SAFEST
Social-Area Framework
for Early Security Triggers at Airports

iNET

Hochschule für Angewandte Wissenschaften Hamburg
*Hamburg University of Applied Sciences*

# On Security in the SAFEST Network

Heiner Perrey, Martin Landsmann, Thomas Schmidt

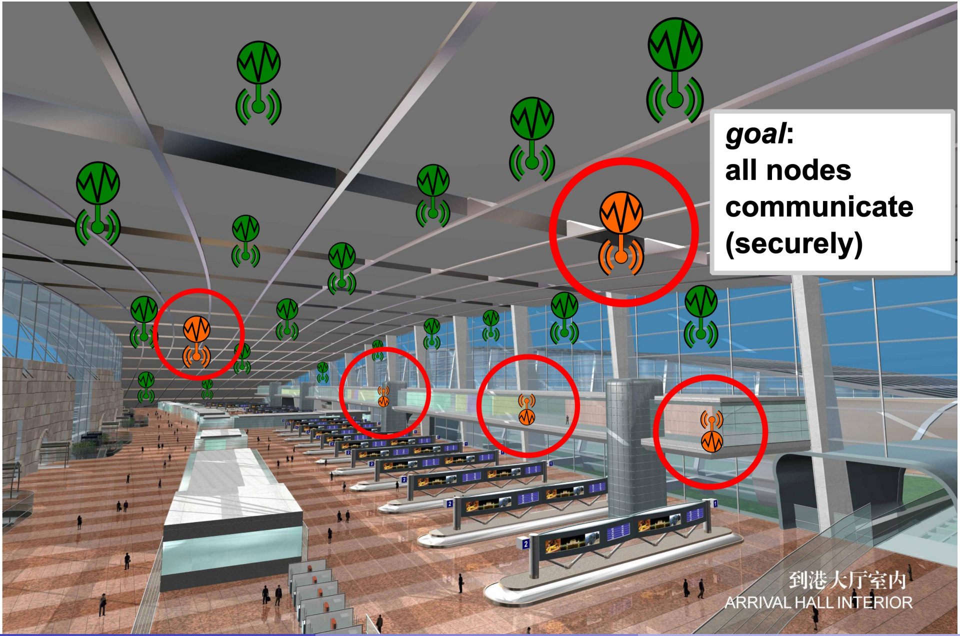
# Overview

1. Motivation for Routing in Low-Power and Lossy Networks
   - Initial Situation: Monitoring Public Places (Airport)
   - Overview on RPL
2. Security Outline on Routing in SAFEST Network
3. Overview and Outlook

# Monitoring Airport: Initial Situation (Picture: [1])

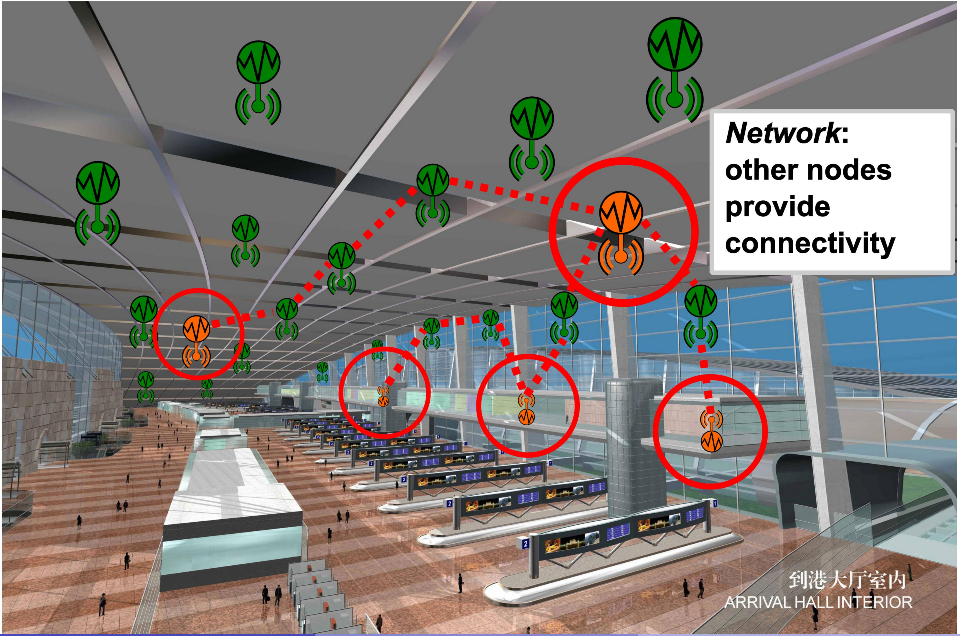
到港大厅室内
ARRIVAL HALL INTERIOR

# Monitoring Airport: Initial Situation (Picture: [1])



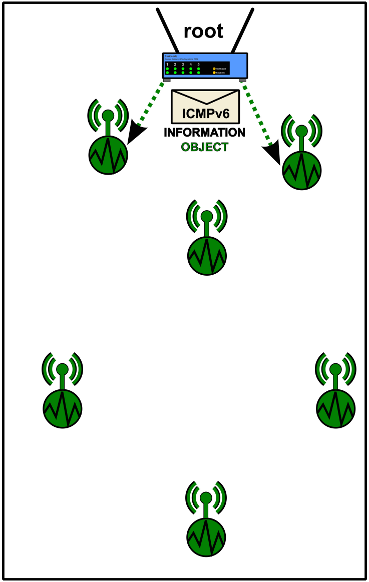
***goal*:**
**all nodes communicate (securely)**

# Monitoring Airport: Routing to Destination (Picture: [1])



***Network*: other nodes provide connectivity**

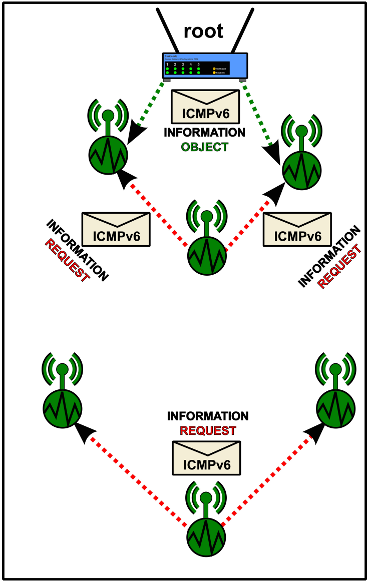
# Routing Protocol For Low-Power and Lossy Networks (RPL): Topology Initialization (RFC [3])



## Creating Routes to the Root

- RPL topology is based on a Destination Oriented Directed Acyclic Graph (DODAG)
- Root begins to send Information Objects (DIO) in ICMPv6 messages
- Nodes may request a DIO using solicitation messages (DIS)

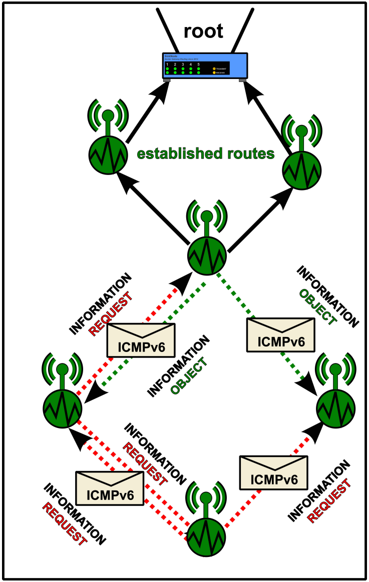
# Routing Protocol For Low-Power and Lossy Networks (RPL): Topology Initialization (RFC [3])



## Creating Routes to the Root

- Nodes may join the DODAG using information in DIO
- Nodes choose a set of parents for forwarding packets
- Each note has a rank (relative position in graph to root)
- Nodes distribute DIO messages

# Routing Protocol For Low-Power and Lossy Networks (RPL): Topology Initialization (RFC [3])



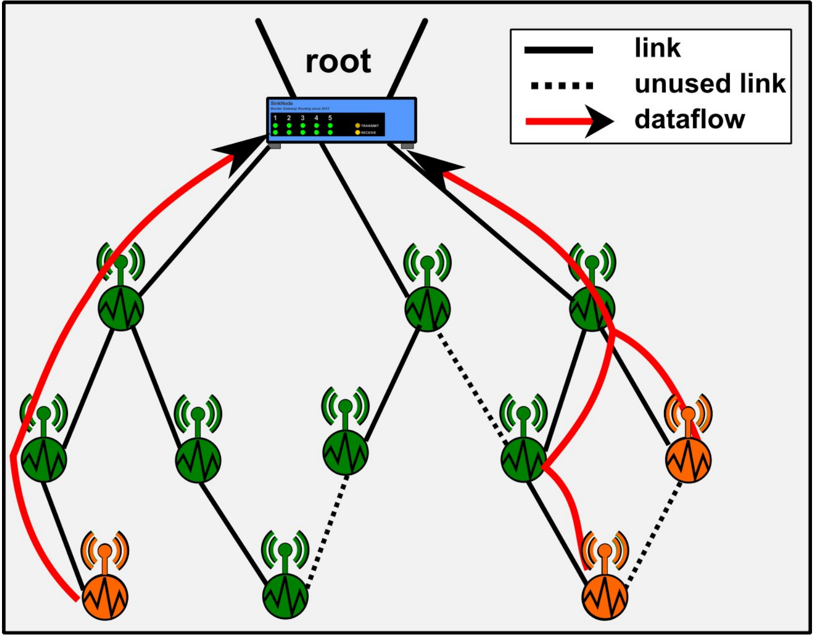
## Topology:

- DIO messages build Upward-routes (towards the root)
- Destination Advertisements (DAO) build downward routes
- Initially topology is created (proactive), inconsistencies (e.g. loops) are detected reactively

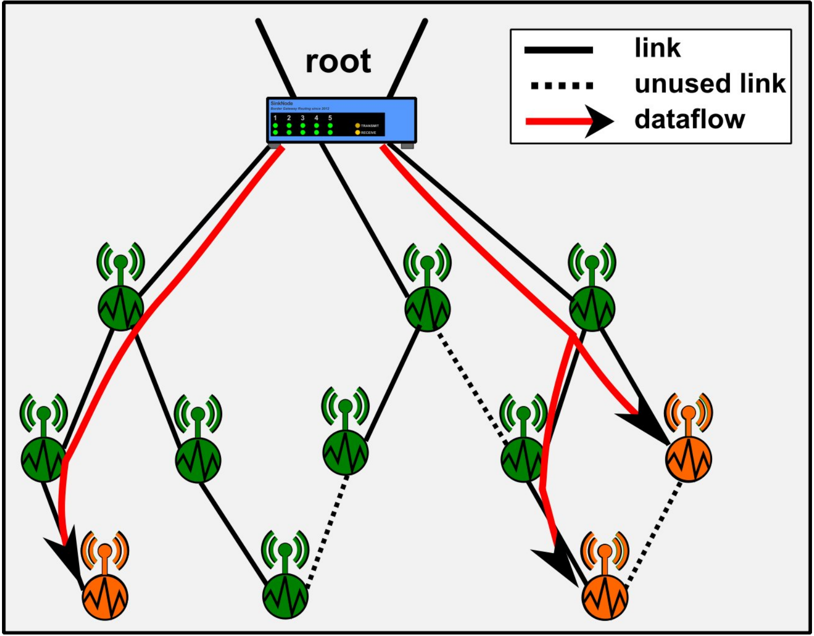
## Traffic Flow

Multipoint-to-point (MP2P), P2MP, and P2P traffic supported

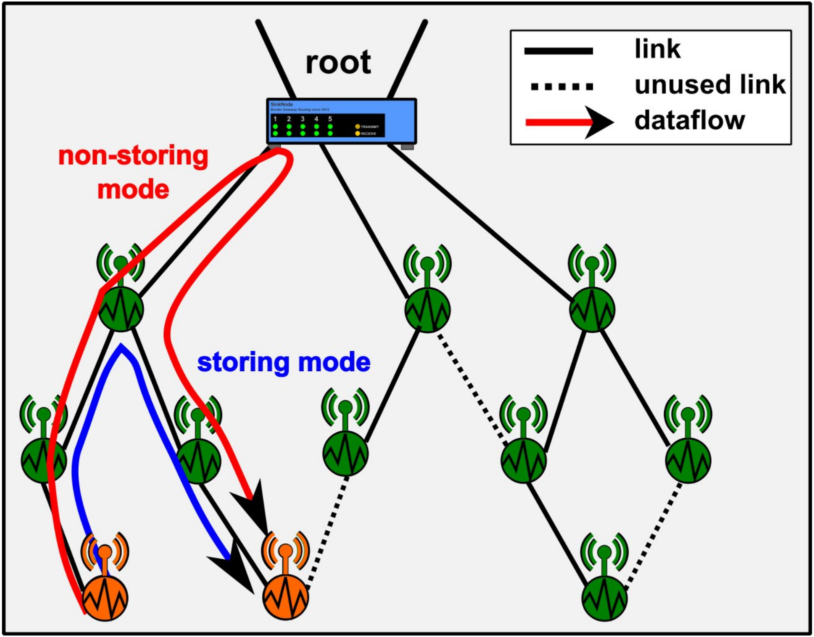
# RPL: Multipoint-to-Point Traffic Flow



# RPL: Point-to-Multipoint Traffic Flow



# RPL: Point-to-Point Traffic Flow



# State of Play

## Why use RPL?

1. **Low rate of control messages**: Bootstrapping topology, reactively repairing inconsistencies
2. **Using IPv6**: connectivity to other part of the internet (Internet of Things)
3. **New academic approach** for promising research

## Final Decision pending

Use of RPL in SAFEST still under discussion! (Comparison e.g. OLSR)

# Content

2 Security Outline on Routing in SAFEST Network

- RPL Security Concepts
- Exemplary Lightweight Approach

# RPL Security Concepts

## Optional Security Modes

- **Unsecure**: no additional security (e.g. using link layer security)
- **Preinstalled**: one (preinstalled) key for Integrity, Confidentiality, Authenticity
- **Authenticated**: one (preinstalled) key to join and a second key for Integrity, Confidentiality, Authenticity

# RPL Security Concepts

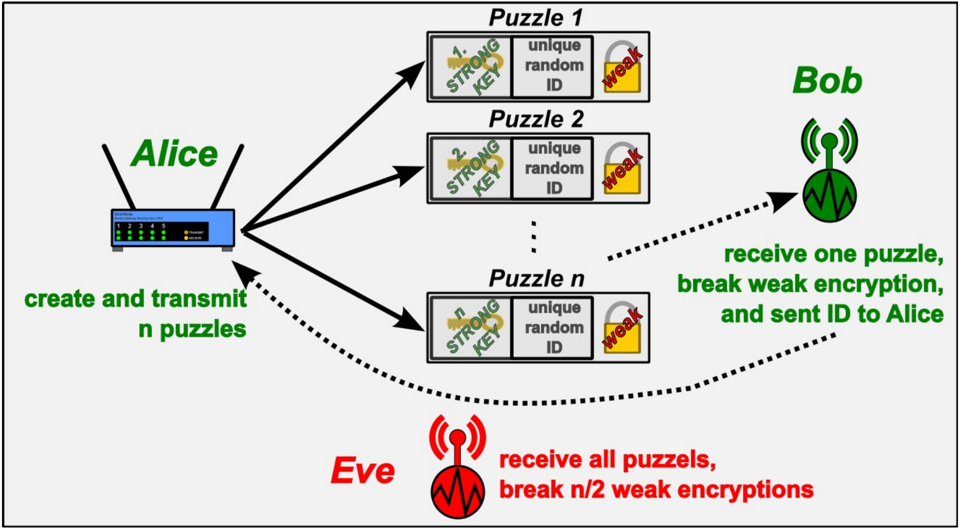
## Security Issues within RPL

- **RPL requires preinstalled keys**, and does not state key management approach.
- **No lightweight security paradigm** in RPL: focus on low-power routing, but not low-power security
- No asymmetric cryptography for authenticated mode defined in RPL (only suitable for stronger nodes!)

## Proposal and Challenges for SAFEST

- **Lightweight security for weak nodes** and basic security for stronger nodes (e.g. asymmetric cryptography)
- Trust establishment between root/nodes
- Feasible attacks and attacker model

# Lightweight Key Agreement with Merkle's Puzzle [2]


Puzzle 1
1. STRONG KEY
unique random ID
weak
Puzzle 2
2. STRONG KEY
unique random ID
weak
Puzzle n
n STRONG KEY
unique random ID
weak
Alice
create and transmit n puzzles
Bob
receive one puzzle, break weak encryption, and sent ID to Alice
Eve
receive all puzzels, break n/2 weak encryptions

# Content

# Overview and Outlook

- **(Secure) Routing in SAFEST Network** for Low Power Sensors
- **Closely considering and researching RPL** for efficient routing in SAFEST, regarding routing decisions and security
- **Proposal of lightweight** and basic security scheme for RPL

[1] Beijing Airport Terminal 3: Going for the Gold.
webpage.
`http://www.hotelclub.com/blog/beijing-airport-terminal-3-going-for-the-gold/` - last checked: 06.11.2012.

[2] R. Merkle.
Secure Communications Over Insecure Channels.
*Communications of the ACM*, pages 294–299, April 1978.

[3] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander.
RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.
RFC 6550 (Proposed Standard), March 2012.