http://www.kom.tu-darmstadt.de

Advanced Topics in Distributed Systems (Spring/Summer 2007)

Mobile Ad hoc Networking II

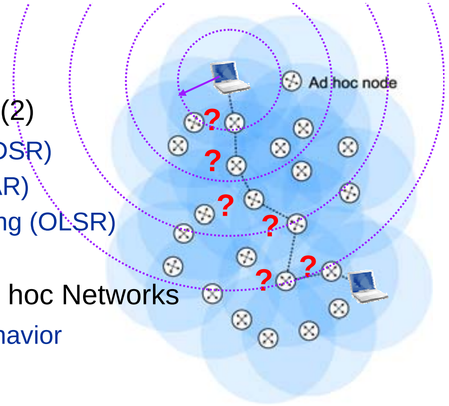
Dr.-Ing. Matthias Hollick, Prof. Dr.-Ing. Ralf Steinmetz

Technische Universität Darmstadt,
Fachbereich Elektrotechnik und Informationstechnik, Fachbereich Informatik (Zweitmitglied),
Fachgebiet Multimedia Kommunikation – KOM, Tel.+49 6151 166158, Fax. +49 6151 166152
Merckstr. 25, D-64283 Darmstadt, Matthias.Hollick@KOM.tu-darmstadt.de

---

http://www.kom.tu-darmstadt.de

Outline (Part 2)



Selected Routing Protocols (2)
- Dynamic Source Routing (DSR)
- Location Aided Routing (LAR)
- Optimized Link State Routing (OLSR)

Routing Dependability in Ad hoc Networks
- The Effects of Node Misbehavior
- Modeling Ad hoc Networks

Performance Evaluation of Ad hoc Networks
- The Art of Performance Evaluation
- Analyzing Ad hoc Network Performance

Research Challenges, Summary and Conclusion

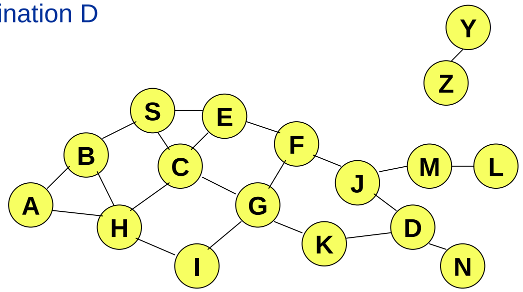
Appendix

---

http://www.kom.tu-darmstadt.de

Dynamic Source Routing (DSR)

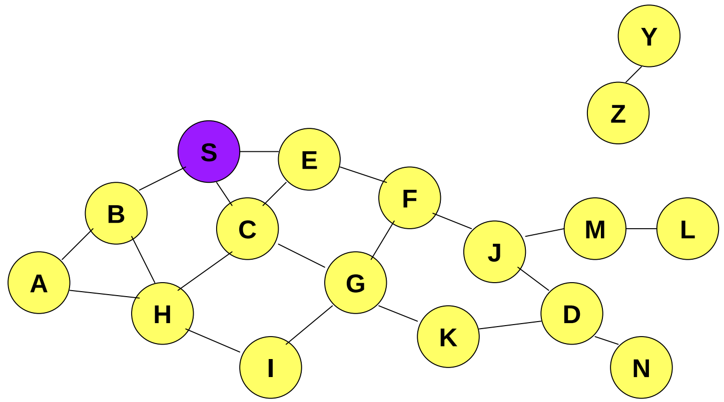
Shares some principles with AODV
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ
- Following an example for a route discovery from source S to destination D



---

http://www.kom.tu-darmstadt.de

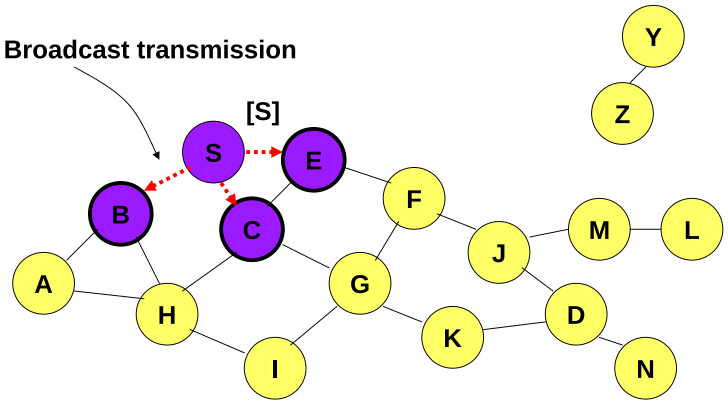
Route Discovery in DSR



Represents a node that has received RREQ for D from S

Source: Nitin Vaidya

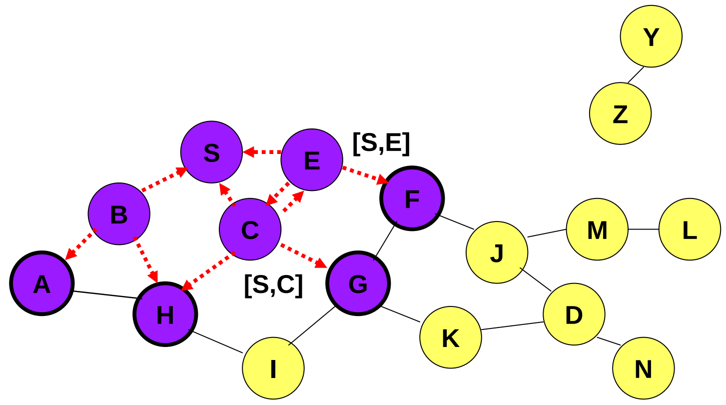
Route Discovery in DSR



Represents transmission of RREQ
[X,Y] Represents list of identifiers appended to RREQ

Source: Nitin Vaidya

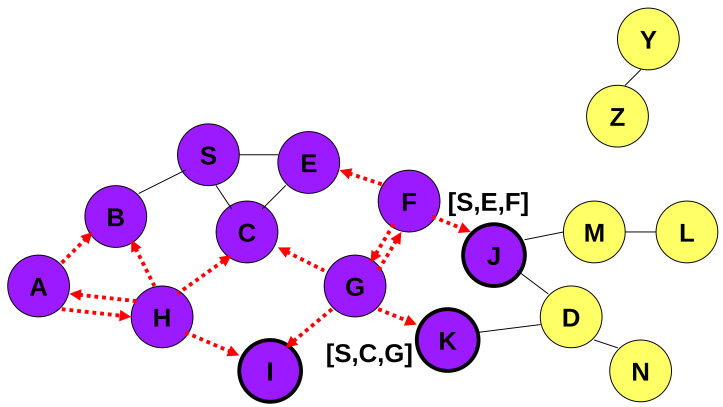
Route Discovery in DSR



Node H receives packet RREQ from two neighbors: potential for collision

Source: Nitin Vaidya

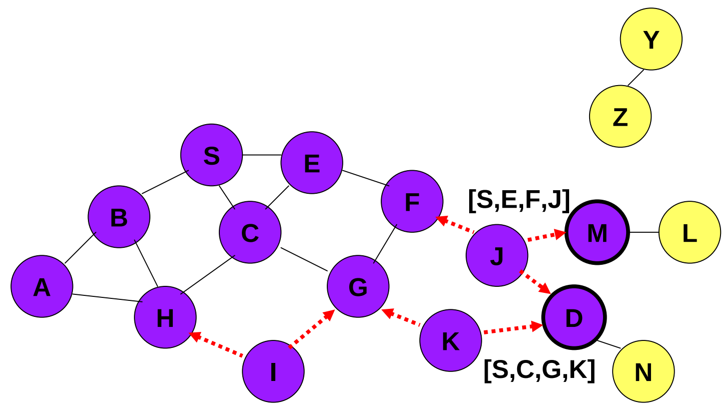
Route Discovery in DSR



Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Source: Nitin Vaidya

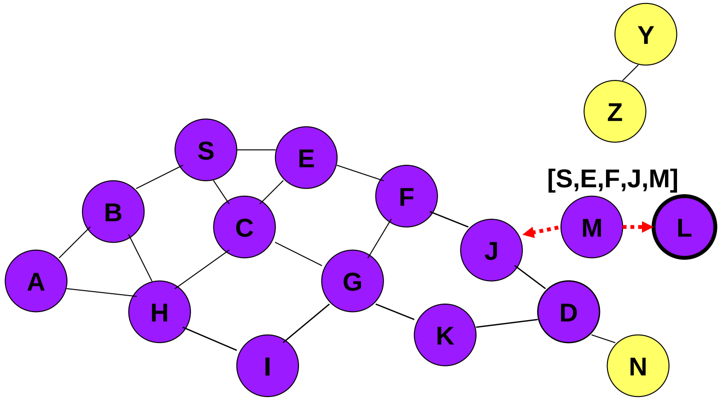
Route Discovery in DSR



Nodes J and K both broadcast RREQ to node D
Since nodes J and K are hidden from each other, their transmissions may collide

Source: Nitin Vaidya

Route Discovery in DSR



Node D does not forward RREQ, because node D is the intended target of the route discovery

Source: Nitin Vaidya

Route Discovery in DSR

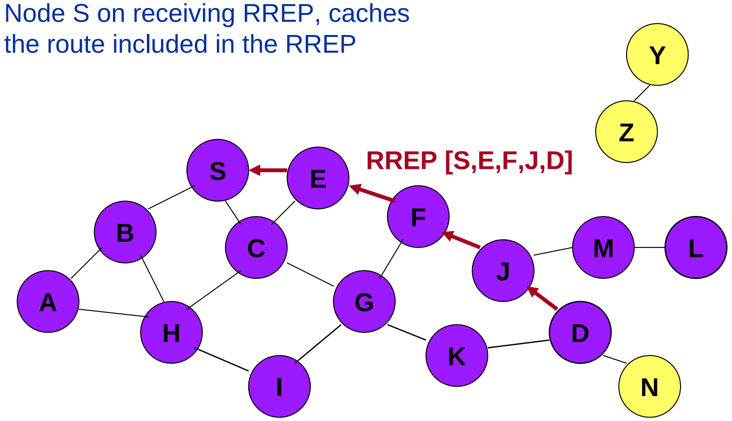
Route Reply (RREP)

- Destination D on receiving the first RREQ, sends a (RREP)
- RREP is sent on a route obtained by reversing the route appended to received RREQ
- RREP includes the route from S to D on which RREQ was received by node D

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S

Route Reply in DSR

Node S on receiving RREP, caches the route included in the RREP



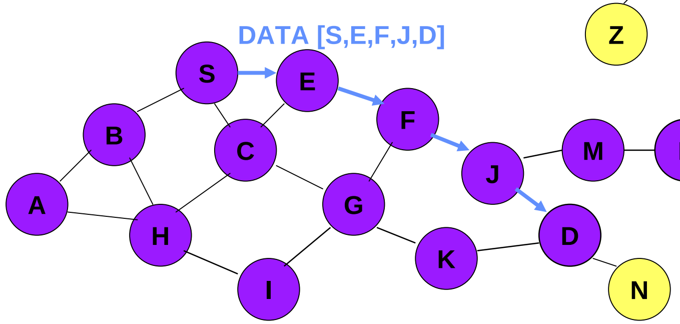
← **Represents RREP control message**

Source: Nitin Vaidya

Data Delivery in DSR

When node S sends a data packet to D, the entire route is included in the packet header (hence the name source routing)

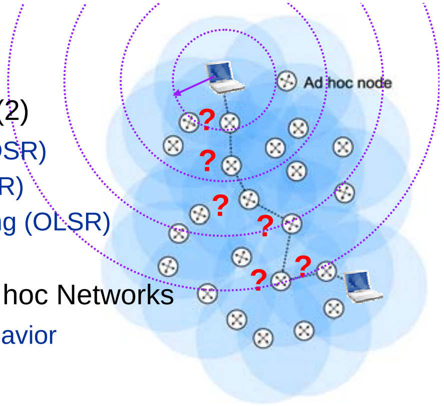
Intermediate nodes forward according this route



Packet header size grows with route length

Source: Nitin Vaidya

Outline (Part 2)



Selected Routing Protocols (2)
- Dynamic Source Routing (DSR)
- Location Aided Routing (LAR)
- Optimized Link State Routing (OLSR)

Routing Dependability in Ad hoc Networks
- The Effects of Node Misbehavior
- Modeling Ad hoc Networks

Performance Evaluation of Ad hoc Networks
- The Art of Performance Evaluation
- Analyzing Ad hoc Network Performance

Research Challenges, Summary and Conclusion

Appendix

Location-Aided Routing (LAR)

Exploits location information to limit scope of flooding for route request
- Location information may be obtained using GPS

Expected Zone is determined as a region that is expected to hold the current location of the destination node (D)
- Expected region determined based on potentially old location information, and knowledge of the destination's speed

Route requests limited to a *Request Zone* that contains the Expected Zone and location of the sender node (S)

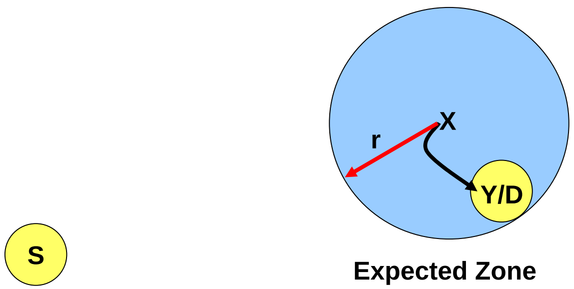
Expected Zone in LAR

S = Source node, D = Destination node

X = last known location of node D, at time t0

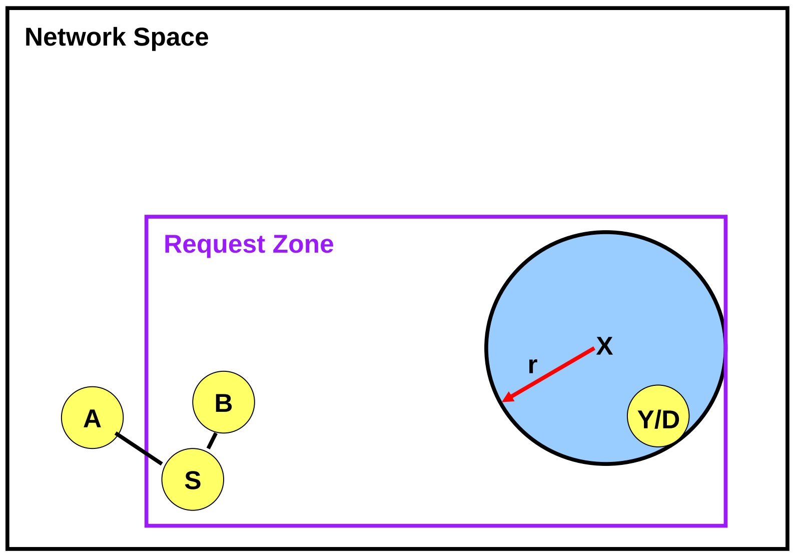
Y = location of node D at current time t1, unknown to sender S

r = (t1 - t0) * estimate of D's speed



Expected Zone

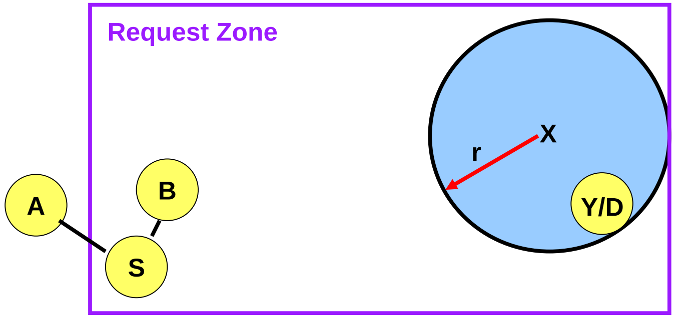
Request Zone in LAR



Operation of LAR (1)

Only nodes within the request zone forward route requests

- Node A does not forward RREQ, but node B does
- Request zone explicitly specified in the route request
- Each node must know its physical location to determine whether it is within the request zone



Operation of LAR (1)

Only nodes within the request zone forward route requests

If route discovery using the smaller request zone fails to find a route, the sender initiates another route discovery (after a timeout) using a larger request zone

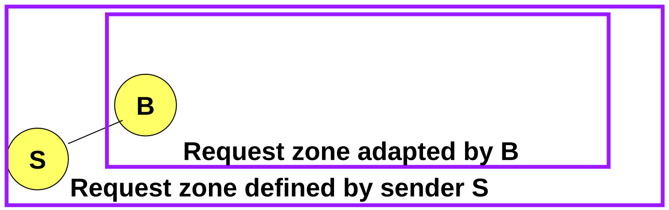
- the larger request zone may be the entire network

Rest of route discovery protocol similar to DSR (will be discussed later)

LAR Variations: Adaptive Request Zone

Each node may modify the request zone included in the forwarded request

- Modified request zone may be determined using more recent information and may differ from original request zone



Until now a route request explicitly specified a request zone

- Implicit Request Zone: A node X forwards a route request received from Y if node X is deemed to be closer to the expected zone as compared to Y
- The motivation is to attempt to bring the route request physically closer to the destination node after each forwarding

Location-Aided Routing

The basic proposal assumes that, *initially,* location information for node X becomes known to Y only during a route discovery

- This location information is used for a future route discovery
- Each route discovery yields more updated information which is used for the next discovery

Variations

- Location information can also be piggybacked on any message from Y to X
- Y may also proactively distribute its location information

LAR Summary – Advantages

- Reduces the scope of route request flood
- Reduces overhead of route discovery

LAR Summary – Disadvantages

- Nodes need to know their physical locations
- Does not take into account possible existence of obstructions for radio transmissions

LAR-Optimization Query Localization

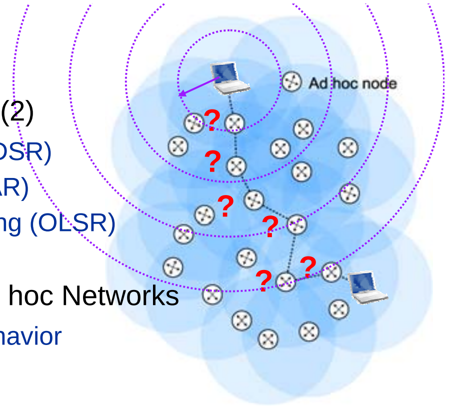
Limits route request flood without using physical information

- Route requests are propagated only along paths that are *close* to the previously known route
- The *closeness* property is defined without using physical location information

Path locality heuristic: Look for a new path that contains at most *k* nodes that were not present in the previously known route

- Old route is piggybacked on a Route Request
- Route Request is forwarded only if the accumulated route in the Route Request contains at most *k* new nodes that were absent in the old route
- This limits propagation of the route request

Outline (Part 2)



Selected Routing Protocols (2)

- Dynamic Source Routing (DSR)
- Location Aided Routing (LAR)
- Optimized Link State Routing (OLSR)

Routing Dependability in Ad hoc Networks

- The Effects of Node Misbehavior
- Modeling Ad hoc Networks

Performance Evaluation of Ad hoc Networks

- The Art of Performance Evaluation
- Analyzing Ad hoc Network Performance

Research Challenges, Summary and Conclusion

Appendix

Optimized Link State Routing (OLSR)

Links state routing in general: Each node …

- … periodically floods status of its links
- … re-broadcasts link state information received from its neighbor
- … keeps track of link state information received from other nodes
- … uses this information to determine next hop to destinations

- Link state routing is proactive
- Local information is disseminated network wide

Reduction of overhead of flooding link state information if fewer nodes to forward the information

- A broadcast from X is only forwarded by selected nodes, so-called multipoint relays (MPR)
- MPRs should globally optimize flooding by optimizing it locally

OLSR – Multipoint Relays

MPR Definitions

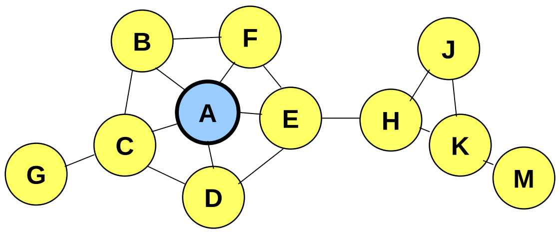
- A node is selected with two rules
  - Any 2-hop neighbor must be covered by at least one multipoint relay
  - The number of multipoint relays should be minimized (per node)
- A node forwards the flooding packets with the following rules
  - Forward if the packet has not already been received
  - The node is multipoint relay of the last emitter

A simple heuristic for computing MPRs

- Start with an empty MPR set
- Add to the MPR set each neighbor that is the only one covering some 2-hop neighbor (must be an MPR anyway)
- Until all 2-hop neighbors are covered repeat:
  - Add to the MPR set a neighbor that covers a maximum of still uncovered 2-hop neighbors

OLSR – MPR Selection (1)

What are MPRs of node A ?

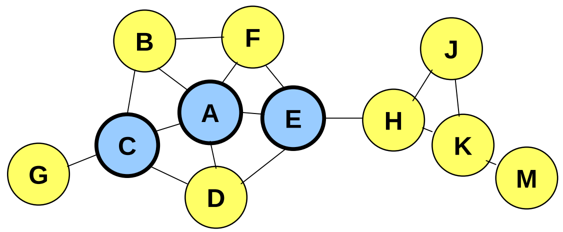


Source: Nitin Vaidya

OLSR – MPR Selection (2)

Nodes C and E forward information received from A

- What are MPRs of node E?



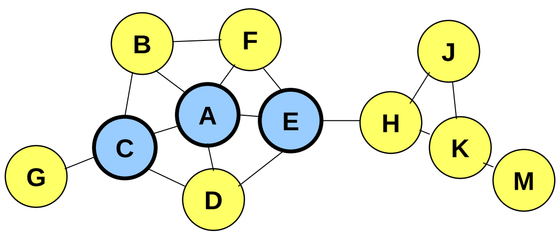
Node that has broadcast state information from A

Source: Nitin Vaidya

OLSR – MPR Selection (3)

Nodes A and H are multipoint relays for node E

- A has forwarded the link state message already



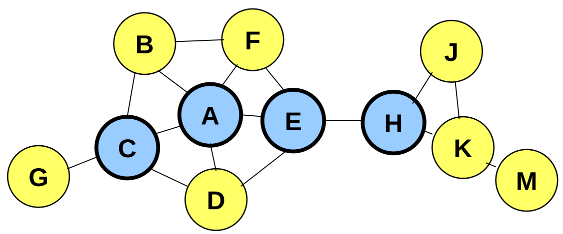
Node that has broadcast state information from A

Source: Nitin Vaidya

OLSR – MPR Selection (4)

Node E and K are multipoint relays for node H

- Node K forwards information received from H in the next step
- E has already forwarded the same information once



Node that has broadcast state information from A

Source: Nitin Vaidya

OLSR Core Protocol Functionality

Link Sensing

- Periodic HELLO messages: a local link set, describing links between "local interfaces" and "remote interfaces" is defined

MPR Selection and MPR Signaling

- Nodes select a subset of their neighbors such that a broadcast message, retransmitted by these selected neighbors, will be received by all nodes 2 hops away
- MPR calculation bases on HELLO messages

Topology Control Message Diffusion (Link State Messages)

- Topology control messages carry sufficient link-state information to allow route calculation to all nodes in the network

Route Calculation:

- Bases on link state information + interface configuration
- The routing table can be calculated at each node

The OLSR standard specifies all messages + mechanisms

Summary OLSR

Target networks

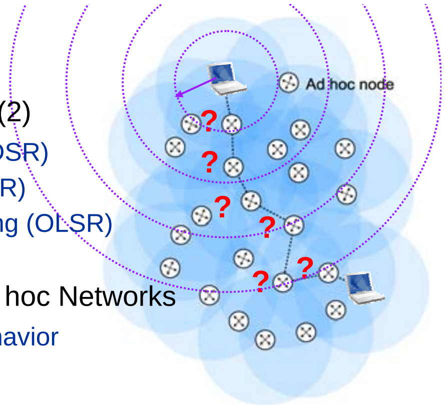
- Large, dense networks
- Low latency for route discovery (proactive)
- Various extensions exist, so-called auxilliary functions to complement the core functionality of OLSR

Multipoint relays reduce the flooding overhead because …

- … only MPRs forward control messages
- … MPRs may flood partial link state, that is, only MPRs generate link state information including MPR Selector information
  - A MPR Selector of node X is a node which has selected its 1-hop neighbor, node X, as its multipoint relay

See demo

Outline (Part 2)



Selected Routing Protocols (2)

- Dynamic Source Routing (DSR)
- Location Aided Routing (LAR)
- Optimized Link State Routing (OLSR)

Routing Dependability in Ad hoc Networks

- The Effects of Node Misbehavior
- Modeling Ad hoc Networks

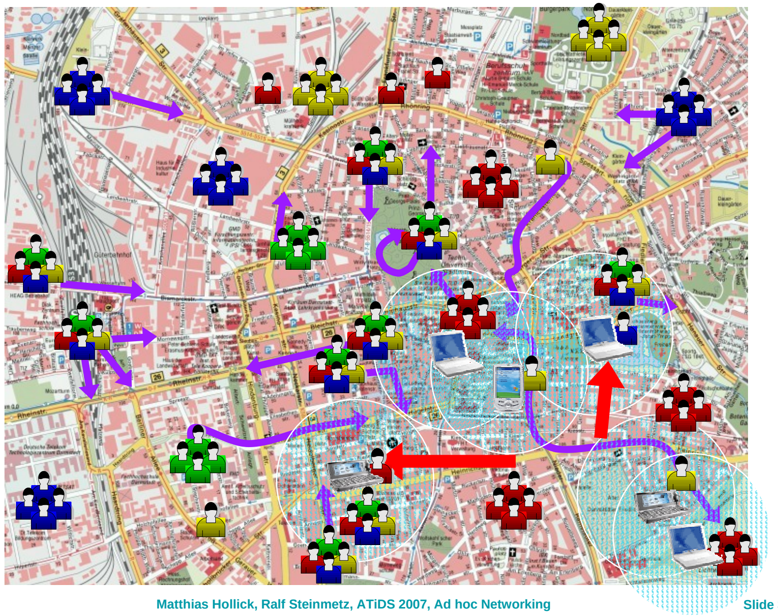
Performance Evaluation of Ad hoc Networks

- The Art of Performance Evaluation
- Analyzing Ad hoc Network Performance

Research Challenges, Summary and Conclusion

Appendix

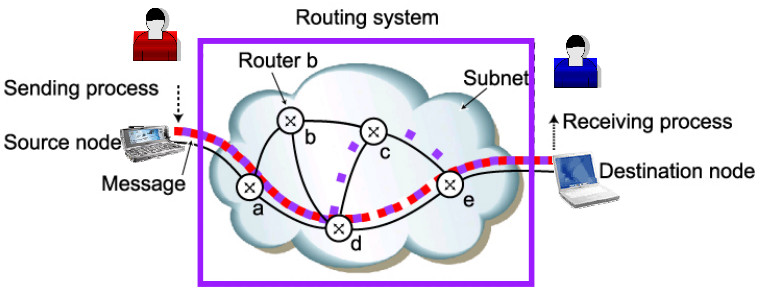
Is MANET Routing Ready for Prime-time?



The Concept of Routing Dependability (1)

Routing System – Definition

*"A **routing system** delivers messages from a source node to a destination node by means of networked intermediate nodes (routers), which implement the functional process (routing) of identity resolution, path computation, and message forwarding."*

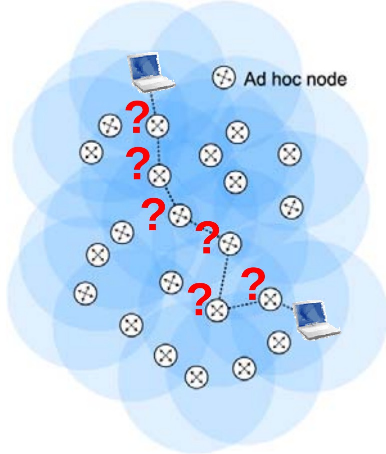


The Concept of Routing Dependability (2)

http://www.kom.tu-darmstadt.de

Routing Dependability – Definition

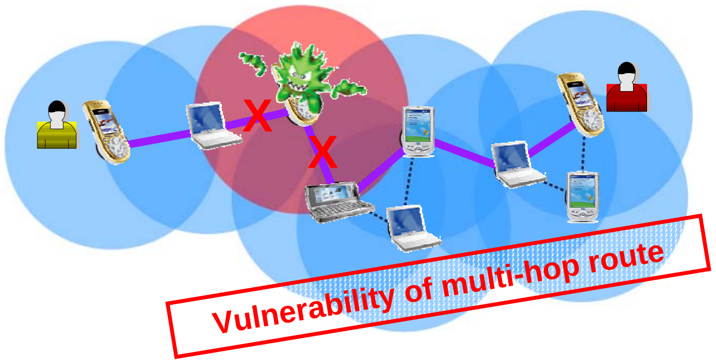
*"**Routing dependability**: the trustworthiness of a routing system such that reliance can justifiably be placed on the consistency of behavior and performance of the routing service it delivers."*



Node Misbehavior

http://www.kom.tu-darmstadt.de

Scenario

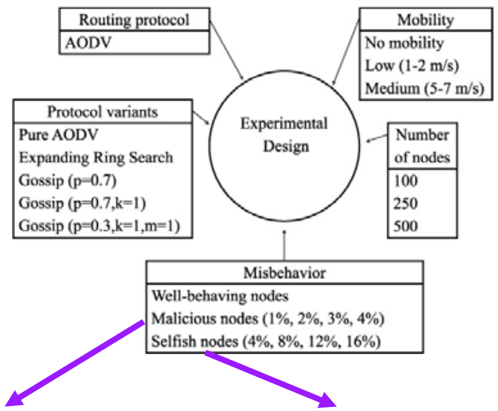


Challenge

- Qualify and quantify the effects of node misbehavior on the overall performance of the routing system

Experimental Simulation Study

http://www.kom.tu-darmstadt.de



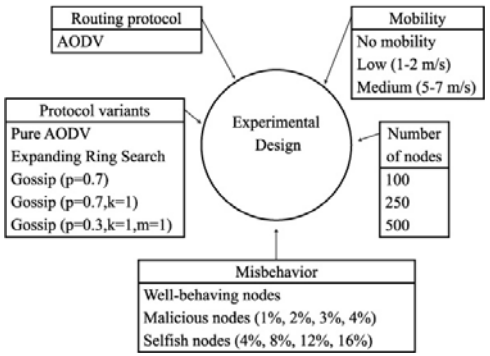
Malicious Nodes

- Inject false information or remove packets from the network (here black holes)

Selfish Nodes

- Optimize their own gain, neglecting welfare of other nodes

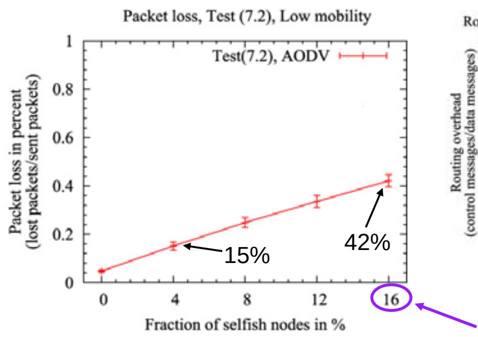
Experimental Simulation Study

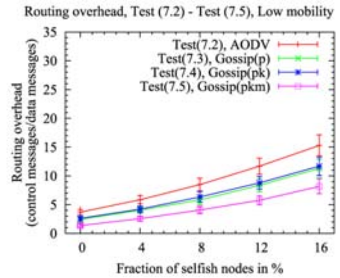


Parameters (250 node setup)

- Average node density = 9; Area = $(2334m)^2$; Simulation time = 900s
- Link layer = IEEE 802.11b with Distributed Coordination Function (DCF)
- Network layer = Ad hoc On-demand Distance Vector Routing, IPv4
- Transport/Application layer = Constant Bit-Rate (CBR) flows over UDP

Observations for Selfish Nodes





Packet loss increases …

- … nearly linearly with the number of selfish nodes
- … with node mobility

Routing overhead increases

How to Measure Dependability?

Quantification of the overall network performance

- Application related response variables?
  - Sent packets [Bytes], Goodput [Bytes], Lost packets [Bytes]
  - Mean end-to-end delay [ms]
  - Maximum e2e delay [ms]
- Routing related response variables?
  - Mean path length [hops]
  - Maximum path length [hops]
  - Total # of routing messages (counted on per hop base) [#]
  - # of routing msg. per host [#]
  - Total # of RREQ, RREP, RERR [#]
- Or better flow level related, session related, etc.?

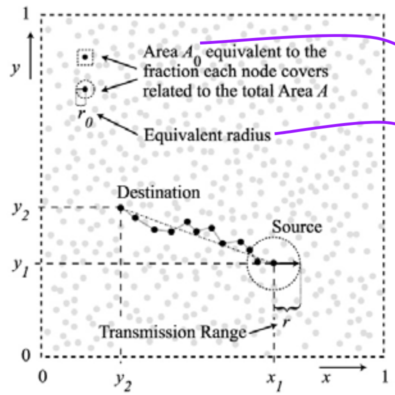
How to obtain a birds eye view of the network

- Route-length distribution as metric
  - Does not substitute other metrics but complements them

Modeling the Route Acquisition Process (1)

Assumptions

- Area *A* is a normalized square of side length 1
- *x* and *y* coordinates of nodes are i.i.d. and uniformly distributed in the interval [0,1]
- All nodes *N* share a uniform transmission range $r \ll 1$. The system consists of *n* nodes



Basic properties of the network

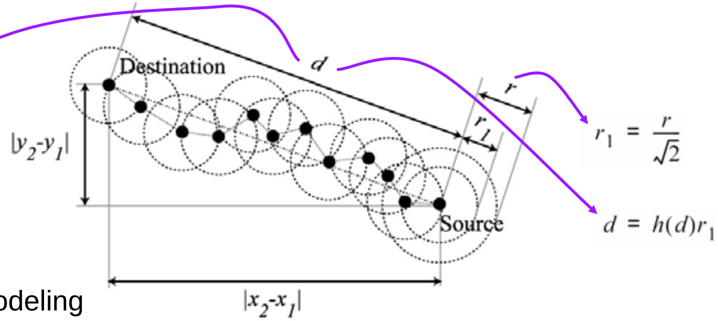
$A_0 = \frac{A}{n}$ Equivalent area

$r_0 = \sqrt{\frac{A}{n\pi}}$ Equivalent radius

The average degree *M* of the network (expected number of nodes in a transmission radius at any point) is

$$M = \frac{\pi r^2}{A_0} = \left(\frac{r}{r_0}\right)^2$$

Modeling the Route Acquisition Process (2)



Modeling

- Average progress per routing step is approximately r_1
- Distance d is function of hop-count h and r_1
- Using the euclidean distance for d and combining with the node distribution we obtain the pdf $p(d)$ of the route length in the network

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \qquad p(d)$$

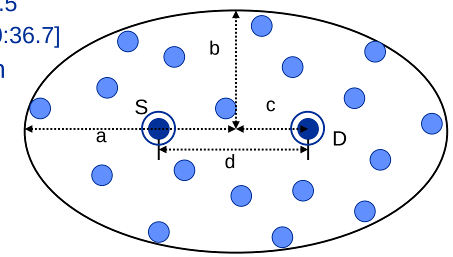
Simulation Study of Average Routing Progress

Simulation parameters

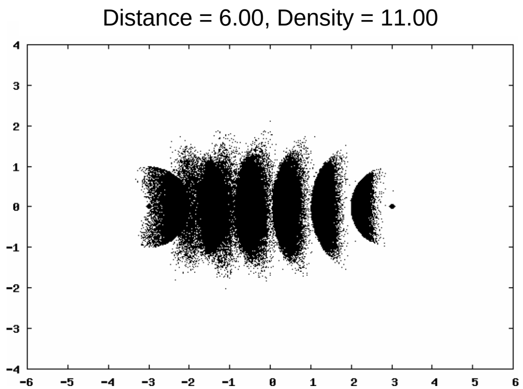
- Search for path between source S and destination D
- Common communication range r = 1
- Elliptical simulation area: a = 3r+c, b = 4r, c = d/2
- Distance
  - d = [1.1r:3r], increment of 0.1
  - d = [3.5r:12r], increment of 0.5
- Node density
  - ρ = [0.25:3], increment 0.25
  - ρ = [3.5:12], increment 0.5
  - i.e., avg. neighbors = [~0:36.7]
- Replications: 50.000 each

Assumptions

- Nodes i.i.d. uniformly distributed, static
- IEEE 802.11, AODV



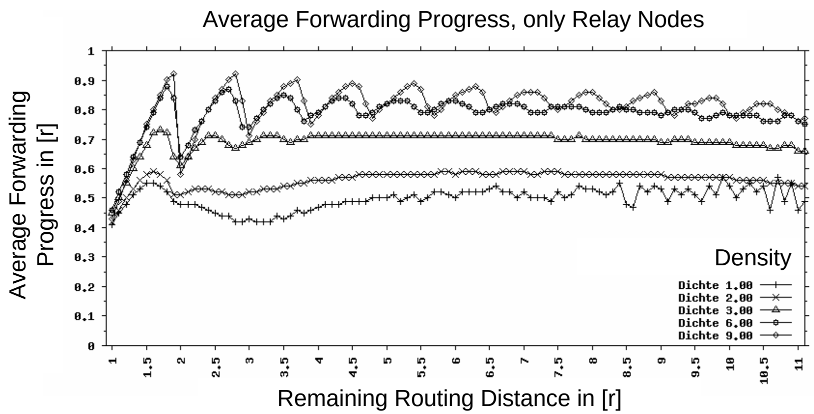
Simulation Study of Average Routing Progress (2)



Selected results (for a very dense network)

- Routing „trend" towards destination is clearly visible
- Only very few routes depart from shortest path

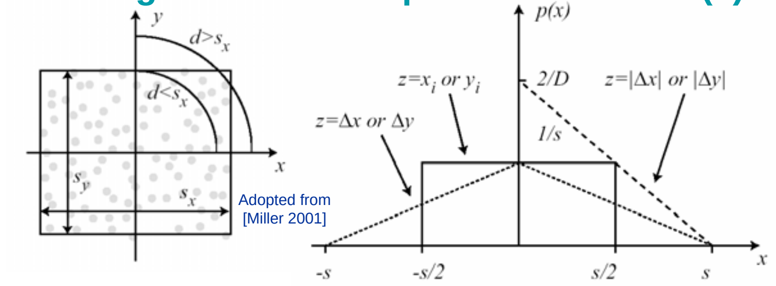
Simulation Study of Average Routing Progress (3)



Results

- Average forwarding progress increases with density
- In dense networks the forwarding progress can be close to the optimal value

Modeling the Route Acquisition Process (3)



Adopted from [Miller 2001]

Modeling using probability densities

- Distribution of nodes $p(x) = \frac{1}{s_x}, |x| \le \frac{s_x}{2}$ $\quad p(y) = \frac{1}{s_y}, |y| \le \frac{s_y}{2}$
- Distribution of node distances

$$p(\Delta x) = \frac{(s_x - |\Delta x|)}{(s_x)^2}, |\Delta x| \le s_x \qquad p(\Delta y) = \frac{(s_y - |\Delta y|)}{(s_y)^2}, |\Delta y| \le s_y$$

- Cumulative distribution function

$$P(d) = \iint_{(x,y)} p(d)\,dx\,dy \quad \text{with} \quad p(d),\ d = \sqrt{\Delta x^2 + \Delta y^2}$$

Modeling the Route Acquisition Process (4)

We obtain

- CDF

$$P(d) = \begin{cases} \frac{1}{2}d^4 - \frac{8}{3}d^3 + \pi & d \le 1 \\ 4\sqrt{d^2-1} + \frac{8}{3}\sqrt{(d^2-1)^3} - \frac{1}{2}d^4 + 2d^2 + \frac{1}{3} & \\ +2d^2\left(\arcsin\left(\frac{1}{d}\right) - \arccos\left(\frac{1}{d}\right)\right) & 1 < d \le \sqrt{2} \end{cases}$$

- PDF

$$p(d) = \begin{cases} 2d(d^2 - 4d + \pi) & d \le 1 \\ 8d\sqrt{d^2-1} - 2d^3 - 4d + 4d\left(\arcsin\left(\frac{1}{d}\right) - \arccos\left(\frac{1}{d}\right)\right) & 1 < d \le \sqrt{2} \end{cases}$$

- Additionally, [Mullen2003] provides some approximations

Additional Features of the Base Model

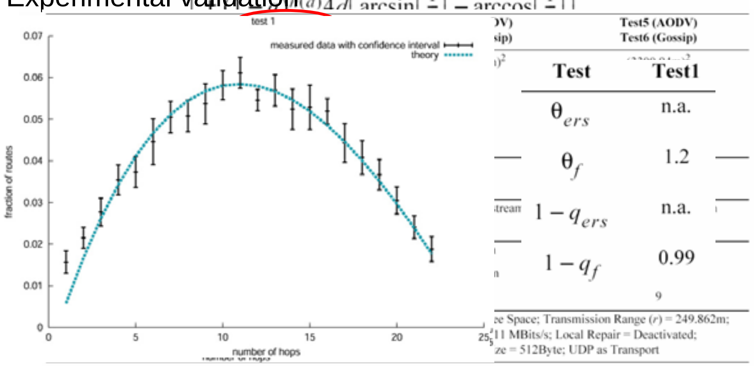
Transmission errors

- In the model: per-hop loss probability q → the success-probability for the complete route is $(1-q)^{h(d)}$

AODV and gossip-enhanced AODV

- In the model: linear correction term θ which describes the elongation of routes compared to ideal routing

Experimental validation

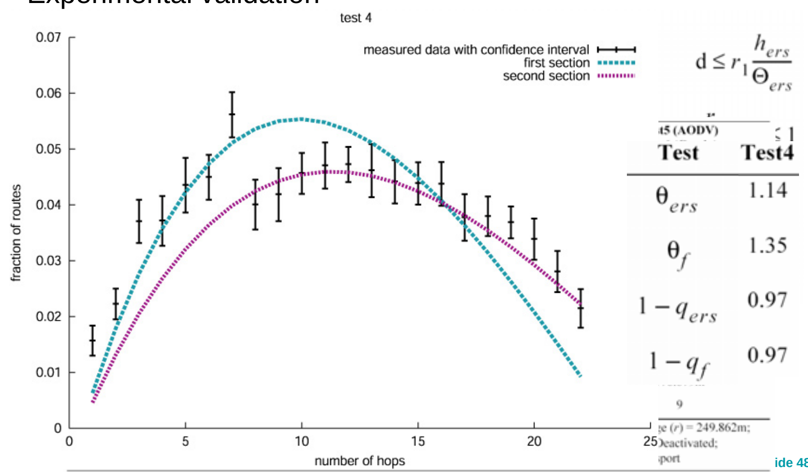


Enhancing the Base Model

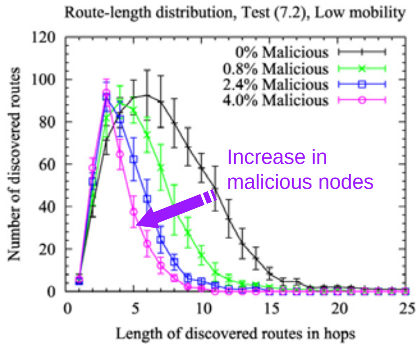
Expanding ring search

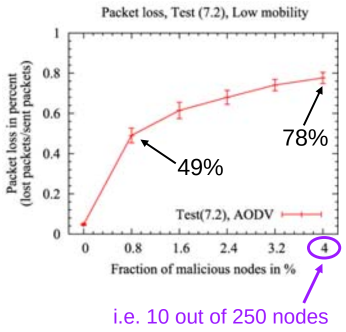
- In the model: use two distinct areas, (f) for pure flooding, (esr) for expanding ring search and apply correction for both areas

Experimental validation



Observations for Malicious Nodes (Black Holes)





Successful communication only in close proximity

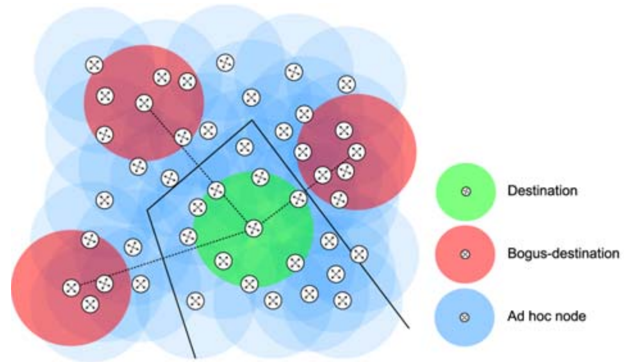
Packet loss …

- … is extremely high, even for few black holes
- … increases with node mobility

Black Holes Explained

Modeling of Black Holes

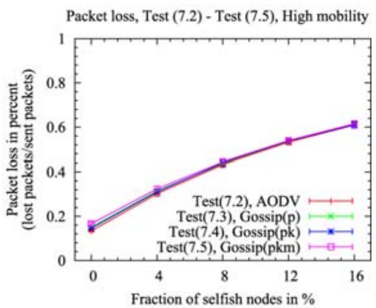
- Black holes masquerade as “bogus”-destination
- Competition between black holes and real destination

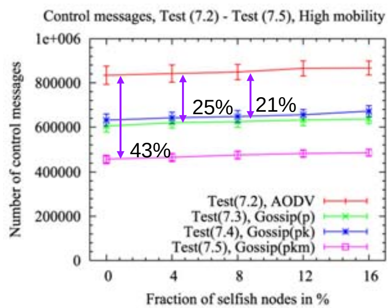


- Black holes reduce the length of successfully acquired routes

There is Room for Improvement

Probabilistic optimization of the route acquisition process …





- … does not increase the observed packet loss
- … yields a substantial reduction in communication overhead

Summary Routing Dependability

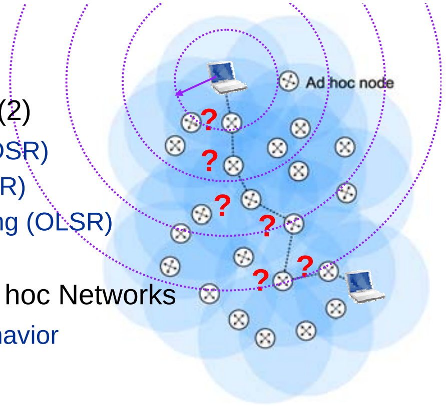
Problems

- Most ad hoc routing algorithms tacitly assume only well-behaving nodes to support multi-hop operation of the network
- Recently proposed QoS-strategies for ad hoc environments assume only well-behaving nodes, too
- Unrealistic assumptions for real world deployment!

Underlying problems

- Induced by mobility
  - High topology dynamics on various timescales
- Induced by wireless communication, other constraints, …
  - Physical security diminishes, MAC may be inefficient
- Induced by missing infrastructure and node misbehavior
  - Loss of control, reliability, trustworthiness
- Induced by application characteristics
  - Military vs. commercial vs. home environment

Outline (Part 2)



Selected Routing Protocols (2)
- Dynamic Source Routing (DSR)
- Location Aided Routing (LAR)
- Optimized Link State Routing (OLSR)

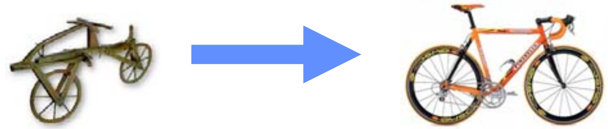
Routing Dependability in Ad hoc Networks
- The Effects of Node Misbehavior
- Modeling Ad hoc Networks

Performance Evaluation of Ad hoc Networks
- The Art of Performance Evaluation
- Analyzing Ad hoc Network Performance

Research Challenges, Summary and Conclusion

Appendix

The Art of Performance Evaluation (1)



"That which is monitored improves."

—unknown Source

The quotes in this lecture part are taken from [Jain1991]

The Art of Performance Evaluation (2)

Basics Terms
- Performance Analysis = Analysis + Computer Systems
- System – any collection of hardware and software
- Metrics – the criteria used to evaluate the system performance
- Workloads – the requests made by the users of the system

Is performance analysis is an art?
- Successful evaluation cannot be produced mechanically
- Every evaluation requires a large set of skills
- Given the same data, two analysts may interpret them differently

Example
- 2 systems, which one is the best?
- Throughputs of two systems A, B measured in transactions/second

System	Workload 1	Workload 2
A	20	10
B	10	20

The Art of Performance Evaluation (3)

Possible Solutions
- (1) Compare the average: both systems are equal

System	Workload 1	Workload 2	Average
A	20	10	15
B	10	20	15

- (2) Compare the ratio with system B as base

System	Workload 1	Workload 2	Average
A	2	0.5	1.25
B	1	1	1

- (3) Compare the ratio with system A as base

System	Workload 1	Workload 2	Average
A	1	1	1
B	0.5	2	1.25

Common Mistakes & How-to Avoid Them (1)

1. No Goals
   - Any endeavor without goals is bound to fail!
   - There is no such thing as a general-purpose model!
   - Goals → correct metrics, workloads, and methodology!
2. Biased Goals
   - “To show that OUR system is better than THEIRS” ?
   - Analysts = Jury!

(Source www.zeit.de)

Common Mistakes & How-to Avoid Them (2)

3. Unsystematic Approach
   - Arbitrary selection of workload → Inaccurate conclusions!

4. Analysis without understanding the problem
   - “A problem well stated is half solved”!

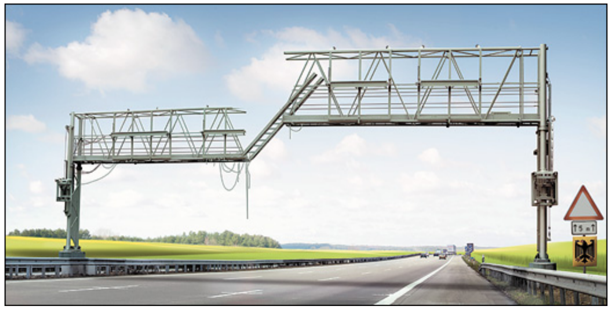
5. Incorrect Performance Metrics
   - Chosen to be easily computed rather to be relevant?

6. Unrepresentative Workload
   - Should represent the actual usage of the system!

… see Appendix for other common mistakes

(Source www.zeit.de)

So Everything Went Wrong …



(Source www.zeit.de)

How-to do it correct from the beginning?
How to Analyze (Mobile Ad hoc) Networks?
Best practice, since there is no perfect solution!

Systematic Performance Evaluation

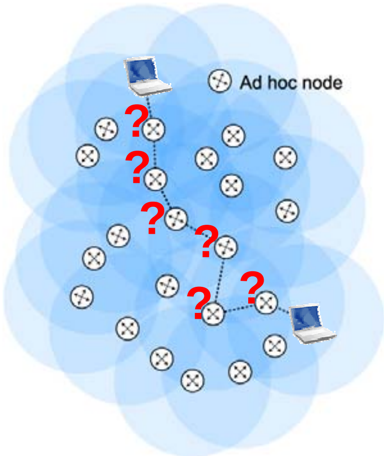
Again: systematic approach to performance evaluation (adopted from [Jain1991])

“Important Files”

1. The definition of the system (boundaries), goals, and services
2. The selection of the performance metrics
3. The definition of the parameters to study
4. The selection of the factors/elements of the parameter set
5. The choice of the evaluation technique
6. The development of the model and selection of the workload
7. The design and conducting of the individual experiments
8. The analysis and interpretation of the obtained data
9. The presentation of the results

Example: Ad hoc Network Performance

Scenario

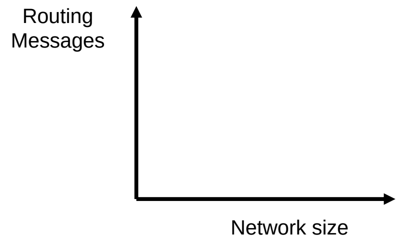


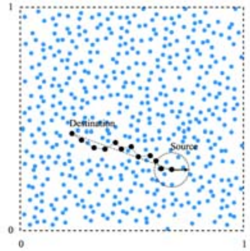
Challenge

- Qualify and quantify the effects of node misbehavior on the overall performance of the routing system

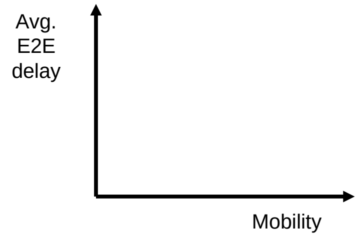
2. Selection of the Performance Metrics (2)

What do we expect?



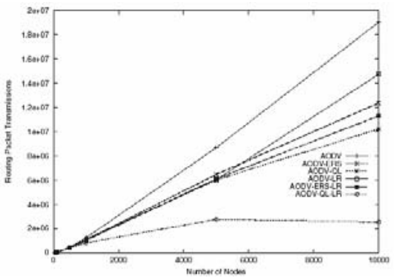


- Criteria to compare the performance (so-called metrics)
- Metrics relate to the speed, accuracy, and availability of services



2. Selection of the Performance Metrics (3)

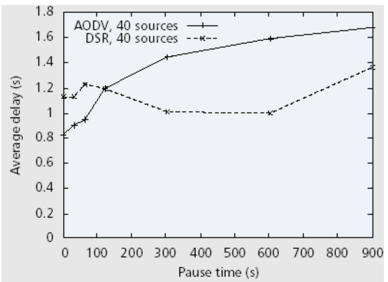
LeBePe2003



Some “realistic?” results

→ only useful in combination with other metrics

PeRoDaMA2001



5. Choice of Evaluation Technique

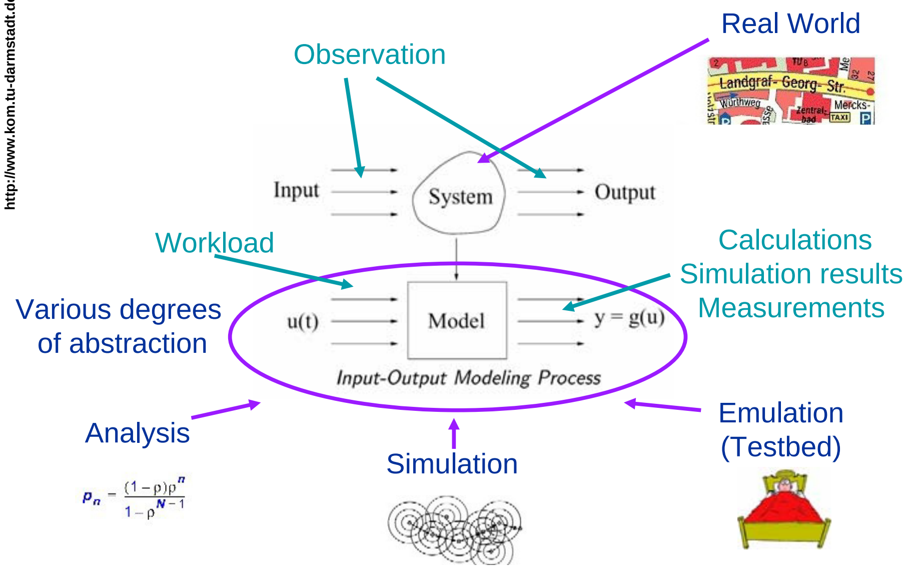
Current investigation methods (boundaries not fix)

Abstraction Level vs. Generality of Results

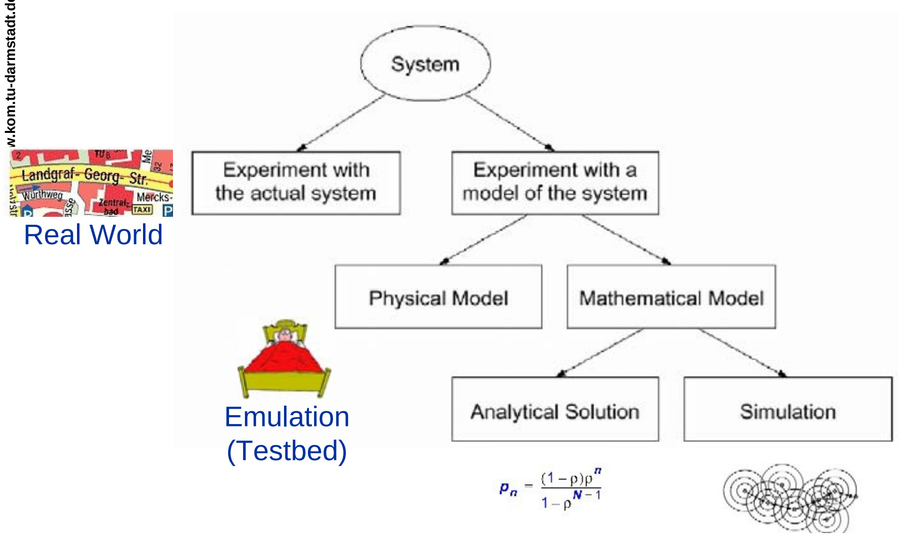
Analysis	Simulation	Emulation (Testbed)	Real World
$p_n = \frac{(1-\rho)\rho^n}{1-\rho^{N-1}}$			

- Real world observations
  - → no large scale MANET, expensive, only deployed technologies
- Emulation / Testbed experiments
  - → only small scale, expensive, complicated (modeling mobility?)
- Simulation studies
  - → medium scale (~50-1000 nodes), restricted to chosen scenarios
- Analytical models
  - → assume ideal protocols, mainly for capacity / connectivity on L2

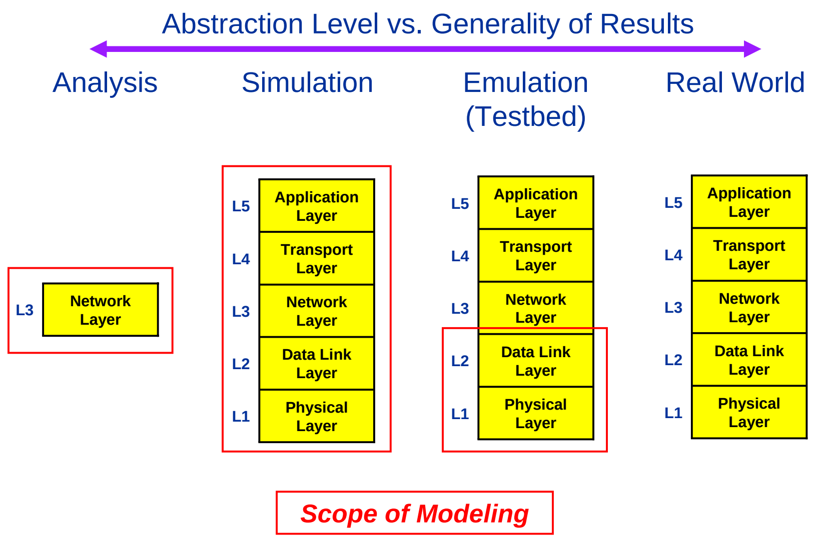
System and Model



Degrees of Abstraction (1)



Degrees of Abstraction (2)



6. Workload
7. Design and Conducting of Experiment

"Would you tell me, please, which way I ought to go from here?"
"That depends a good deal on where you want to get to," said the Cat.
"I don't much care where —" said Alice.
"Then it doesn't matter which way you go," said the Cat.

— Lewis Carroll, Alice's Adventures in Wonderland

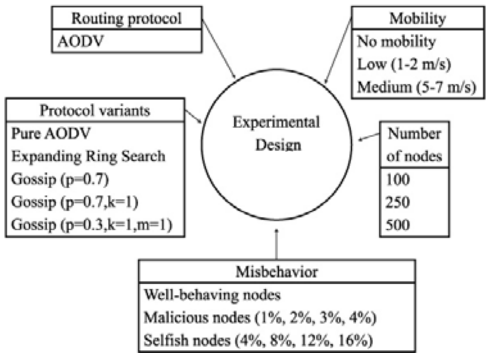
Workload is crucial

- Services exercised, Level of detail
- Representativeness, Timeliness
- Also consider load level!

Experimental Design

- Simple Designs (vary one factor at a time)
- Full/ Fractional Factorial Designs (utilizes full/partial combination of levels of all factors)
- How many experiments?
  - Given k factors, with the i th factor having n_i levels

7. Design and Conducting of Experiments (2)



Workload in Example

- Moderate
- Artifical
- 8% of nodes are sources (random)
- We use constant bitrate traffic over UDP.

Factors that are kept constant (250 node setup)

- Average node density = 9; Area = $(2334m)^2$; Simulation time = 900s
- Link layer = IEEE 802.11b with Distributed Coordination Function (DCF)
- Network layer = Ad hoc On-demand Distance Vector Routing, IPv4
- Transport/Application layer = Constant Bit-Rate (CBR) flows over UDP

8. Analysis and Interpretation of Data (1)

A man with one watch knows what time it is.
A man with two watches is never sure.
— Segal's Law

Steps contd.

- The analysis only produces results and not conclusions
- Based on these results the analysts/decision makers can draw conclusions
- Outcomes of measurements/simulations are random quantities
  - They change with each replication
- Take into account the variability of the results
- Simply comparing the means can lead to inaccurate conclusions
  - Proper statistics are basis for a unbiased analysis
- Each analysts will probably draw different conclusions are given the same set of results …

8. Analysis and Interpretation of Data (2)

2800	3200
5000	7000
5000	8000
8000	15000
10000	20000
10000	20000
20000	20000
60000	25000
75000	30000
100000	40000
100000	40000
100000	50000
100000	50000
100000	65000
150000	80000
180000	99999
250000	100000
250000	100000
300000	100000
400000	125000
500000	200000
500000	200000
550000	200000
1500000	300000
1500000	300000
17000000	750000

"Then there is the man who drowned crossing a stream with an average depth of six inches."
— W. I. E. Gates

Some statistics …

How many street lamps are operated in Frankfurt (am Main) …

- First guess vs. "educated" guess, N = 26 participants
- The correct solution was ~ 64,000 to 65,000 (or 42 ;-)
  - First guesses range from 2,800 to 17,000,000
    Mean = 914,454, 95% Confidence interval = +/- 437,160
    Median = 100,000, σ = 3,304,848
  - Educated guesses range from 3,500 to 750,000
    Mean = 113,392, 95% Confidence interval = +/- 20,590
    Median = 57,500, σ = 155,656

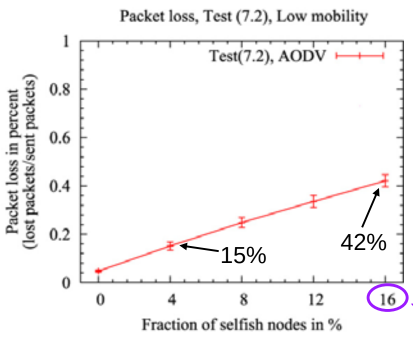
8. Analysis and Interpretation of Data (4)

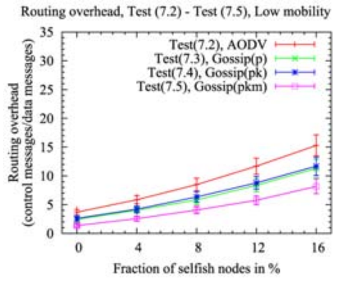
Tell me what you see:

Summary of Results for Test (7.2), AODV with ERS, low mobility, 250 nodes.

		Misbehavior									
	Factor	No	Selfish Nodes				Malicious Nodes				
	Fraction of misbehaving nodes	0	4%	8%	12%	16%	0.8%	1.6%	2.4%	3.2%	4.0%
(A)	Average end-to-end delay in ms										
(E)	Average loss										
(D)	Avg. path length										
(B)	Control Msg. per Data Msg.										
	RREQ/Ctrl.Msg.	95,1%	94,8%	94,6%	94,5%	94,4%	90,2%	87,2%	84,9%	82,6%	80,0%
(C)	RREP/Ctrl.Msg.	3,3%	3,4%	3,4%	3,4%	3,4%	7,5%	10,2%	12,3%	14,3%	16,3%
	RERR/Ctrl.Msg.	1,6%	1,8%	2,0%	2,1%	2,2%	2,3%	2,6%	2,8%	3,2%	3,6%

8. Analysis and Interpretation of Data (5)
Observations for Selfish Nodes





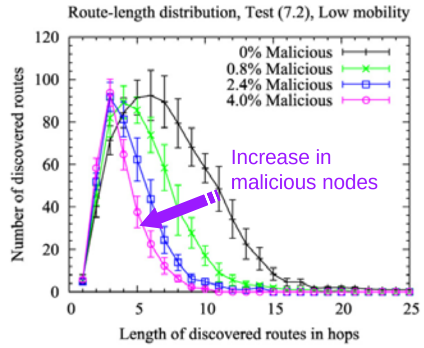
i.e. 40 out of 250 nodes

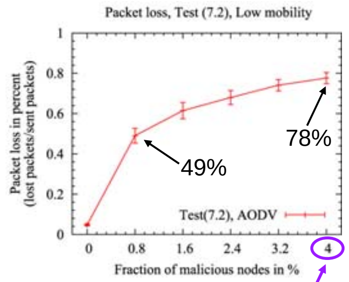
Packet loss increases …

- … nearly linearly with the number of selfish nodes
- … with node mobility

Routing overhead increases

8. Analysis and Interpretation of Data (6)
Observations for Black Holes





i.e. 10 out of 250 nodes

Successful communication only in close proximity

Packet loss …

- … is extremely high, even for few black holes
- … increases with node mobility

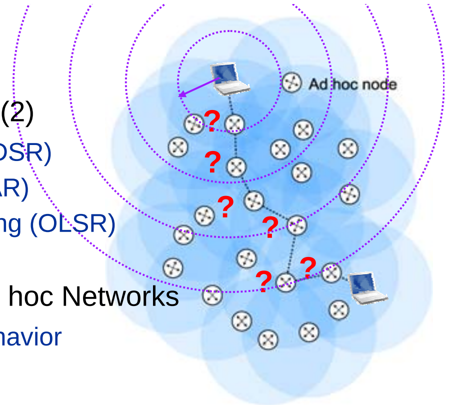
Closing the Art of Performance Evaluation

“Do not plan a bridge capacity by counting the number of people who swim across the river today.”

—Heard at a presentation

The quotes in this lecture part are taken from [Jain1991]

Outline (Part 2)



Selected Routing Protocols (2)

- Dynamic Source Routing (DSR)
- Location Aided Routing (LAR)
- Optimized Link State Routing (OLSR)

Routing Dependability in Ad hoc Networks

- The Effects of Node Misbehavior
- Modeling Ad hoc Networks

Performance Evaluation of Ad hoc Networks

- The Art of Performance Evaluation
- Analyzing Ad hoc Network Performance

Research Challenges, Summary and Conclusion

Appendix

Challenges in the Area of Ad Hoc Networks

Interesting problems spanning multiple layers
- Security, QoS, Scalability, Heterogeneity, Adaptation, Dependability

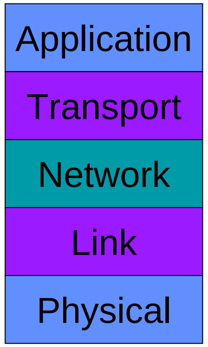
Application Layer
- Feasibility of Client-Server paradigm (DNS, Certificate Authorities)
- Discovery of Services, where to place services, service awareness

Transport Layer
- Esp. TCP-performance

Network Layer
- Adaptation of routing protocols, multicast routing
- Autoconfiguration of IP-Addresses
- Deal with routing misbehavior

Link Layer
- Medium Access Control / Scheduling
- Multiple Channels

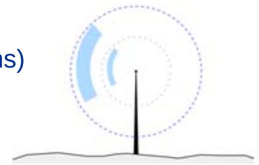
Physical Layer
- Adaptive Modulation, Smart Antennas
- Power Control (to maximize power-usage / to minimize interference)



Directional / Smart Antennas

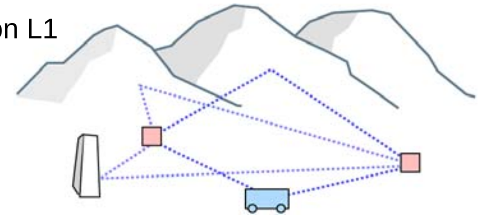
http://www.kom.tu-darmstadt.de

Various capabilities
- Sectored antennas (fixed beam positions)
- Beam steering
- Tracking a transmitter



Problems
- MAC and routing protocols for ad hoc networks using such antennas
- How to take into account antenna capabilities?
- Network may be heterogeneous (with respect to antennas)

Other interesting areas on L1
- Various diversity techniques
- Efficient coding schemes

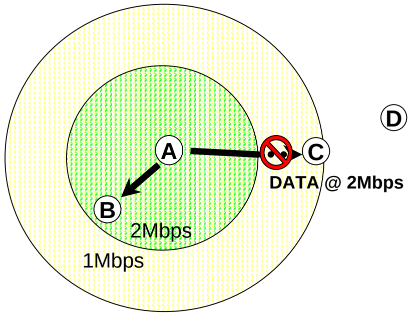


Autorate Fallback MAC Protocols

http://www.kom.tu-darmstadt.de

Asymmetric conditions

Sender-Based Protocol
- Sender decreases rate after N consecutive ACKS are not received
- Sender increases rate after Y consecutive ACKS are received



Receiver-Based Protocol
- Sender sends RTS containing its best rate estimate
- Receiver chooses best rate for the conditions and sends it in the CTS
- Sender transmits DATA packet at new rate
- Information in data packet header implicitly updates nodes that heard old rate

Layer 2 Scheduling

http://www.kom.tu-darmstadt.de

When multiple packets pending transmission, which packet to transmit next?

Choice should depend on
- Receiver status (blocked by some other transmission?)
- Congestion at receivers
- Noise level at receivers
- Tolerable delay for pending packets
  - Need interaction between upper layers and MAC
  - (→ for a master thesis about cross layer optimization in mesh networks do not hesitate to contact me)

MAC for Multiple Channels
- How to split bandwidth into channels?
- How to use the multiple channels?
  - Dedicated channel for control?

Routing Issues

Base protocols are quite well-understood (reactive, proactive)

- Interesting problems persist when other issues are considered (such as QoS or physical layer properties)
- No "one size fits all" solution
- Choice of protocol depends on
  - Density/number of nodes, mobility characteristics, application

How to design adaptive protocols?

- Existing proposals use a straightforward combination of reactive and proactive protocols
  - Proactive within "radius" K, reactive outside K
  - Choose K somehow
- There are also hierarchical protocols, clustered protocols, …

Completely other routing paradigms

- Geographical routing

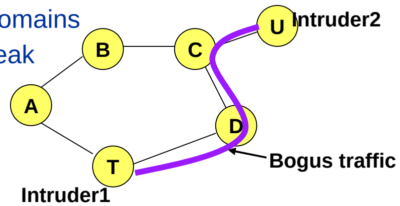
Security Issues - What's New ?

Characteristics

- Wireless medium easy to snoop on
- With ad hoc networking, hard to guarantee connectivity
- Easier for intruders to insert themselves into network
- New attacks: resource depletion attack

MANET vs. traditional security mechanisms

- Rely on infrastructure vs. absence of infrastructure
- Granularity and timescale of security relationships
  - Short lived, high number
- Handling of different security domains
- Limited resources / physical weak



Summary

Mobile ad hoc networks (MANET)

- Self-organizing, mobile and wireless nodes
- Absence of infrastructure, multi-hop routing necessary
- Systems are both, terminals (end-systems) and routers (nodes)
- Constraints (dynamics, energy, bandwidth, link asymmetry)

Characteristics include

- Mobility, wireless, application / traffic, and system characteristics

Routing is a central problem in ad hoc networks

- Topology-based, destination-based, hierarchical, geographical, cluster-based, etc. strategies
- Proactive, reactive, hybrid, etc. protocols
- Problems persist: QoS, Security, Scalability, Heterogeneity, …

Mobile Ad Hoc Network = MANET = Manet?

There is even more to the name MANET

- Édouard Manet (1832 – 1883)
- "Godfather" of impressionisms

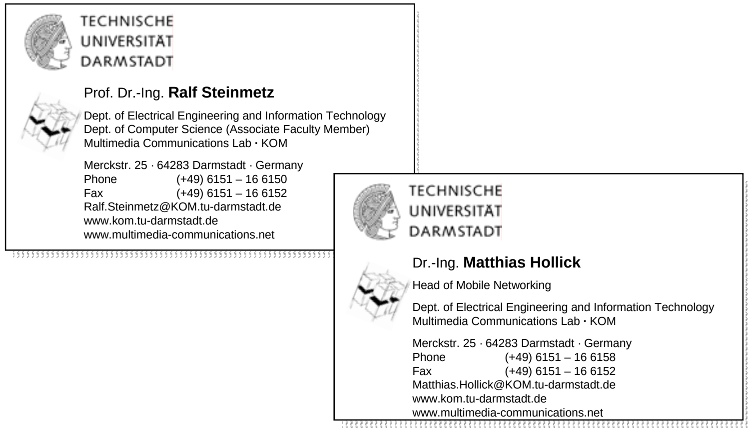
Acknowledgements, Copyright Notice

Acknowledgements for the ad hoc part go to various sources:

- N. Vaidya @ UIUC
- C. Perkins @ Nokia
- S. Corson @ UMD
- P.R. Kumar @ UIUC
- D. Johnson @ Rice
- Zhenqiang Ye @ UCR
- R. G. Herrtwich @ DaimlerChrysler
- WWRF
- The colleagues of the Mobile Networking Group @ KOM

Copyright Notice

Contact


TECHNISCHE UNIVERSITÄT DARMSTADT
Prof. Dr.-Ing. **Ralf Steinmetz**
Dept. of Electrical Engineering and Information Technology
Dept. of Computer Science (Associate Faculty Member)
Multimedia Communications Lab · KOM
Merckstr. 25 · 64283 Darmstadt · Germany
Phone (+49) 6151 – 16 6150
Fax (+49) 6151 – 16 6152
Ralf.Steinmetz@KOM.tu-darmstadt.de
www.kom.tu-darmstadt.de
www.multimedia-communications.net

TECHNISCHE UNIVERSITÄT DARMSTADT
Dr.-Ing. **Matthias Hollick**
Head of Mobile Networking
Dept. of Electrical Engineering and Information Technology
Multimedia Communications Lab · KOM
Merckstr. 25 · 64283 Darmstadt · Germany
Phone (+49) 6151 – 16 6158
Fax (+49) 6151 – 16 6152
Matthias.Hollick@KOM.tu-darmstadt.de
www.kom.tu-darmstadt.de
www.multimedia-communications.net

Additional information

http://www.KOM.tu-darmstadt.de

Appendix: Additional Readings (1)

Research Papers

- See course download page for selected research papers
  - Laura M. Feeney, *A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks*, Technical Report 1999
  - Young Bae-Ko and Nitin Vaidya, *Location-Aided Routing (LAR) in Ad Hoc Networks*, Infocom 1998

IETF Standardization

- MANET WG http://www.ietf.org/html.charters/manet-charter.html
  - AODV: http://www.ietf.org/rfc/rfc3561.txt
  - DSR: http://www.ietf.org/rfc/rfc4728.txt
  - OLSR: http://www.ietf.org/rfc/rfc3626.txt
  - TBRPF: http://www.ietf.org/rfc/rfc3684.txt
- The papers/standards are not mandatory for the course but you might find them interesting

Appendix: Additional Readings (2)

Books

- Raj Jain: "*The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*" (ISBN 0-471-50336-3)

Common Mistakes & How-to Avoid Them (1)

1. No Goals
   - Any endeavor without goals is bound to fail!
   - There is no such thing as a general-purpose model!
   - Goals → correct metrics, workloads, and methodology!
2. Biased Goals
   - "To show that OUR system is better than THEIRS" ?
   - Analysts = Jury!

(Source www.zeit.de)

Common Mistakes & How-to Avoid Them (2)

3. Unsystematic Approach
   - Arbitrary selection of workload → Inaccurate conclusions!
   - Systematic approach is key to solve performance problem!
4. Analysis without understanding the problem
   - The "world" model is the goal → No!
   - "A problem well stated is half solved"!
5. Incorrect Performance Metrics
   - Chosen to be easily computed rather to be relevant?
6. Unrepresentative Workload
   - Should represent the actual usage of the system!

… see Appendix for other common mistakes

(Source www.zeit.de)

Common Mistakes & How-to Avoid Them (3)

7. Wrong Evaluation Technique
   - Use the technique you know best vs. the appropriate one?
   - Methods are measurement, (emulation), simulation, analysis!
8. Overlooking Important Parameters
   - Just do it?
   - Make a list of all system/workload characteristics!
9. Ignoring Significant Factors
   - Vary only well-understood parameters?
   - Use the factors that impact the performance most!
10. Inappropriate Experimental Design
    - Naïve: each factor changed one by one → cross-influences?
    - Improper selection → Waste of time!
11. Inappropriate Level of Detail
    - Too narrow vs. too broad …
    - Slight variations to study → detailed model!

Common Mistakes & How-to Avoid Them (4)

12. No (bad) Analysis
    - Measure, measure more, ... → you've just produced tons of data!
    - Produce summary, include analysis + measurement background!
13. Erroneous Analysis
    - Average of ratios (example earlier)?
    - Too short simulations?
14. No Sensitivity Analysis
    - Fact vs. evidence! → very much depends on workload!
    - Clarify relative importance of parameters!
15. Ignoring Errors in Input
    - Uncertainty because of inaccurate measurements?
    - Biased input?
16. Improper Treatment of Outliers
    - Too high or too low values? → real system phenomenon or outlier needs to be clarified!

Common Mistakes & How-to Avoid Them (5)

17. Assuming No Change in the Future
    - Future is same as past? → carefully limit assumptions!
18. Ignoring Variability
    - Analyze only the mean performance?
    - E.g. take only daily average of load demands if peak hours exist?
19. Too Complex Analysis
    - Reality: the more complex the model the “easier” to publish …
    - Simple models are beneficial for day-to-day purposes!
20. Improper Presentation of Results
    - Right metric to measure performance of analyst is not number of analyses performed but number of helpful analyses!
21. Ignoring Social Aspects
    - Underestimation of presentation? → social skills important!
22. Omitting Assumptions and Limitations
    - Missing assumptions in report? → results are falsely transferred!