Resource Charging in Ad-hoc Networks by Password Capabilities

Stanley Gunawan <stanleyg@csse.monash.edu.au>

Supervisors:
Dr. Ronald Pose <rdp@csse.monash.edu.au>
Dr. Carlo Kopp <carlo@csse.monash.edu.au>
Outline

- Ad-Hoc Networks
- Resource charging
- Password Capabilities
- Decentralised Password Capabilities
- Summary
Ad-hoc Networks

- Ad-hoc connection: one node directly connects to another.
- Ad-hoc networks: a group of ad-hoc connections.
Ad-Hoc Networks (cont.)

Emergent network, no extra infrastructure necessary.
Cooperation

- Independence from infrastructure, but reliance on shared resources.

- Main resource: network link.
  - Rely on intermediate nodes to pass on packets.

- Other resources:
  - authentication.
  - data encryption.
  - limitless applications -- limitless shareable resources.

- Problem: they might not cooperate if it benefits them.
Resource charging

- Charge resource usage
- Selfish nodes will run out of money

Aim:
- Provide incentive to co-operate
  - Sharing resources
  - Not overusing resources
- Load balancing
Bank

- Where to store money? No commonly trusted node.
- Security and fault tolerance by collective actions:
  - Neighbours: directly connected nodes
  - Neighbours act as bank.
  - Node joining the network is given an account with some amount of money.
  - Banks give the node the 'capability' to withdraw & deposit.
Capabilities

- Fine-grained access control system.
- Grant the possessor a capability to do something to an object.
  - Simplest example: object reference in programming.
- A capability infers a set of access rights.
- Need a way to protect capability.
Password Capabilities

A Password-Capability System: M. Anderson, R.D. Pose, and C. S. Wallace

- Password capability: Location | ID | Password.
- Protection by sparsity: use randomly generated password as name.
- A password capability can be:
  - Passed around (it’s just a data).
  - Derived to a more restrictive capability.
  - Revoked.
Resource charging by password capabilities

- Password capabilities act as cheques.
- Bank gives client node the capability to withdraw $X amount of money.
- That capability act as a cheque, and can be passed to other nodes as payment.
- Bank also gives capability to deposit, given a withdraw capability as parameter.
- Uses Distributed Hash Tables to route capabilities to the right nodes.
1. A exercise its deposit capability with B’s cheque as parameter.
2. BankA sends request to BankB to decrement B’s account by $X$ amount.
3. BankB complies
4. BankB sends acknowledgement to BankA
5. BankA increments A’s Account by $X$ amount.
Side notes

- No charging if resources isn’t scarce.
- Generalisation of dpcap:
  - Can be used as general capability-based access control system for any data in Distributed Hash Tables.
  - Problem: operating on encrypted data.
Co-operation is necessary for ad-hoc networks to work.

Described a reliable, flexible, secure and decentralised resource charging system that stimulates cooperation by limiting usage based on community work.

Which also balances network load.
Future works

- What’s done:
  - Protocol design
  - Security analysis

- Future works:
  - Implementation
  - Simulation
  - Finding good parameters