Security in Wireless Ad hoc Networks

CMS'03

October 2, 2003

Refik Molva
Institut EURECOM
molva@eurecom.fr

Mobile Ad Hoc Networks (MANET)

- Collection of wireless mobile hosts forming a temporary network
- No fixed network infrastructure
- No (or limited) organization

- Military and Emergency
- Sensor Networks
- Civilian applications, ubiquitous computing

Trust in MANET

- Managed environment
  - A-priori trust
  - Entity authentication $\Rightarrow$ correct operation
  - But:
    requirement for authentication infrastructure

- Open environment
  - No a-priori trust
  - authentication does not guarantee correct operation
  - *New security paradigm*

Node Misbehavior

Selfish Nodes

- Do not cooperate
- Priority: battery saving
- No intentional damage to other nodes.
- **Exposure:**
  - passive denial of service
  - black hole
  - idle status

Malicious Nodes

- Goal: damage to other nodes
- Battery saving is not a priority
- **Exposure:**
  - active attacks
  - denial of service
  - traffic subversion
  - attacks exploiting the security mechanism

MANET Requirements

Wireless & Mobile

- Limited Energy
- Lack of physical security

Ad Hoc

- No(or limited) infrastructure
- (Lack of organization)

- Cooperation Enforcement
- Secure Routing
- Key management

Cooperation Enforcement in MANET

- Routing and Packet Forwarding cost energy.
- Selfish node saves energy for itself
- Without any incentive for cooperation network performance can be severely degraded.

[Michiardi, Molva EW'02]

Cooperation enforcement mechanisms

Token-based [Yang,Meng,Lu] } Threshold cryptography

Nuglets [Buttyan,Hubaux]
SPRITE [Zhong, Chen, Yang] } Micro-payment

CONFIDANT [Buchegger,Le Boudec]
CORE [Michiardi,Molva]
Beta-Reputation [Josang,Ismail] } Reputation-based

CORE

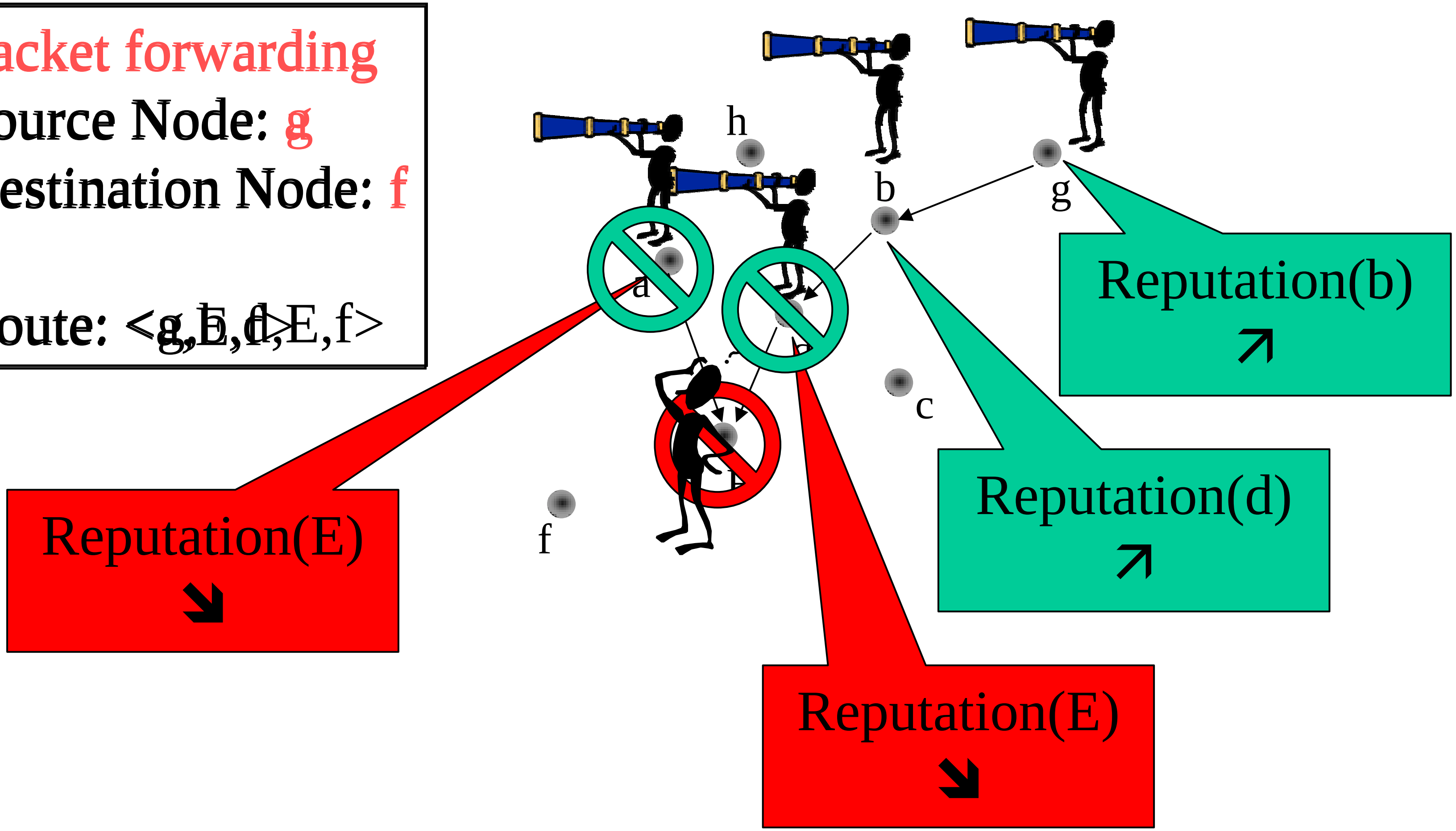
Packet forwarding

Source Node: g

Destination Node: f

Route: <g,b,d,E,f>

Route: <g,E,f>



Cooperation Enforcement Evaluation with Game Theory

- Cooperative GT
  - Study the ***size*** (***k***) of a ***coalition*** of cooperating nodes

utility function $: U(k) = \alpha_i \, u(y_i) + \beta_i \, r(\sigma_i)$

relative share $: \sigma_i = \dfrac{y_i}{\sum_j y_j}$

  - Nash Equilibrium $\rightarrow$ lower bound on ***k***

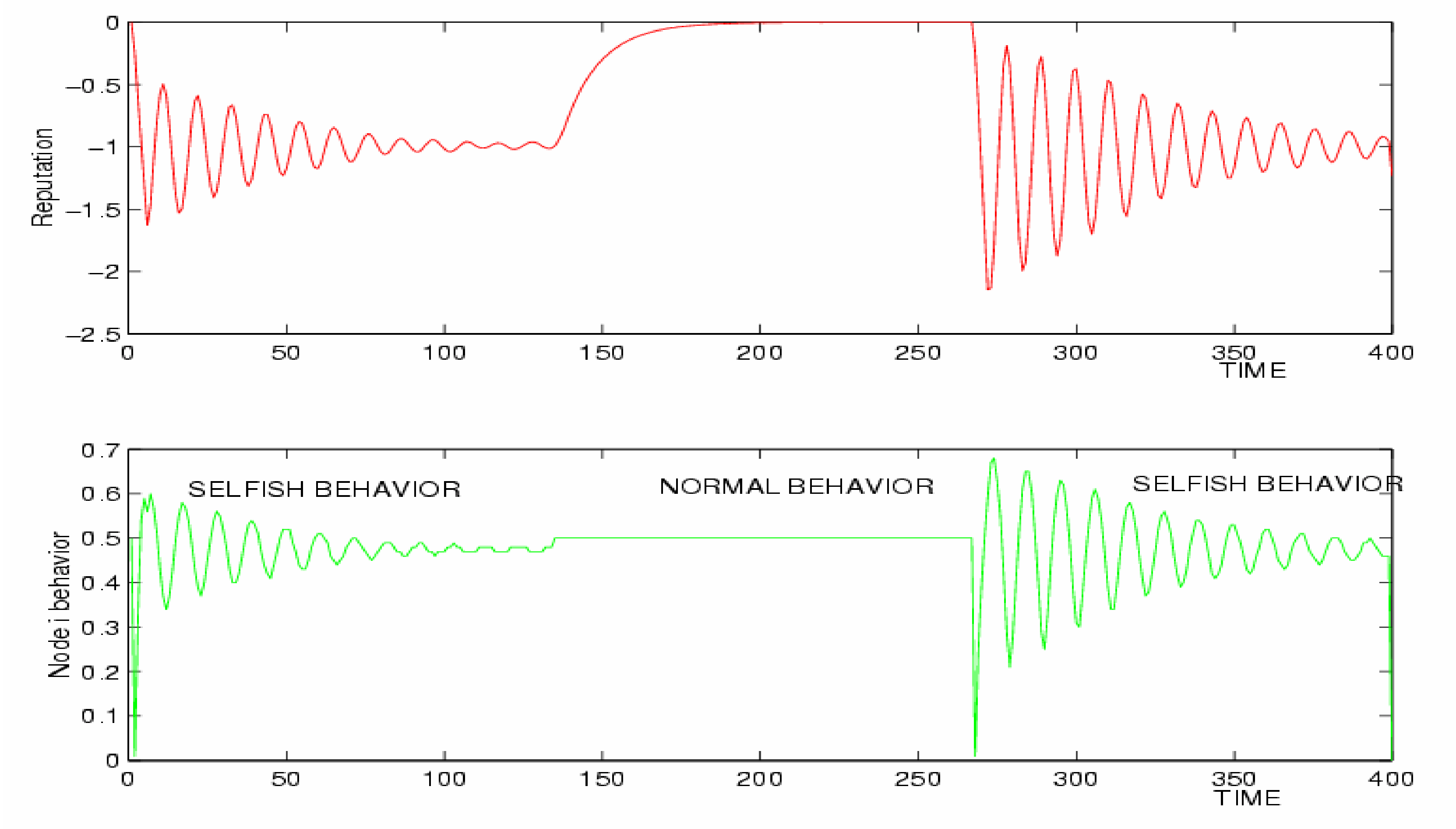
- Non-cooperative GT
  - Utility function with ***pricing***

$$u_i(b_i, b_j) = f(E_{self}, E_R, E_{PF}, b_i, b_j, r_i)$$

  - Pricing used to guide the operating point (i.e. maximum of utility function) to a fair position
  - r_i: dynamic reputation of node n_i evaluated by her neighbors

[Michiardi,Molva,CMS'02, WiOpt'03] [Srinivasan,et al.,INFOCOM'03]

Non-cooperative GT with pricing



Secure Routing - Vulnerabilities

- Modification
- Impersonation
- Fabrication
- Wormhole attack
- Lack of cooperation

Secure Routing - Objectives

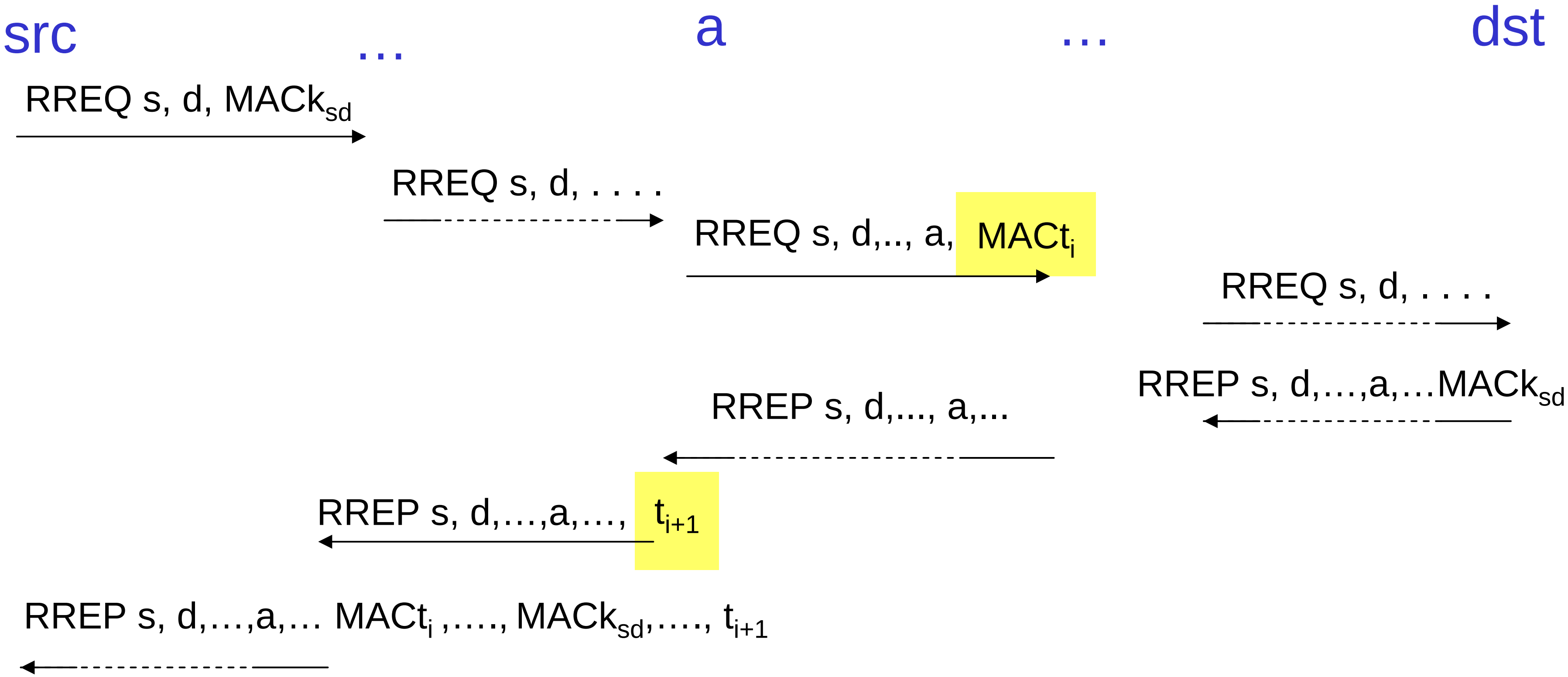
- Authentication (Integrity) of routing information
- Entity authentication
  - Source
  - Destination
  - Intermediate node
- Correct behavior (of algorithm, if any)
- Asymmetric vs. Symmetric Crypto
- Pro-active vs. Reactive routing protocols

Routing in MANET

- Reactive (on-demand)
  - Dynamic Source Routing (DSR)
  - Ad Hoc On-demand Distance Vector (AODV)
- Pro-active
  - Destination Sequenced Distance Vector (DSDV)
  - Optimized Link State Routing (OLSR)
- Hybrid
  - Zone Routing Protocol (ZRP)
  - Distributed Dynamic Routing (DDR)
- Location-based
  - Location-Aided Routing (LAR)

ARIADNE [Hu, et al.]

- On-demand Routing Protocol DSR
- k_{sd}: shared secret known by (src, dst)
- $t_i = h^{n-i}$(secret): TESLA key of a node valid for time interval T_i disclosing t_{i+1} in T_{i+1} authenticates the node



Prerequisite: distribution of authenticated TESLA keys (h^n(secret))

Other Secure Routing Proposals for MANET

- Secure Routing Protocol [Papadimitriou, Haas]
  - security associations between source end destination only
- ARAN [Dahill, et al.]
  - PK certificates for IP @
- SEAD [HU, et al.]
  - proactive routing authenticated hash chains
- TESLA with instant key disclosure (TIK)
  - can cope with wormhole attack

Secure Routing Summary

- No new requirement other than self-organized key management

- All solutions rely on some key set-up prior to secure routing operation

- Contradiction: long-lived security associations in self-organized MANET

Key Management Requirements

- Secure routing
- Basic security services
  - Authentication
  - Confidentiality
  - Integrity
  - Non-repudiation
- Symmetric or Asymmetric Keys

Key Management Challenges

Lack of (or limited)

- Security infrastructure
  - Key servers (KDC, CA, RA)
- Organization (a priori trust)
  - p2p
  - Authentication is not sufficient to build trust

Key Management Objectives

- Bootstrapping from scratch
- Fully distributed
- Minimum dependency

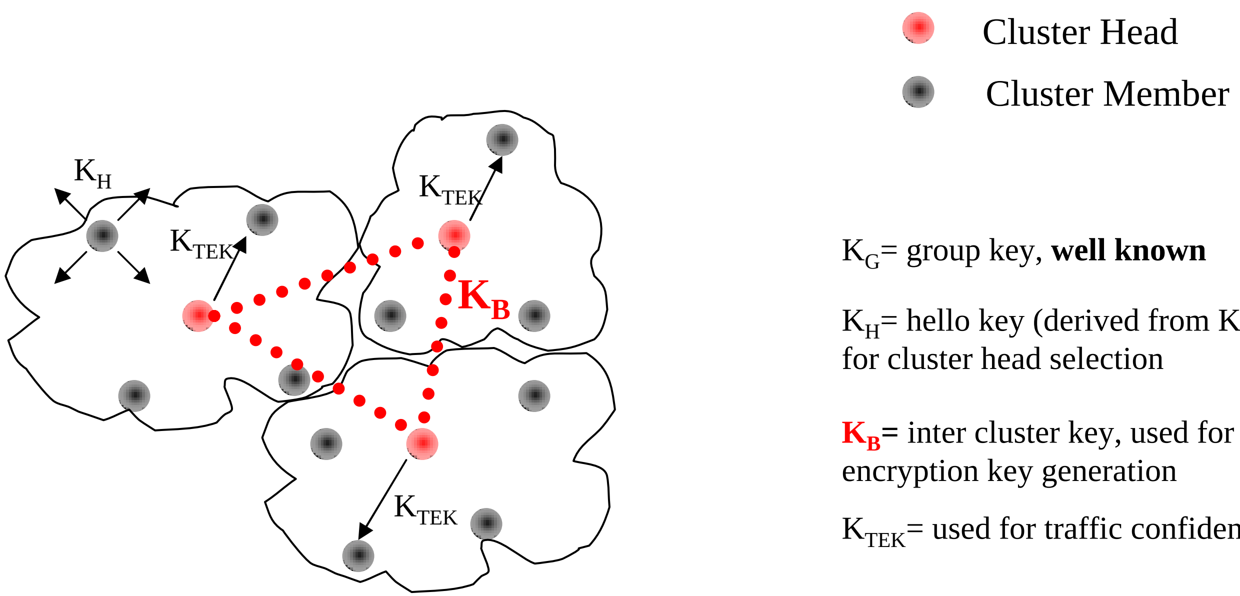
Key Management Approaches

- Based on symmetric crypto
- (ID, PK) binding
  - PK Certificate = $(ID,PK)_{CA}$
    - Self-organized CA
    - Web of trust(PGP)
  - No certificate
    - Crypto-based IDs: ID = h(PK)
    - ID-based Crypto: PK = f(ID)
- Context-dependent authentication
  - location-limited channels
  - Shared passwords

Key Management Based on Symmetric Cryptography

Secure Pebblenets [Basagni et al.]

- cluster formation algorithm



K_G= group key, **well known**

K_H= hello key (derived from K_G), used for cluster head selection

K_B= inter cluster key, used for traffic encryption key generation

K_{TEK}= used for traffic confidentiality

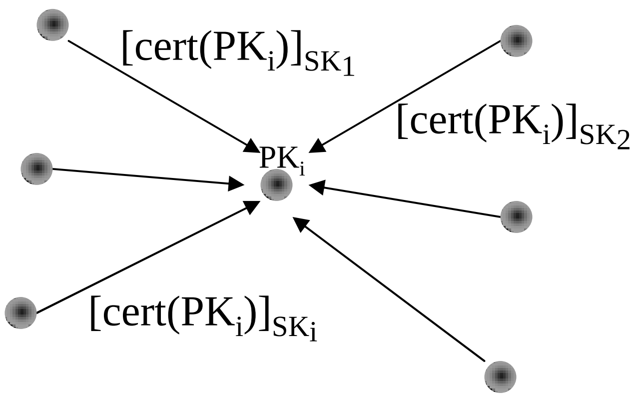
Assumption: no malicious nodes

(ID, PK) binding

Self-organized CA

[Zhou, Haas] [Kong, et al.] [Yi, Kravets] [Lehane, et al.]

- Based on threshold cryptography



$$CERT(PK_i)_{SK} \left\{ \begin{array}{l} [cert(PK_i)]_{SK_1} \\ [cert(PK_i)]_{SK_2} \\ \ldots \\ \\ [cert(PK_i)]_{SK_i} \\ \ldots \end{array} \right.$$

Verification of $CERT(PK_i)_{SK}$ by any node using well known PK

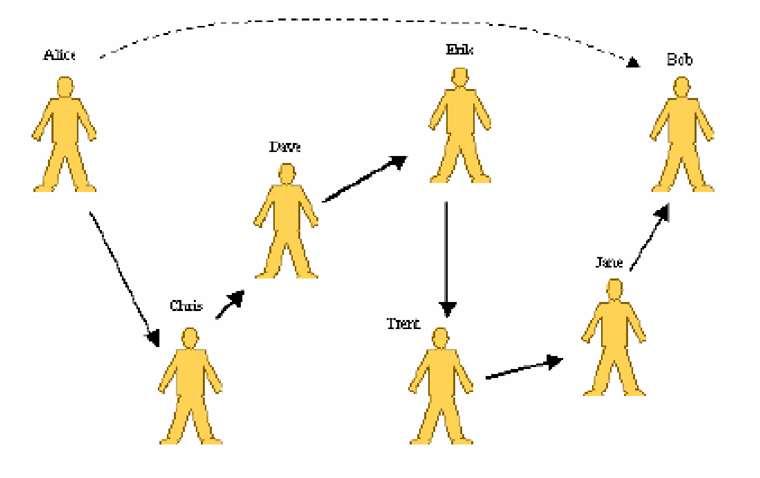
- PROs: distributed, self-organized
- CONs: share distribution during bootstrap phase, network density, Sybil attack

(ID, PK) binding

Web of Trust (PGP)

[Hubaux, Buttyan, Capkun]

- No CA
- Alice $\rightarrow$ Bob and Bob $\rightarrow$ Eve $\Rightarrow$ Alice $\rightarrow$ Eve
- Merging of certificate repositories



- PROs: no centralized TTP
- CONs: initialization, storage, transitivity of trust

(ID, PK) binding

Crypto-based ID

- SPKI [Rivest]
- Statistically Unique Cryptographically Verifiable IDs [O'Shea, Roe] [Montenegro, Castellucia]

  IPv6 @ = NW Prefix | h(PK)
- DSR using SUCV-based IP addresses [Bobba, et al]

PROs: no certificates, no CA

CONs: generation of bogus IDs

(ID, PK) binding

ID-based Crypto

[Halili, Katz, Arbaugh]

[Boneh, Franklin, CRYPTO 2001]

- ID-based
  - PK = h(ID)
  - SK computed by TTP

- Threshold Crypto to distribute TTP

PROs: no certificates, no centralized server

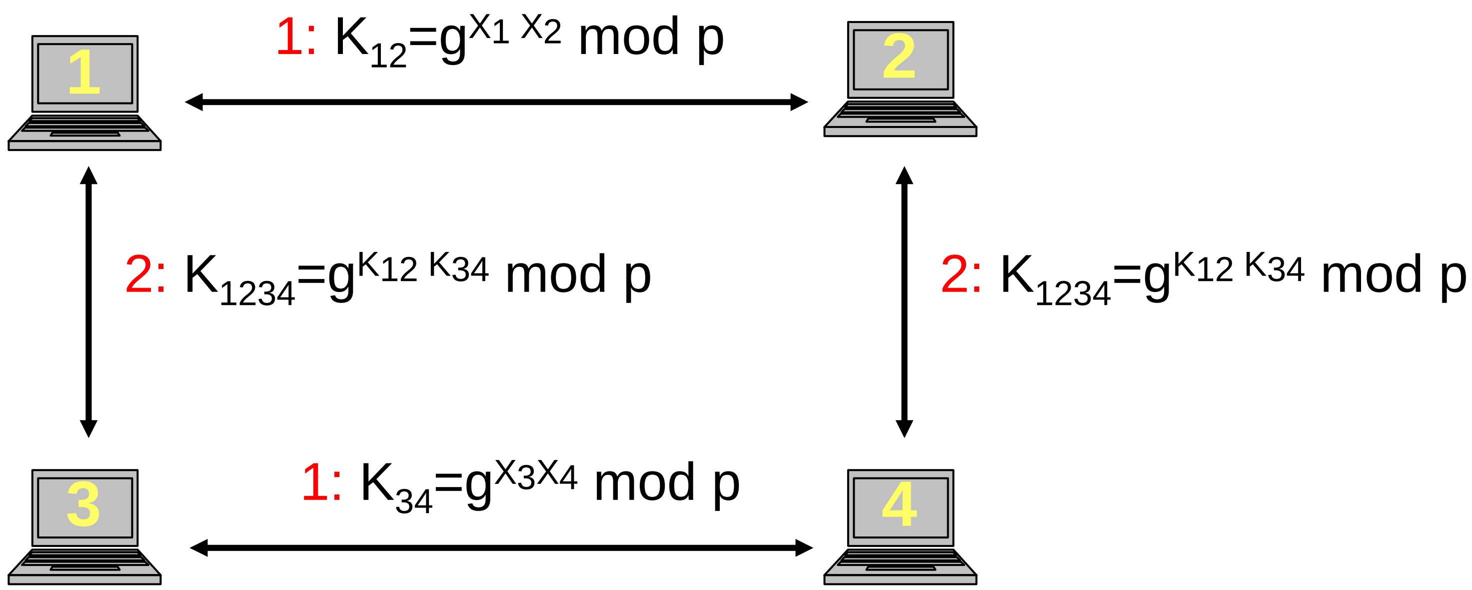
CONs: distribution of initial shares

Context-dependent Authentication

Password Authenticated Key Exchange

[Asokan, Ginzborg]

HyperCube Protocol (Diffie-Hellman)



PROs: self-organized, fully distributed

CONs: shared password

Context-dependent Authentication

Secure channel

- [Balfanz, et al.] establish pairwise security association based on vicinity of devices
- [Capkun, et al.] secure channel + web of trust
- PROs: self-organized, fully distributed
- CONs: reliance on secure side channel

Layer 2 vs MANET Security

- IEEE 802.11 and Bluetooth
  - weaknesses
  - secure extensions to wireline networks
- Layer 2 mechanisms in MANET
  - managed environments: L2 sufficient if node integrity is guaranteed (tamper-proof HW)
  - open environments (no a priori trust): L2 cannot cover higher layer (3,4, ..) security

State of the art - Summary

- Specific requirements
  - Cooperation enforcement
  - Bootstrapping security associations
- Solutions yet to come . . .
- Interesting applications of cryptography
- Some untruths and non-sense

Main Flaw

- Security requirements in MANET are stronger than in “classical” networks.
- MANET networking still is a research topic
- Security retrofitted as add-on mechanisms as if network technology was established.

Right Approach

- Address security at early stages of protocol design: i.e. Routing Protocol dealing with Routing+Cooperation+Key Management

- Old model based on verification of credentials and authentication not suitable, identities are meaningless

- Further develop & integrate new concepts
  - A *posteriori* trust (based on observation, reputation, imprinting)
  - Partial assurance
  - Substitute infrastructure with context information (location, physical distance, history)
  - . . . . Others to be invented

Conclusion

- Wireless Ad Hoc Security still in its infancy
  - Lack of integrated approach
  - Looking for suitable new paradigms
  - Partial coverage (privacy, intrusion detection, physical attacks, etc.)

$\Rightarrow$ Room for creativity

THANK YOU