Self-organization in Ad Hoc Networks

Jean-Pierre Hubaux
EPFL

http://lcawww.epfl.ch/hubaux

Introduction

- Ad hoc networks are expected to run autonomously, at least for a given period of time
- No infrastructure ➔ The nodes have to provide all the mechanisms
- This situation calls for self-organized solutions
- Routing in ad hoc networks is an example of self-organized mechanism
  - Proposed solutions (DSR, AODV,…) are different from the conventional ones (RIP,OSPF, BGP,…)
  - Many new proposals, including very recent ones (FRESH and GOAFR, Mobihoc 2003)
  - Unsolved problem: definition of rigorous, quantitative comparison techniques

Ad Hoc Networks are not just About Routing

Other research topics have been identified and investigated, in particular:

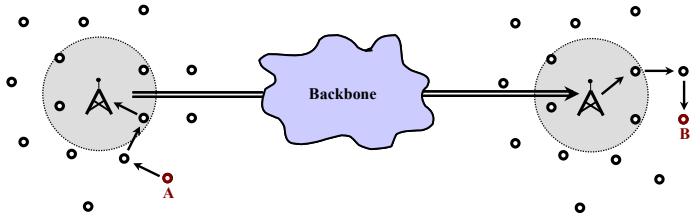
- Appropriate MAC layer (IEEE 802.11 was not designed for multi-hop ad hoc networks and is notoriously unfit for them)
- Power management (impact on connectivity, on interferences,…)
- Transport layer (behaviour of TCP flows over multi-hop wireless links,…)
- Multicast
- Group communication
- **Cooperation**
- **Security**

Cooperation in Ad Hoc Networks

- Problem: assuming that each node is its own authority, how can cooperation be encouraged (or enforced)?
- Main proposals so far (chronological order):
  - Marti et al. (Stanford, Mobicom 2000):
    - *Watchdog:* identification of misbehaving nodes
    - *Pathrater*: construction of routes avoiding these nodes
  - Buttyan & Hubaux (EPFL, Mobihoc 2000): *Nuglets* (virtual currency)
  - Buchegger & Le Boudec (EPFL, Mobihoc 2002): Reputation system
  - Michiardi & Molva (Eurécom, IFIP-CMSC 2002): Reputation system
  - Zhong et al. (Yale University, Infocom 2003): SPRITE
    - (Off-line) central authority that collects receipts from the forwarding nodes and increases/decreases their accounts
  - Srinivasan et al. (UCSD, Infocom 2003):
    - Can cooperation exist without incentive mechanisms?
    - Study of Nash equilibria on a simplified network model
  - Lamparter et al. (NEC Europe, J. of Computer Comm., 2003)
    - A wireless ISP authenticates the nodes and rewards the well-behaving ones
- No solution is likely to work completely independently from a backbone

Our Solution for Multi-hop Cellular Networks

- **Multi-hop cellular networks** combine the characteristics of cellular and ad hoc networks
- Set of base stations connected to a backbone
- Cell = The geographic area under the control of a base station
- A node beyond the the reach of the base station coverage can use other mobile stations as relays



- Expected Advantages:
  - Increase the coverage of the network
  - Small number of base stations (fixed antennas)
  - Reduce the energy consumption of the sending mobile station
  - Immediate side effect: Reduced interference

Problem Statement

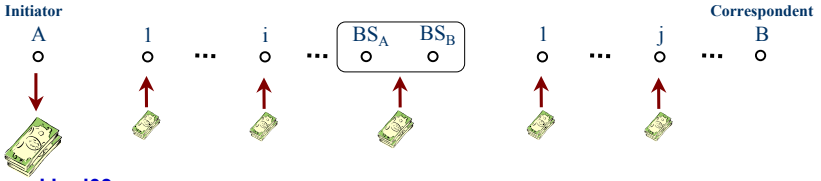
- Multi-hop cellular networks represent a new and promising paradigm, but …

Why would the intermediate nodes use their battery to relay packets for other nodes?

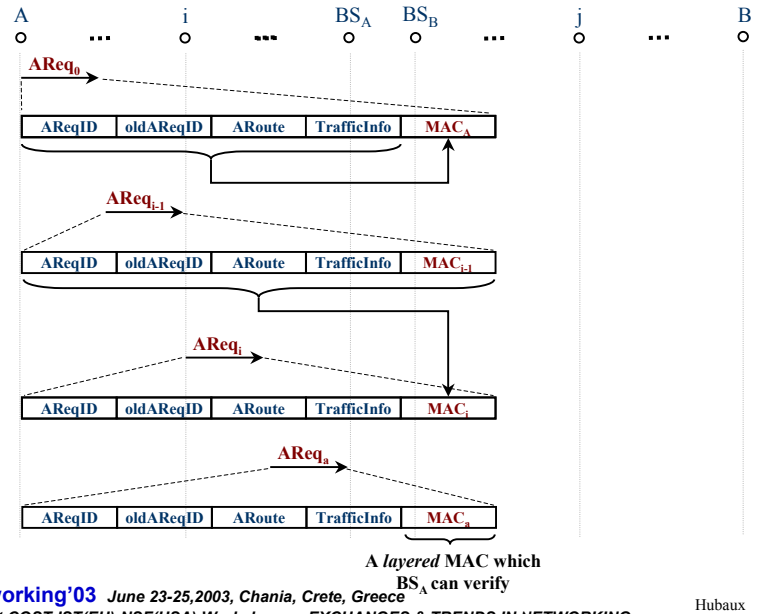
- No cooperation = back to conventional cellular networks

Charge the initiator A of the communication
Reward the cooperative forwarding nodes (and the operator)

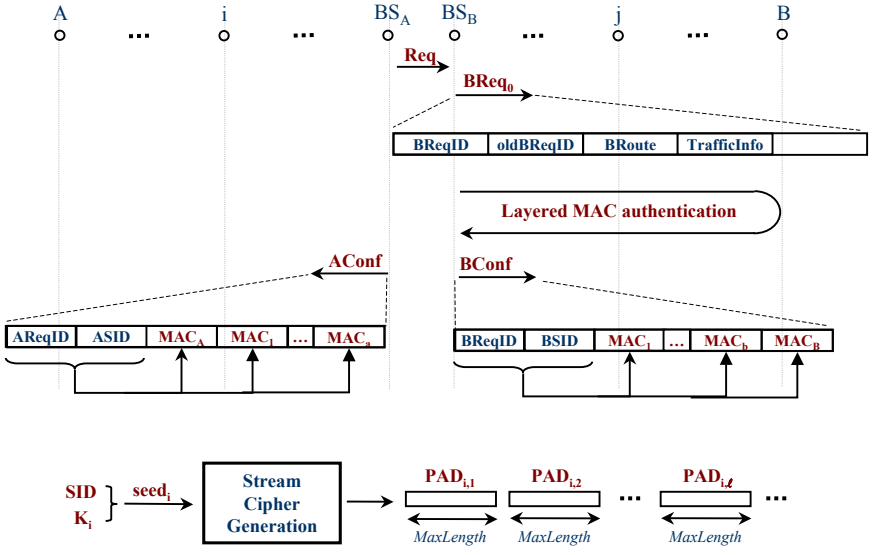
- We exclusively consider the packet forwarding service



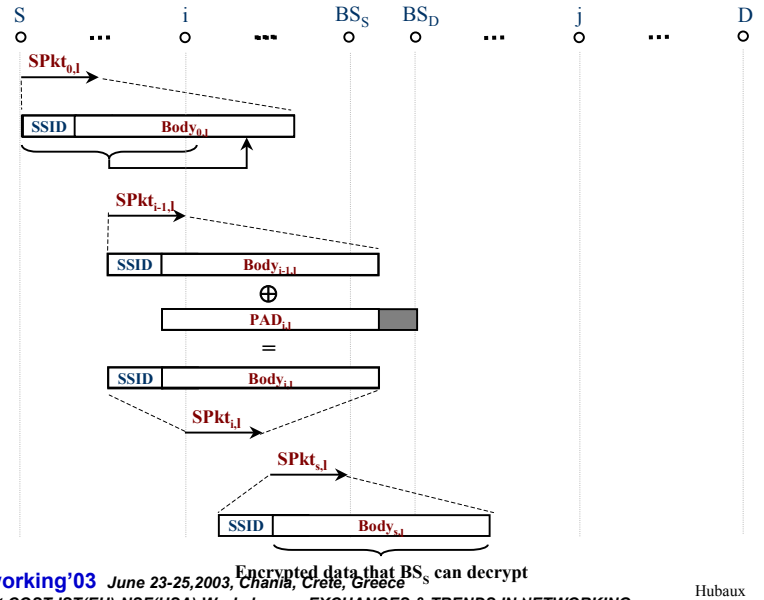
Session Setup (1/2)



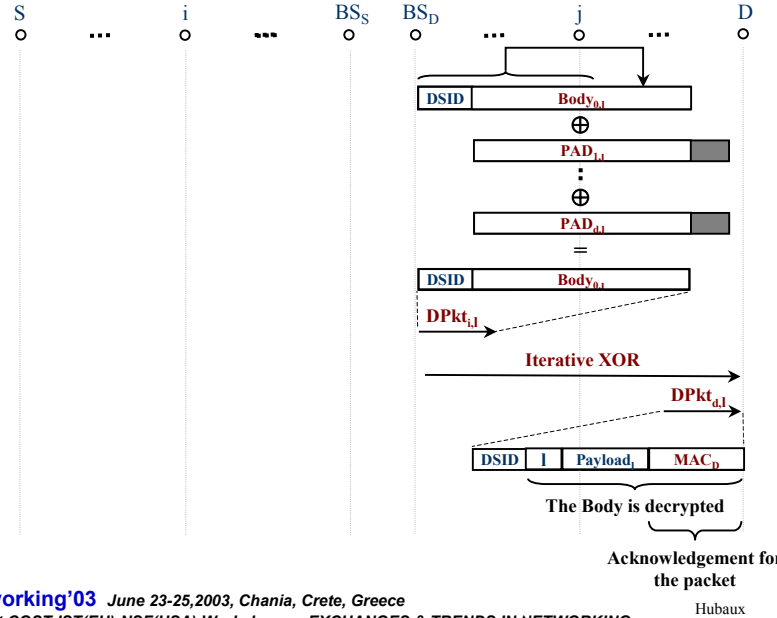
Session Setup (2/2)



Packet Sending (1/2)



Packet Sending (2/2)



Conclusion on Cooperation in Multi-Hop Cellular

- We have proposed a solution based on a charging and rewarding mechanism
- We were able to prove that the protocol encourages cooperation and that it resists a number of attacks
- We have quantified the life time of the sessions and shown that the usage of our scheme leads to a very moderate overhead

Note: The cooperation of nodes in multi-hop cellular networks involves the authority (hence it is *not* fully self-organized)

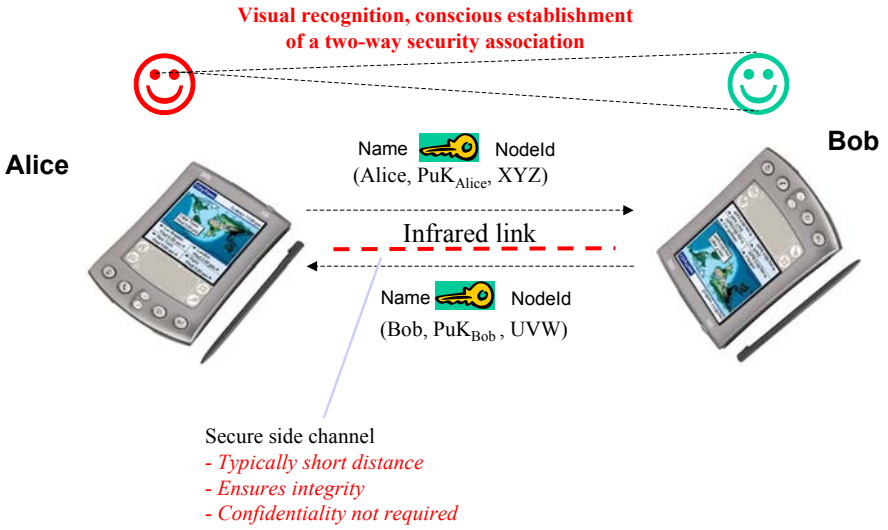
Ongoing work:

- Malicious attacks
- Routing misbehavior
- Several operators
- Charge the correspondent

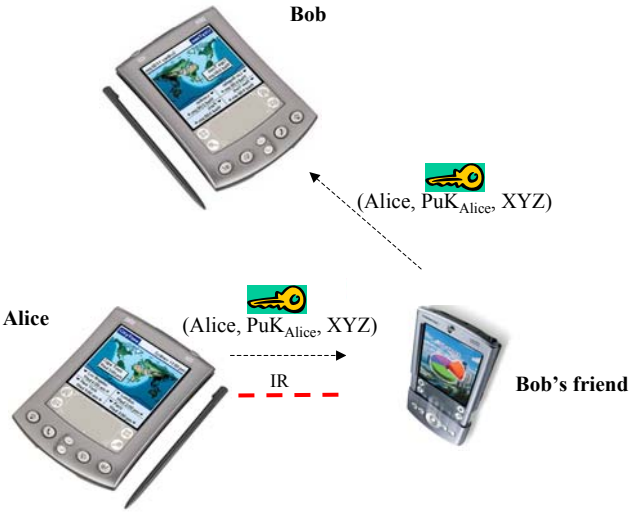
Building up Security Associations in Fully Self-organized Ad Hoc Network

- Problem statement: build up security associations between users in an ad hoc network without any authority or any server
- Definition: If a user *i* can relate the name (or the face) of another user *j* to his (*j*'s) public key, there is a one-way security association (SA) from *i* to *j*
- Technique: establish the SAs by means of a secure side channel (SSC)

Establishment of security associations



Friends…

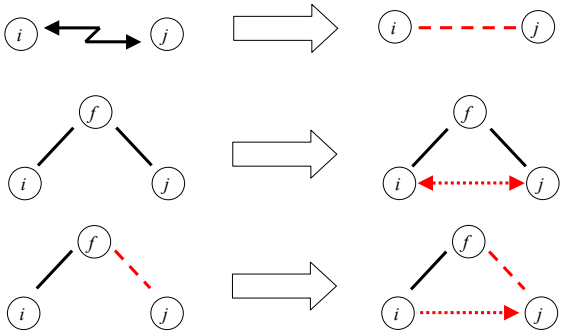


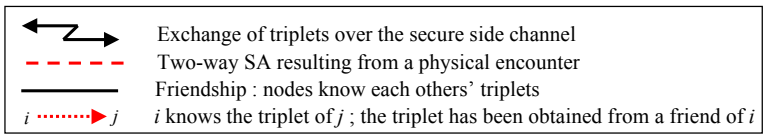
Mechanisms to establish Security Associations

a) Encounter and activation of the SSC

b) Mutual friend

c) Friend + encounter





Note: there is no transitivity of trust (beyond your friends)

Protocols

Protocol 1: Direct Establishment of a Security Association (a)		
msg1	$i \rightarrow j:$	$r_i \mid u_i \mid k_i \mid a_i$
msg2	$j \rightarrow i:$	$r_j \mid u_j \mid k_j \mid a_j$
	$i:$	$u_j?;\ match(k_j, a_j)?$
	$j:$	$u_i?;\ match(k_i, a_i)?$
msg3	$i \rightarrow j:$	$\sigma_i(r_j \mid u_i \mid u_j)$
msg4	$j \rightarrow i:$	$\sigma_j(r_i \mid u_j \mid u_i)$

Protocol 1': Direct Establishment of a Security Association (b)		
msg1 (secure side ch.)	$i \rightarrow j:$	$a_i \mid \xi_i = h(r_i \mid u_i \mid k_i \mid a_i)$
msg2 (secure side ch.)	$j \rightarrow i:$	$a_j \mid \xi_j = h(r_j \mid u_j \mid k_j \mid a_j)$
msg3 (radio ch.)	$i \rightarrow j:$	$r_i \mid u_i \mid k_i \mid a_i$
msg4 (radio ch.)	$j \rightarrow i:$	$r_j \mid u_j \mid k_j \mid a_j$
	$i:$	$h(r_j \mid u_j \mid k_j \mid a_j) = \xi_j?;\ u_j?;\ match(k_j, a_j)?$
	$j:$	$h(r_i \mid u_i \mid k_i \mid a_i) = \xi_i?;\ u_i?;\ match(k_i, a_i)?$
msg5 (radio ch.)	$i \rightarrow j:$	$\sigma_i(r_j \mid u_i \mid u_j)$
msg6 (radio ch.)	$j \rightarrow i:$	$\sigma_j(r_i \mid u_j \mid u_i)$

Protocol 2: Friend-Assisted Establishment of a Security Association		
msg1	$i \rightarrow f:$	$req : u_j \mid r_i$
msg2	$f \rightarrow i:$	$u_j \mid k_j \mid a_j \mid \sigma_f(r_i \mid u_j \mid k_j \mid a_j)$

Pace of establishment of the security associations

- **Depends on several factors:**
  - Area size
  - Number of communication partners: s
  - Number of nodes: n
  - Number of friends
  - Mobility model and its parameters (speed, pause times, …)

Desired security associations :

$$p_{ij} = \begin{cases} 1 & \text{if } i \text{ wants to know the public key and node address of node } j \\ 0 & \text{otherwise} \end{cases}$$

Established security associations :

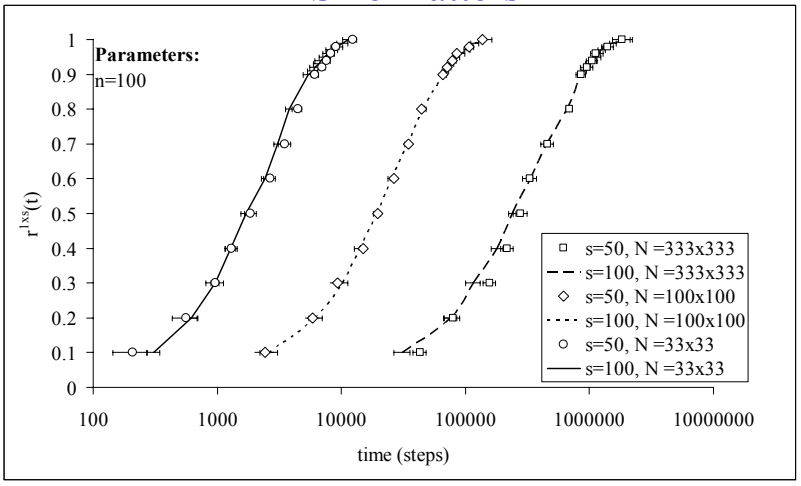
$$e_{ij}(t) = \begin{cases} 1 & \text{if, at time } t, \ i \text{ knows the public key and node address of node } j \\ 0 & \text{otherwise} \end{cases}$$

Convergence:

$$r(t) = \frac{\sum_{i,j}^{n} e_{ij}(t) \cdot p_{ij}}{\sum_{i,j}^{n} p_{ij}} \qquad (1)$$

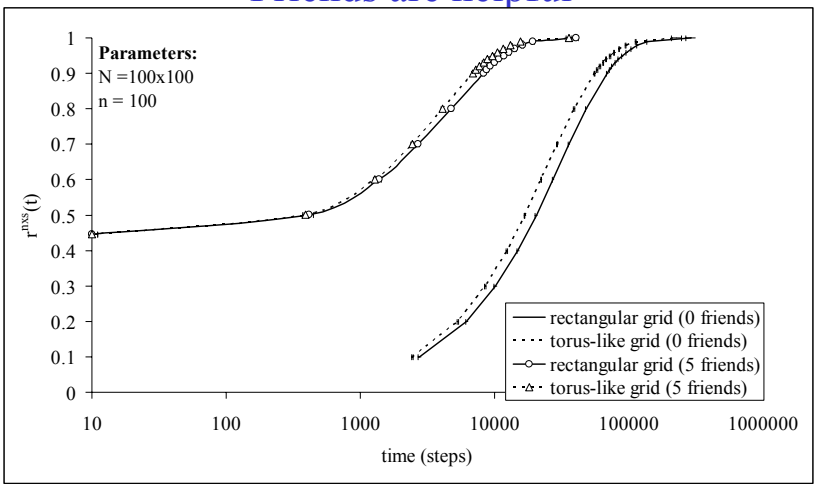
and the **convergence time** t_M is the earliest time at which $r(t_M) = 1$.

Simulation results, random walk (1/2): Size matters



s : number of communication partners
no friends
t_M = O(N logN)

Simulation results, random walk (2/2)
Friends are helpful



$t_M^{(f)} = t_M/(f+1)$

where f is the number of friends

Conclusion on Establishment of Security Associations

- Security can quite easily be fully self-organized
- Mobility is instrumental for this purpose
- The design of the related security protocols is straightforward
- The pace of establishment of the security associations is strongly influenced by the area size, the number of friends, and the speed of the nodes
- The proposed mechanism also supports re-keying

Ongoing work:

- Closed-form expression for the pace of establishment of security associations with random walk
- Application of our scheme to secure routing protocols
- Key revocation
- Improved scalability

Conclusion

- Self-organization is the main challenge for ad hoc networks
- All mechanisms (routing, power control, security,…) in ad hoc networks should be self-organized
- There exist various *degrees* of self-organization (characterized typically by the level of involvement of a backbone, of a central server, or of an authority).

References:

- N. Ben Salem, L. Buttyan, J.-P. Hubaux, and M. Jakobsson: "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks" *MobiHoc* 2003
- S. Capkun, J.-P. Hubaux, and L. Buttyan "Mobility helps Security in Ad Hoc Networks" *MobiHoc* 2003

Papers available at: www.terminodes.org