The Identity-Anonymity Paradox

On the Relationship between Identification, Anonymity and Security in Mobile Ad Hoc Networks

Leonardo A. Martucci
Karlstad University

Outline

- Introduction and Research Questions
- Security and Anonymity in Mobile Ad Hoc Networks
- The Identity-Anonymity Paradox

Introduction

- Mobile Ad Hoc Networks

"... autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed net "

RFC 2501__

- A paradigm-shift from the current network infrastructure model
  - every device is responsible to provide its own services
  - service provisioning, routing, security, network addressing…

Research Questions

- *Q1. How to provide network security in mobile ad hoc networks?*
- *Q2. What are the requirements and how to provide anonymous comm. in mobile ad hoc networks? Can existing P2P anonymous comm. mech. be directly deployed in mobile ad hoc networks?*
- *Q3. What is the relationship between anonymous comm., security and identification in mobile ad hoc networks?*

Contributions of this thesis

- A security model and architecture for mobile ad hoc networks
  - application framework for developing new applications
  - a group authentication mechanism
- Chameleon – overlay anonymous communication mechanism
  - requirements for anonymous comm. in mobile ad hoc networks
  - evaluation of P2P anonymous comm. mechanisms
- The Identity-Anonymity Paradox
  - \+ the consequences of the paradox

Outline

- Introduction and Research Questions
- Security and Anonymity in Mobile Ad Hoc Networks
- The Identity-Anonymity Paradox

Mobile Ad Hoc Network Security

- Security models can be divided into 3 families:
  - security relies on Internet services
  - security relies on some key devices in the ad hoc network
    - local scope CA
    - threshold cryptography
  - PGP-like systems

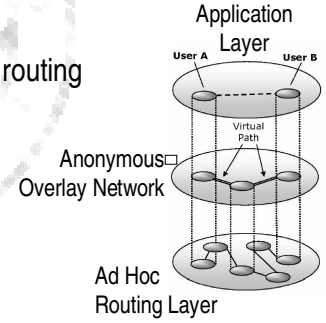
Securing Mobile Ad Hoc Networks

Q1. How to provide network security in mobile ad hoc networks?

- Trust-based security model and architecture
  - running on top a service-based network
  - mobile ad hoc network is divided into trusted groups
    - group authentication mechanism
    - certificates with embedded trust information
  - dynamic trust values and extension of the CA concept
  - implementation of an { application framework
    proof-of-concept applications

Anonymous Communications

- Anonymity can be defined as ⇨ *"the state of not being identifiable within a set of subjects, the anonymity set"*
- Anonymous Communication in Mobile Ad Hoc Networks
  - Routing layer
    + transparency towards application
    - incompatibility with standard ad hoc routing
  - Overlay applications
    + independency from routing layer
    - not transparent to applications



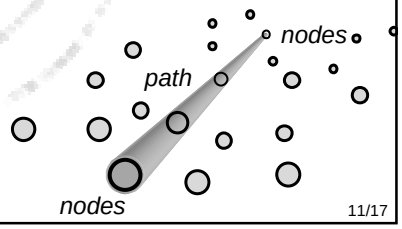
Requirements for Anonymous Comm.

Q2. What are the requirements and how to provide anonymous comm. in mobile ad hoc networks? Can existing P2P anonymous comm. mechanisms be directly deployed in mobile ad hoc networks?

- The identified requirements are:
  - scalability
  - strong anonymity
  - fair workload distribution
  - acceptable performance
  - P2P model
  - dynamic topology

Chameleon

- Anonymous Communication in Mobile Ad Hoc Networks
  - low-latency overlay anonymous communication mechanism
  - inspired on Crowds-system
    - forwarding is determined by a toss of a biased coin
  - evaluated against requirements from Paper IV
    - extended attacker model (wireless devices)
  - identification based on certificates



Outline

- Introduction and Research Questions
- Security and Anonymity in Mobile Ad Hoc Networks
- The Identity-Anonymity Paradox

Mobile Ad Hoc Networks Identifiers

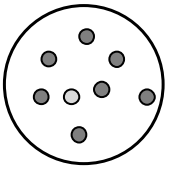
- Current Status ⇨ no addressing schemes
  - no native trustworthy identification in mobile ad hoc networks
  - is that perfect environment for achieving anonymity?

- is anonymity natively deployed in these environments?
  - just change MAC and IP addresses constantly

    ⇨ Anonymous Devices

    … of course there are always some problems…

    The Sybil Attack



The Identity-Anonymity Paradox

- *Q3. What is the relationship between anonymous comm., security and identification in mobile ad hoc networks?*

- Identity-Anonymity Paradox
  - anonymity provisioning demands security and trusted identities
  - security and anonymity provisioning are connected by identifiers

  ⇨ uniqueness must be provided by the security model

  - *"may operate in isolation"* does not mean *must* operate in complete isolation – or Sybil attacks are unavoidable

Future Directions

- Current Work
  - usage of anonymous credentials in mobile ad hoc networks (in collaboration with KU Leuven and RWTH Aachen)
  - the simulation of Chameleon to evaluate its performance
- Future Work
  - analyze the benefits of using cross-layer information for the benefit of security and privacy
  - ?

Contributions of this thesis

- A security model and architecture for mobile ad hoc networks
  - application framework for developing new applications
  - a group authentication mechanism
- Chameleon – overlay anonymous communication mechanism
  - requirements for anonymous comm. in mobile ad hoc networks
  - evaluation of P2P anonymous comm. mechanisms
- The Identity-Anonymity Paradox
  - \+ the consequences of the paradox

Fim

The Sybil Attack

"*a small number of network nodes counterfeiting multiple identities so to compromise a disproportionate share of the system*"

- originally applied for P2P networks

but fits well in the context of mobile ad hoc networks

⇨ an identity authority is needed to provide identifiers