[KHS08-2] *André König, Matthias Hollick, Ralf Steinmetz;* **Security for Future Wireless and Decentralized Communication Networks - Harnessing Cooperation, Space, and Time.** In: Proceedings of the 8th Wuerzburg Workshop on IP: Joint EuroNF, ITC, and ITG Workshop "Visions of Future Generation Networks" (EuroView2008), July 2008. Seite

Security for Future Wireless and Decentralized Communication Networks – Harnessing Cooperation, Space, and Time

André König, Matthias Hollick, Ralf Steinmetz
[Andre.Koenig; Matthias.Hollick; Ralf.Steinmetz]@KOM.tu-darmstadt.de
Multimedia Communications Lab (KOM), Technische Universität Darmstadt

Wireless and decentralized networks enable enhanced communication services beyond the borderlines of 'traditional' centralized, infrastructure-based systems. As an example, projects have been initiated that scrutinize the applicability of a combination of mobile ad hoc networks (MANETs) and Peer-to-Peer (P2P) systems to support on-site units in highly dynamic emergency response scenarios. This new class of networks demands for new security mechanisms. Due to the wireless and infrastructureless nature, MANETs and P2P systems lack the well defined network borders and the central trusted instances on which security mechanisms (Gateways, Firewalls, etc.) deployed in 'traditional' environments are based. Thus, these security mechanisms cannot be transferred directly. In our work, we present security mechanisms that cope with the challenging conditions in wireless and decentralized systems. We show how cooperative decisions can counterbalance missing central instances and how networks being aware of space and time constraints can survive without well defined network borders.

I. Harnessing Cooperation

Security mechanisms that ensure objectives such as authentication and access control are commonly based on central trusted instances. In decentralized P2P systems, the (constant) availability of these central trusted instances cannot be taken as granted. Making security relevant decisions jointly, by a set of authorized peers, is a promising approach to counterbalance missing central trusted instances. This way, a security level that is comparable to that of contemporary security mechanisms can be achieved.

The mathematical foundation for a joint decision process is given by threshold cryptography or multisignatures. Both techniques can be utilized to enforce the cooperation of a specific number $n_{threshold}$ of peers to perform cryptographic operations such as signing certificates that enable the access to restricted resources. Threshold cryptography allows for anonymous voting, whereas multisignatures render the voting traceable and enable a detailed mapping of administrative hierarchies to the structure of the network.

Predefined security policies for any security relevant decision possible will most likely not be available regarding the highly dynamic application domain targeted. Thus, a user interaction may well be required. Minimizing the number $n_{request}$ of users requested for one joint decision is an obvious optimization goal. To describe the trade-off between $n_{request}$ and the probability p_{succ} that a joint decision is successful (i.e. enough peers w.r.t. $n_{threshold}$ issued their votes within a reasonable amount of time), as shown in Figure 1, we developed stochastic models. The derived closed-form description of these models serves as a tool allowing for the online adaptation of key parameters which control the success of joint decisions while guaranteeing low overhead in the network.

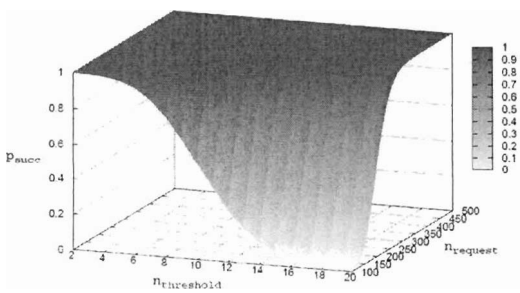


Figure 1: Success probability for cooperative decisions

II. Harnessing Space and Time

Establishing networks without an infrastructure, as it is done in a MANET, requires an accurate cooperation of the nodes involved. Effects of misbehaviour, may it be intended or not, can lead to a massive disruption of the network's services.

A prominent example of (intended) misbehaviour in MANETs is the black hole attack. In analogy to a black hole in astronomy, a black hole in a MANET draws data, which is dropped instead of being forwarded to the actual receiver. Very few of such black hole nodes are sufficient to cause a breakdown of the entire network.

Preventing any misbehaviour possible is hardly feasible. Prevention strategies, though thoroughly designed, have been shown to be susceptible to attacks, recently. However, reactive security measures like intrusion detection systems combined with intrusion response mechanisms offer a promising means to mitigate the effects of misbehaviour in MANETs. While intrusion detection systems have been studied comprehensively, only minor attention has been paid to how to react to intrusions detected. Mostly, response mechanisms which exclude adversaries detected from the network based on their addresses have been proposed. Since devices in MANETs are beyond the control of a central instance, changing addresses is possible with little effort. This way, address-based intrusion response approaches can be subverted easily. For this reason, we have proposed *GeoSec*, a location-based intrusion response strategy. By setting up temporal quarantine zones in areas where misbehaviour has been detected, network traffic is redirected and, thus, is geographically kept away from misbehaving nodes. Figure 2 shows *GeoSec*'s performance compared to a defenseless network and to an address-based response strategy, subject to the data that is dropped by black hole nodes.

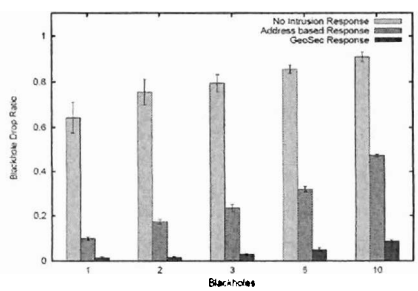
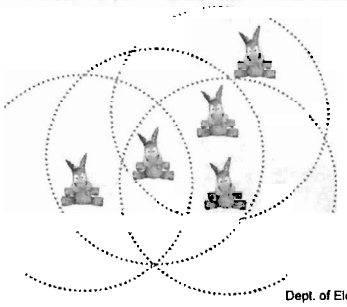


Figure 2: Address-based vs. location-based intrusion response

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

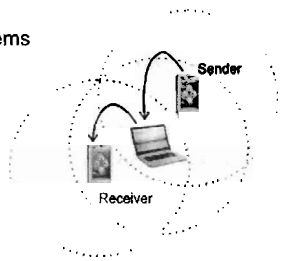
Motivation

TECHNISCHE UNIVERSITÄT DARMSTADT

Decentralized Systems

Enable communication beyond borderlines of 'traditional' systems

- Here: Mobile ad hoc networks and peer-to-peer systems

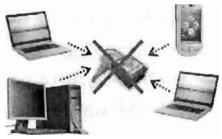


But: Highly dynamic scenarios, wireless transmission

→ 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)

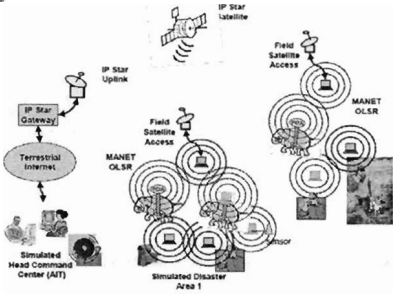
TECHNISCHE UNIVERSITÄT DARMSTADT

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

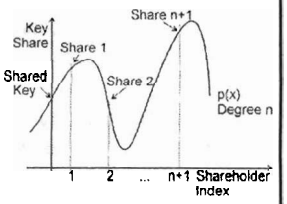
Group of collaborating peers

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

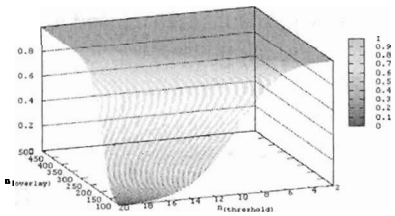
- All security relevant requests in spontaneous networks hard to foresee

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

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

5

Harnessing Space and Time

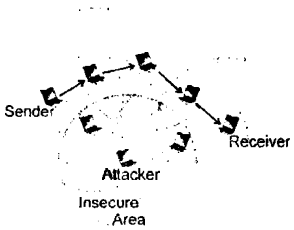
TECHNISCHE UNIVERSITÄT DARMSTADT

Challenge: No gateways, firewalls, ...

- Low-effort attacks on network possible

Thus: Exclusion of misbehaving devices required

Reactive approach seems promising



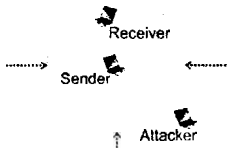
But: Devices from many administrative domains

→ 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

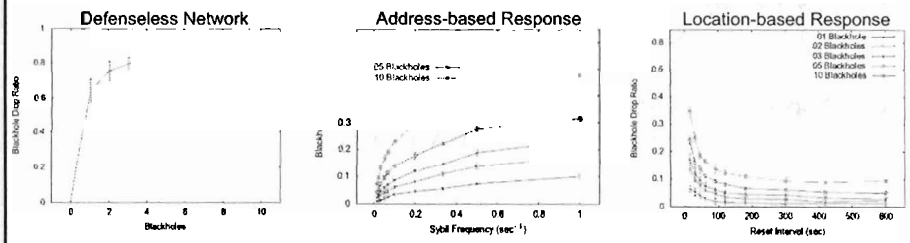
6

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

TECHNISCHE UNIVERSITÄT DARMSTADT

- [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