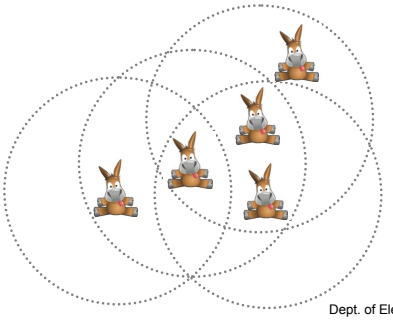
# Security for Future Wireless and Decentralized Communication Networks

## Harnessing Cooperation, Space, and Time

TECHNISCHE UNIVERSITÄT DARMSTADT



**André König, Matthias Hollick, Ralf Steinmetz**

FirstName.LastName@KOM.tu-darmstadt.de
Tel.+49 6151 166150

KOM - Multimedia Communications Lab
Prof. Dr.-Ing. Ralf Steinmetz (Director)
Dept. of Electrical Engineering and Information Technology
Dept. of Computer Science (adjunct Professor)
TUD – Technische Universität Darmstadt
Merckstr. 25, D-64283 Darmstadt, Germany
Tel.+49 6151 166150, Fax. +49 6151 166152
www.KOM.tu-darmstadt.de

3. Juli 2008

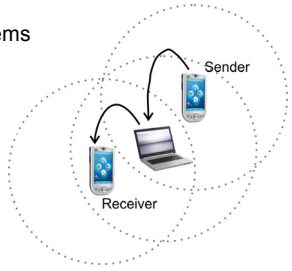


## Motivation

TECHNISCHE UNIVERSITÄT DARMSTADT

**Decentralized Systems**

- Enable communication beyond borderlines of 'traditional' systems
- Here: Mobile ad hoc networks and peer-to-peer systems




**But: Highly dynamic scenarios, wireless transmission**

→ No well defined network borders
→ Functionality based on cooperation
→ Devices from many administrative domains

**But: No constant availability of devices and services**

→ No central, trusted instances
→ No e.g. RADIUS, Kerberos

**→Decentralized Systems are beyond borderlines of 'traditional' security measures**

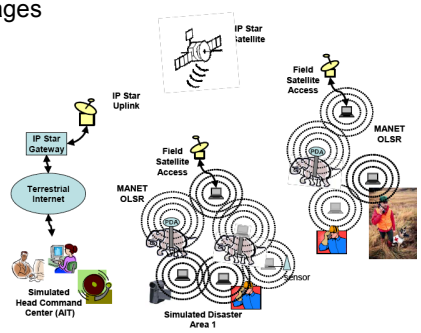
## Motivation (cont'd)

TECHNISCHE UNIVERSITÄT DARMSTADT

### DUMBO (Digital Ubiquitous Mobile Broadband OLSR)

- Research project of Thailand, France, and Japan
- Communication services for emergency response scenarios
- Designed for wide area deployment (natural disasters)
- Offers video streaming, VoIP, text messages

Source: [Kanchanasut2007a]




Source: [Kanchanasut2007b]



## Harnessing Cooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

### Idea: Counterbalance missing trusted instances

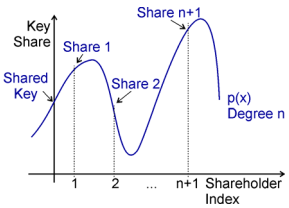
- Enforce cooperation for security relevant decisions
- Distribute required cryptographic operations


### Alternative: Threshold Cryptography

- Based on Shamir's secret sharing [Shamir1979a]
- One cryptographic key distributed among multiple peers
- Enables anonymous cooperation
- E.g. Shoup's threshold signatures [Shoup2000a]

### Alternative: Multisignatures

- Naïve approach: List of signatures and signers
- One cryptographic key per peer
- Enables detailed mapping of administrative structures
- E.g. Boldyreva's multisignatures [Boldyreva2003a]



## Harnessing Cooperation (cont'd)

TECHNISCHE UNIVERSITÄT DARMSTADT

**Challenge: No predefined decision policies**

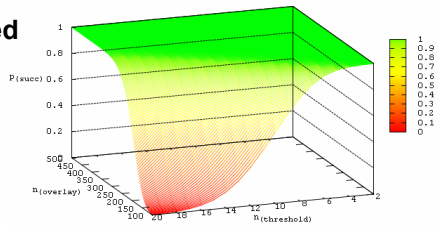
- All security relevant requests in spontaneous networks hard to foresee

**Thus: User interaction may be required**

- To decide on non-predefined requests

**But: Users may not reply in time**

- Sending redundant requests reasonable




**Our Approach: Models for overhead / performance trade-off**

- To offer runtime adaptation of relevant parameters

$$p_{succ} \geq \left( \frac{p_{reply}(n_{gossip} - n_{threshold} + 1)}{(1 - p_{reply})(n_{threshold} - 1)} \right)^{n_{threshold}-1} \cdot \left( \frac{(1 - p_{reply})(n_{threshold} - 1)}{n_{gossip} - n_{threshold} + 1} + (1 - p_{reply}) \right)^{n_{gossip}}$$



## Harnessing Space and Time

TECHNISCHE UNIVERSITÄT DARMSTADT

**Challenge: No gateways, firewalls, …**

- Low-effort attacks on network possible

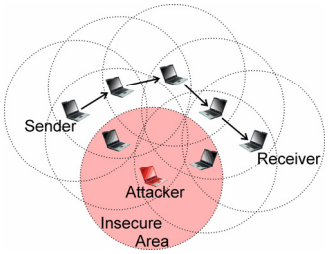
**Thus: Exclusion of misbehaving devices required**

- Reactive approach seems promising

**But: Devices from many administrative domains**

→ Changing addresses easily possible

→ How to identify misbehaving nodes?

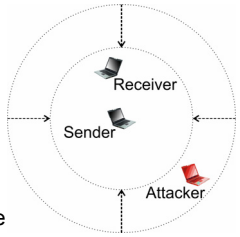



**Our Approach: Location-based intrusion response**

- Quarantine zones as temporal network borders

**Further Enhancements**

- Adaptive transmission power to reduce size of quarantine zones
- Harnessing delay tolerance
  - E-mail, SMS, ... may be delayed until node left quarantine zone

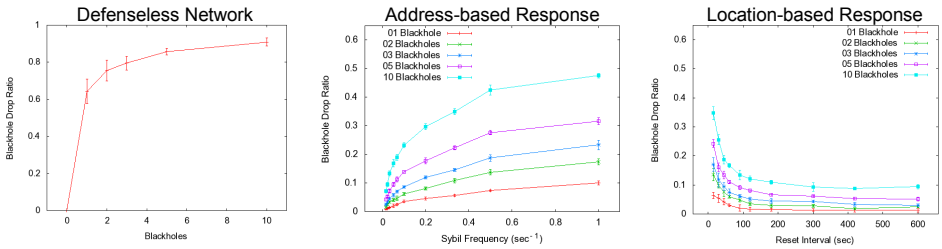


## Harnessing Space and Time (cont'd)

TECHNISCHE UNIVERSITÄT DARMSTADT

**Comparison of address-based and location-based intrusion response**

- When confronted with black hole and Sybil attack
- 1000 nodes, 7-8 neighbors, pedestrian speed, 1 hour simulated time
- Metric: Drop ratio caused exclusively by black hole nodes






## Thanks for Your Attention!

TECHNISCHE UNIVERSITÄT DARMSTADT

Department of Electrical Engineering
and Information Technology
**Multimedia Communications Lab - KOM**

TECHNISCHE UNIVERSITÄT DARMSTADT

Dipl.-Inform. André König

Andre.Koenig@KOM.tu-darmstadt.de
Merckstr. 25
64283 Darmstadt
Germany

Phone +49 (0) 6151/166137
Fax +49 (0) 6151/166152
www.kom.tu-darmstadt.de

**Further Information**

- www.kom.tu-darmstadt.de/en/research/security/overview
- www.kom.tu-darmstadt.de/en/people/staff/andre-koenig

## References


- [Kanchanasut2007a] Kanchanasut, K.; Tunpan, A.; Awal, M. A.; Wongsaardsakul, T.; Das, D. K. & Tsuchimoto, Y.: Building A Long-distance Multimedia Wireless Mesh Network for Collaborative Disaster Emergency Responses. submitted to IEEE Network Magazine, 2007
- [Kanchanasut2007b] Kanchanasut, K.; Tunpan, A.; Awal, M. A.; Das, D. K.; Wongsaardsakul, T. & Tsuchimoto, Y.: A Multimedia Communication System for Collaborative Emergency Response Operation in Disaster-affected Areas. Internet Education and Research Laboratory (intERLab), Asian Institute of Technology (AIT), 2007
- [Shamir1979a] Shamir, A.: How to Share a Secret. Communications of the ACM, 1979, 22, 612-613
- [Shoup2000a] Shoup, V.: Practical Threshold Signatures. Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRPYT 2000), Springer, 2000, 1807, 207-220
- [Boldyreva2003a] Boldyreva, A.: Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme. Proceedings of the 6th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003), Springer, 2003, 2567, 31-46