



## Friendly Clustering

A strategy for the Maniac Challenge 2009

Heiko Will, Felix Juraschek

Institute of Mathematics and Computer Science

March 8, 2009

1. Friendly Clustering
2. Neighbor Monitoring
3. Routing Decisions
4. Partner Communication
5. Implementation
6. Evaluation

## Basic idea

- Split the neighborhood into good and bad nodes
- Observe forwarding behaviour
- Comparison of node scores
- Routing decisions depend on source and destination
- Quick reactions to node behaviour changes

## Involved components

- Neighborhood monitoring
- Routing decisions
- Exchange gathered data with the partner node

- Packet tracking for each neighbor
- Counters for forwarded, dropped, and redirected packets
- Separate statistics based on receiver/sender class
- Information source: packet queue and the sniff queue
- Detailed forwarding statistics for known nodes

## Idea

- Partition neighbors in a good cluster and a bad one
- Forward to/from good guys, ignore bad guys

## Decision making

- Only the last hop and destination of a packet are important
- Choose best router for partner traffic
- Decisions are calculated based on the statistics
- **No random decisions**

## Idea

- Exchange node statistics
- UDP
- Fixed intervals

## Advantages

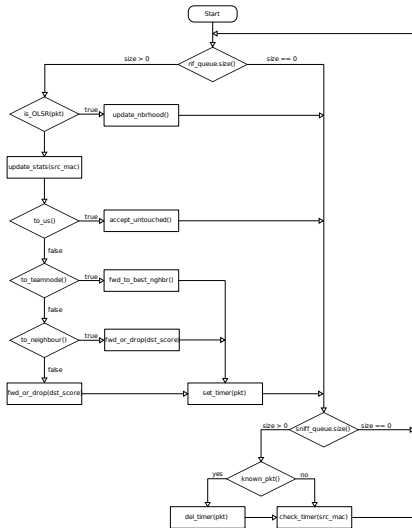
- Faster reaction to topologie changes
- More empirical data for calculating scores
- Shorter learning phase, more accurate decisions

## Basic data structures

- References to nodes in 2 binary trees (ip, mac)
- Hashes of incoming packets stored in FIFO and map for efficient access

## Important features

- Timestamps for recognizing dropped packets
- Optimized polling of both queues
- Packet handling is shorter than transmission time
- Routing decisions as a state machine



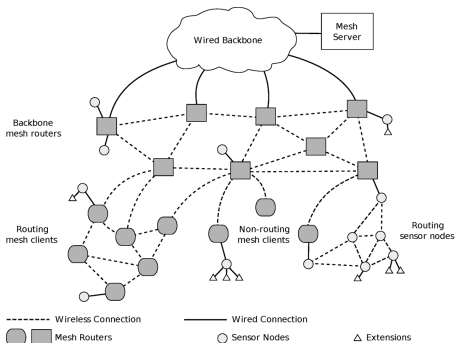
- Non-synchronized packet queues
- Matching MACs to IPs
- No uniqueness of packets
- Promiscuous mode seems to be unreliable
- Hidden / Exposed nodes
- Instable links

## Foundation

- Only real world testing
- DES-Testbed

## Testruns

- Different strategies
- Various topologies
- Synthetic and real world traffic (*iperf* and *nuttcp*)
- Monitoring nodes



## Architecture

- 70 DES-Nodes with multiple 802.11a/b/g NICs
- Overlapping sensor and network

## Research focus

- Used for long-term experiments
- Used in EU funded projects WiseBed and OPNEX
- Current research focus: long-term experiments, routing, channel assignment ...



## Results

- Reliable node classification
- Prediction of forwarding probability close to reality
- Need for weight function based on node actions

## Weaknesses

- Find them yourself!

Thank you for your attention.  
Questions?