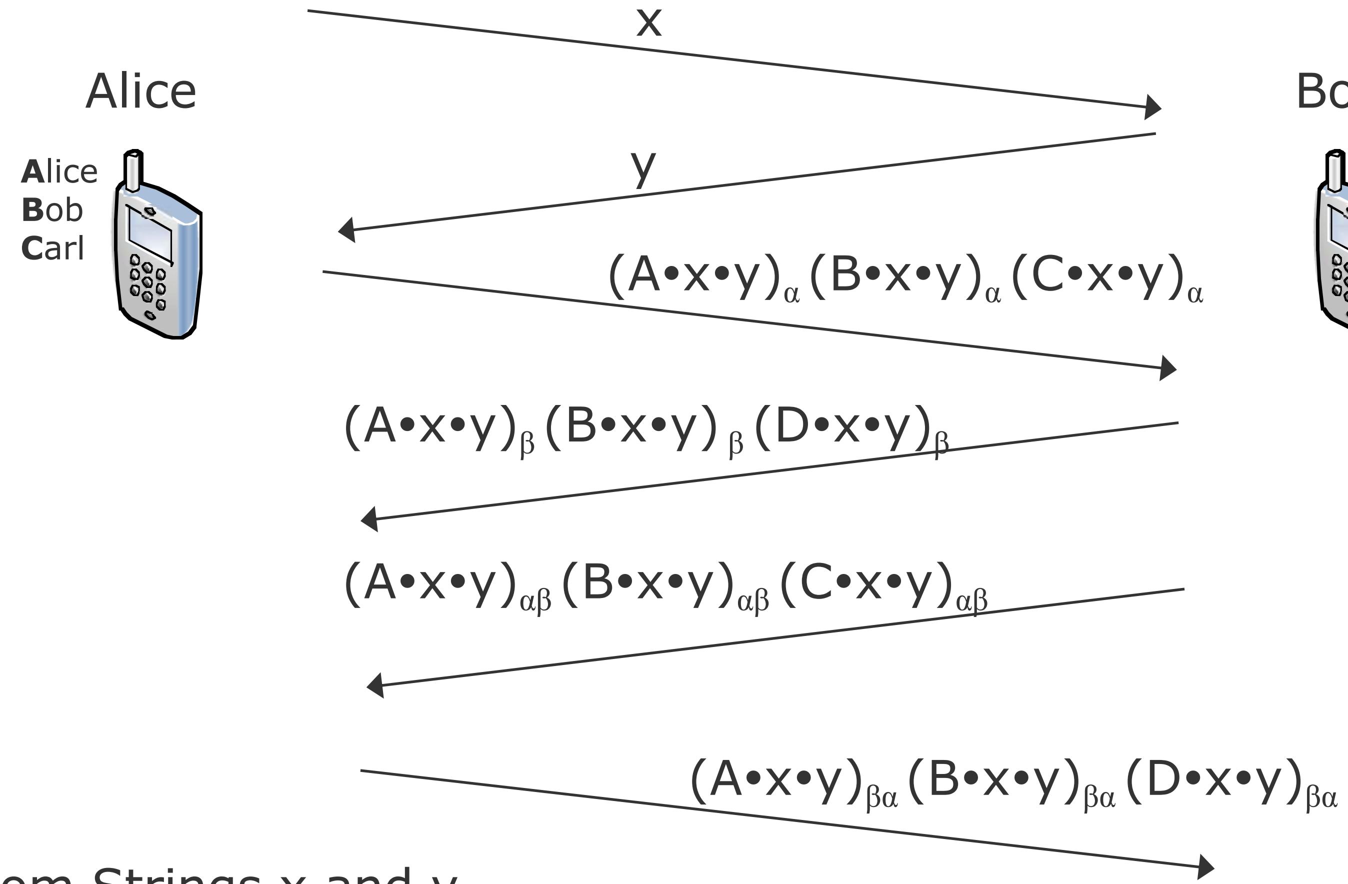
Preparation of entries

- Exclusion of business contacts, hotlines, …
- Normalization of numbers and email addresses
  - E.g., 0800-…, +4940-8382313

Exchange of contact lists

- Near field communication technology
  - E.g., Bluetooth
- Commutative encryption
  - All data transmitted is encrypted
  - Eavesdroppers gain no contact information
  - The communication partners only know the identity of mutual contacts

Contact list exchange



x

Alice

Bob

Alice
Bob
Carl

y

Alice
Bob
Damian

$(A\bullet x\bullet y)_{\alpha}\,(B\bullet x\bullet y)_{\alpha}\,(C\bullet x\bullet y)_{\alpha}$

$(A\bullet x\bullet y)_{\beta}\,(B\bullet x\bullet y)_{\beta}\,(D\bullet x\bullet y)_{\beta}$

$(A\bullet x\bullet y)_{\alpha\beta}\,(B\bullet x\bullet y)_{\alpha\beta}\,(C\bullet x\bullet y)_{\alpha\beta}$

$(A\bullet x\bullet y)_{\beta\alpha}\,(B\bullet x\bullet y)_{\beta\alpha}\,(D\bullet x\bullet y)_{\beta\alpha}$

Random Strings x and y

Concatenation operator $\bullet$

Secret private keys α and β

Commutative encryption: $A_{\alpha\beta} = A_{\beta\alpha}$

Roundup

A new way to establish trust between smartphones

- Ad-hoc
  - Initial level of trust can be assigned at first interaction
- Autonomous
  - Utilizing solely the social network data inherent to mobile phones
- Reciprocal
  - Relaying node can simultaneously evaluate its incentives

But there are still open questions…

Discussion I

Possible attacks

- The users learn about the reciprocal selection of contacts
  - → Randomization of encrypted contacts
  - → Marking of sensible contacts
- An attacker can gather social information in advance
  - → Avoid "phone book attack" by limiting contacts to compare
- The device of a friend is compromised
  - Malware or theft
  - → Grouping contacts by risk

Discussion II

Intense communication is not a good indicator for closeness

- Could also point to ongoing conflict

→ More likely to denote close relationship [Gilbert'09]

  - Especially if duration of relationship is long

Not all mutual contact entries can be identified

- No false positives
- Prediction less optimistic

→ no security risk

Conclusion and outlook

New concept to assign initial trust

- Establishing trust between technical devices on a sociological basis
  - Based on the user's social network data available on mobiles
- Autonomous and spontaneous
  - No central instance necessary
  - Every phone make its own decision

Next steps

- More detailed evaluation
  - Ongoing implementation
- Defining a metric to assign trust based on tie strength
- Expand idea to other application scenarios
  - Similar set of data available on most home PCs
  - Automatic friends suggestions or creation of group of close friends

Research Agenda

Tie Strength

- Defining an absolute or relative scale
- Accuracy of characterization of real-life relationships
- What more observable phenomena can be used

Assigning trust

- Metric for deriving trust out of tie strength

Analyzing logs

- Time interval to observe for reliable information

Commutative encryption

Encryption function based on Diffie-Hellman key exchange

$$E_K(m) = h(m)^K \bmod p$$

- $p = 2q + 1$, with p, q prime
- κ Element of 1, 2, ..., q-1
- h hash function

Commutative character

$F_k(x) = x^k \bmod p$

$$F_{kh}(x) = (x^k \bmod p)^h \bmod p = x^{kh} \bmod p = (x^h \bmod p)^k \bmod p = F_{hk}(x)$$