Advanced Topics in Communication Networks

Prof. Dr. Bernhard Plattner
Dr. Martin May
Dr. Merkouris Karaliopoulos
Dr. Ulrich Fiedler
Dr. Thrasyvoulos Spyropoulos

Assistant : Georgios Parissidis

Autumn semester 2007
Linking to the previous lectures and ATCN...

- First three courses were on autonomic network communication
  - Discussed basic *generic* principles of autonomic communications and also future network architectures that best accommodate them
    - self-* features (awareness, configuration, optimization, healing)
    - blurring the *protocol layering* in favor of network compartments

- In the next three lectures we are going to talk about *particular network paradigms* that
  - have been a serious motivation for *rethinking the Internet architecture*
  - bear strong elements of *self-organization* and benefit enormously from *cross-layer* approaches
### Notation

を持っているあなた！
- Check point for your understanding or background
- Who answers?
  - student k, where k = (slide_number mod 8) + 1
  - numbering runs bottom-up, right-left
  - when two questions in the same slide, or second answer needed, student k+1 answers

👍 advantage, strength
- Used mainly with regard to protocol/algorithm/model properties or

👎 disadvantage, weakness
Wireless multihop networks: challenges, state-of-the-art, and open issues
Basic definitions

- Wireless multihop networks: an umbrella-term for different types of networks
  - mobile ad hoc networks
  - static wireless mesh networks
  - sensor networks

- Common features
  - they are wireless
  - they involve multiple wireless hops
  - have self-organization features (functionality distributed amongst network nodes)

- Different paradigm with respect to conventional wireless networks
  - Cellular mobile (GSM, GPRS, UMTS)
  - Wireless LANs
Example WMN scenario: Community mesh networks

- Infrastructure belongs to the users
- Often exists in parallel with mainstream access technologies
  - Cable, ADSL or wireless (WLL, WiMAX)
Community mesh network applications

- Shared broadband Internet access
  - one pays, many get Internet access

- Exchange of content amongst the network users
  - movies, clips, photos

- Applications of local interest
  - Neighborhood watch (video surveillance)
  - Local announcements (billboard)

- Distributed backup
Example WMN scenario: Wireless Metropolitan networks

- When community networks scale up...

  Athens Wireless Metropolitan Network (AWMN), Greece

  Melbourne Wireless Metropolitan Network, Australia

Top Zürich Wireless Metropolitan Network ??
Example WMN scenario: Vehicular networks

- Vehicles ≈ moving platforms of sensor and actuators

- Ad hoc network of vehicles exchanges information about traffic but also entertainment purposes
…and sth more futuristic: Flying wireless mesh network

- Ad hoc network set up via a swarm of flying robots for search and rescue operations
Yet another network...

- in the end of the day, all I have is a network that has to transfer data from one node to the other while
  - satisfying the application requirements
  - and making efficient use of the network resources

What are typical **application requirements** from the network?

What are the **network resources**?
Outlook

Three lectures on Wireless Multihop Networks

- Lecture 1: Challenges

- Lecture 2: Engineering WMNs – part 1: Routing
  - Routing protocols and metrics

- Lecture 3: Engineering WMNs – part 2
  - Transport
  - Alternative MAC solutions
  - Topology control
  - Co-operation enforcement and security attack countermeasures
Lecture summary: challenges for communication in WMNs

- Wireless propagation environment
  - Radio channel dynamics
  - Interference

- Distributed MAC layer protocols
  - Decisions made on basis of local knowledge

- Mobility
  - Issue primary for MANETs

- Energy constraints
  - Handheld, low-end devices, sensors

- Security/co-operation
  - Both from information-level point of view
  - But also from system-level point of view
**dB and dBm - just in case...**

- both used broadly in engineering
  - relevance to link engineering – link budgets

- **dB**: relative logarithmic unit for the ratio $A$ of two quantities $x_1, x_2$
  - $A \ [\text{dB}] = 10(20) \log_{10} (x_1/x_2)$
  - 10 or 20 depends on the context of $x_1, x_2$
    - e.g., voltage : 10, power : 20

- **dBm(dBW)**: absolute logarithmic unit, fixed reference 1mW(1W)
  - $P \ [\text{dBm}] = 10 \log_{10} (P/1\text{mW})$

💡 **dB arithmetic**

- If $P_1 = 10\text{dBm}$ and $P_2 = 10\text{dBm}$, how many dBm is $P_1+P_2$?
Radio propagation: relevance

\[ P_R = P_T - L - L_T - L_R + G_T + G_R \text{[dB]} \]

Link budget equation

- Link engineering practice
  - known sender/receiver characteristics \((L_T, L_R)\) and antenna gains \((G_T, G_R)\)
  - required \(P_R\) is a function of the application and receiver characteristics but known
  - need to estimate \(L\) in order to set \(P_T\) => requirement for modeling the radio propagation channel
Radio propagation: first comes the Physics

- Electromagnetic energy propagates in space via various mechanisms
  - reflection and refraction
    - upon change of electromagnetic properties of the medium
  - diffraction
    - explains the existence of field in the “shadow” region behind obstructions
  - scattering
    - explains spread of energy from “electromagnetically rough” surfaces
      - “Roughness” \( \propto \) surface roughness but also \( \theta_i \)

- In mobile environments one must also consider
  - shadowing
  - multipath fading
...then comes the modeling

- Three types of models for radio propagation loss
  - Physical
    - Take into account information about the terrain (buildings, obstacles) and apply ray tracing
      👍 better insight to the actual phenomena
      👎 needs a lot of detail for reliable estimates, computationally intensive
  - Empirical
    - based on measurement data and fitting techniques
      👍 very simple to use
      👎 no insight to the phenomena, their reuse is questionable
  - Statistical
    - Probability distribution functions for signal properties
    - Intermediate solution with respect to the provided insights and complexity
Mobile wireless links: the three signal components

- **distance-based component**
  - Physically and empirically modeled
  - Function of inverse power law
    - Log distance model: \( P_r(d) = P_r(d_0) - a \cdot 10 \log(d/d_0) \) [dB]
    where \( \alpha \) : path loss exponent, typically \( 2 < \alpha < 5 \)

- **shadowing component**
  - due to buildings and trees on the signal path
  - correlations in the order of building/tree dimensions
  - dominant modeling approach : statistical
    - shadowing amplitude follows a Lognormal distribution
  🧐 What is the distribution of the respective dB values?

- **multipath component**
  - dominant modeling approach : statistical (Rayleigh, Rice, Nakagami,...)
  - correlations in the order of the wavelength
  🧐 how much is the wavelength (order of size)?
The three scales of signal variation

- **distance-based component**
- **multi-path fading**: fast signal variations
  - in the order of 20dB
- **shadowing**: slow signal variations
- separation can be achieved with filtering
  - though not perfect
Multipath fading: implications

- Signal propagates via multiple paths to the receiver
  - Rayleigh fading: no line-of-sight component between Tx-Rx
  - Several signal replicas add at the receiver
    - may add constructively or destructively
  - the resulting variations sit on top of the mean signal power and reduce the communication margin
Multipath fading 1\textsuperscript{st} order signal statistics

- fading amplitude probability distribution function (pdf) and cumulative distribution function (cdf)
  - used in the link dimensioning process

Example:

- a mobile receiver achieves acceptable\* bit error rates when the instantaneous SNR > 9dB. What mean SNR is required under Rayleigh multipath fading to get those acceptable rates for 99% of time?

\* acceptable BER $\Rightarrow 10^{-3}$ for legacy voice. $10^{-6}$ for data
Multipath fading 2\textsuperscript{nd} order signal statistics

- Autocorrelation process, level crossing rate, average fade duration
  - Used to dimension transceiver elements (interleaver)

  \[ f_m = f_c \cdot \frac{v}{c_0} \]
  For \( v=50 \text{km/h}, f_c = 2 \text{GHz}, f_m = 92.6/\text{sec} \)

- Autocorrelation falls down to 0.707 within 1.9ms and to zero in around 4.3ms
  - i.e., within 1 sec the channel changes ~ 250 times...
Interleaver

Concept: spread the bits in time, so that the errors due to a fade appear adequately random at the decoder input
Multipath fading: the other side of the coin

Half-empty or half-full?

- half-empty view: see fading as a signal impairment and accommodate it in the link budget with additional margin (fade margin)

- half-full view: diversity techniques
  - Spatial diversity: multiple physically separated Tx and/or Rx antennas
  - Time diversity: send a slightly delayed in time replica of the signal
  - Combine the signal replicas at the receiver
Indoor propagation models

- largely empirical models --two basic approaches in empirical modeling

- 1st approach: use the same empirical models used for outdoor but change the path loss exponent depending on the environment
  - For example: \( P_r(d) = P_r(d_0) - a \cdot 10 \log(d / d_0) \) [dB]

- 2nd approach: use the same empirical models as in outdoor but account explicitly for the in-building loss due to walls and floors

<table>
<thead>
<tr>
<th>Environment</th>
<th>Path loss exponent, ( \alpha )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free space</td>
<td>2</td>
</tr>
<tr>
<td>Urban cellular radio</td>
<td>2.7 to 3.5</td>
</tr>
<tr>
<td>Shadowed urban cellular radio</td>
<td>3 to 5</td>
</tr>
<tr>
<td>In building line-of-sight</td>
<td>1.6 to 1.8</td>
</tr>
<tr>
<td>Obstructed in building</td>
<td>4 to 6</td>
</tr>
<tr>
<td>Obstructed in factories</td>
<td>2 to 3</td>
</tr>
</tbody>
</table>
Indoor propagation models: effect of walls and floors

- Set the path loss exponent equal to 2 (free space) but add explicit wall- and floor-related factors

\[ P_r(d) = P_r(d_0) - 20 \log(d / d_0) + n_f \alpha_f + n_w \alpha_w \text{ [dB]} \]

\( n_f(w) \): number of floors (walls) \( \alpha_f(w) \): attenuation factors of floors (walls)

- Include the wall effect into the path loss exponent and explicitly add a floor-effect factor (ITU-R model)

\[ L_T = 20 \log f_c + 10 \alpha \log r + L_f(n_f) - 28 \text{ [dB]} \]
Indoor propagation models: multipath and shadowing

- **Shadowing**
  - Still modeled as Lognormal, only now the location variability depends more strongly on the environment
  
  \[ P_r(d) = P_r(d_0) - a \cdot 10 \log(d / d_0) + X \, [\text{dB}] \]

<table>
<thead>
<tr>
<th>Frequency [GHz]</th>
<th>Residential</th>
<th>Office</th>
<th>Commercial</th>
<th>Laboratory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.8 – 1.0</td>
<td>-</td>
<td>3 [Keenan*]</td>
<td></td>
<td>6 [Keenan]</td>
</tr>
<tr>
<td>1.7 – 2.0</td>
<td>8 [ITU]</td>
<td>10 [ITU]</td>
<td>10 [ITU]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 [Keenan]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Multipath**
  - Main difference in the second-order statistics
  - Equally “wild” short-term signal amplitude variations

Broadcast/ multicast: wired vs. wireless - just in case...

- wired networks
  - physical links are primarily unicast
  - Multicast/broadcast has to be emulated at network or higher (e.g., application layer)

- wireless networks
  - physical links are *a priori* broadcast
  - multicast is emulated *a posteriori*, via filtering at MAC or higher layers

👍 Hence, in wireless, one can reach many easier
👎 ...but this is where interference kicks in, right?
Interference

- External interference: from transmissions of other systems in the same band or adjacent bands
  - in general, frequency bands are licensed
  - possible in the ISM band (2.4-2.483 GHz), where 802.11b/g operates

- System-internal interference
  - co-channel interference
    - channel: frequency band (FDMA), time slot (TDMA), code (CDMA)
    - frequency reuse techniques
  - adjacent channel interference
    - power spill over of transmissions in neighboring bands
    - strict specifications of filter masks
  - MAI (multiple access interference)
    - CDMA systems: power control
Interference in 802.11x networks

- external interference due to operation in the unlicensed band
  - microwaves, cordless phones primarily
  - 11-chip Barker code yields a ~10dB spreading gain over external interfering source

- System-internal interference
  - 802.11b/g has 13 channels in Europe, 5MHz wide, centered on 2.412+5k GHz, k=0..12
  - the standard requires a receiver filter rejection of 35dBm at distances > 25MHz apart from the centre frequency
  - there are max three non-overlapping channels, {1, 6, 11} –most production networks experience adjacent channel interference
Interference in 802.11x networks

- Interference in 802.11x networks often used in different context
  - Has to do with the way CSMA/CA works and the phenomena it gives rise to
  - We will say more on this when talking about MAC in more detail...
References


- M. Gast, 802.11 Wireless Networks: the definitive guide, O’ Reilly, April 2005


- D. Tse, P. Viswanath, Fundamentals of wireless communications, Cambridge University Press, 2005
MAC: what do I want to do with it?

- I want stations to share the wireless medium *efficiently*
  - must allow access to everyone
  - should do this in a “fair” manner
  - should avoid unnecessary transmissions (collisions, retransmissions)
    - reduce throughput/utility of the medium
    - waste battery of the device
      - Could be a problem with energy constrained devices

- plus...
  - this has to be done in a *distributed* manner
  - compare this for a moment with centralized MAC
Centralized network functions - an example

- Cellular network – 3G

“dump” node – physical layer

“Brains” of the radio network

Internet
Carrier Sense Multiple Access (CSMA)

- CSMA: sense the medium to see whether it is busy
  - if not, transmission can start
  - if it is, defer transmission for later doing exponential back-off

- In wired networks, Collision Detection (CD) is possible (e.g., Ethernet)
  - a station can infer the collision while it happens, interrupt its transmission and send a jam signal to inform other nodes before doing back off

- In wireless media CD is not possible
  - transmit signal much stronger than the received one, would require expensive hardware to sense the collision
  - there are cases (hidden nodes) which cannot hear the transmissions
  - IEEE 802.11 uses CSMA/CA (Collision Avoidance)
IEEE 802.11x medium sensing mechanisms

- **Physical sensing**
  - use directly the electronics to sense the received power over the air
  - medium is assumed busy when the power at the antenna connectors is higher than the CCA (Clear Channel Assessment) threshold
  - the receiver may consider *any* signal or an *802.11x* signal

- **Virtual carrier sensing**
  - use RTS/CTS packets to notify other nodes for the intention to transmit
  - a certain field in the packet “reserves” the medium for certain time
  - the nodes that receive the packets update their *Network Allocation Vector* and know that the medium will be busy for the respective interval
Three relevant radio ranges

- Reception range ($r_{RX}$)
  - Range within which a packet is successfully received under no interference (only thermal noise)
  - Determined by sender transmission power and radio environment

- Carrier Sensing range ($r_{CS}$)
  - Range within which a transmitter can be sensed (physical sensing) by other nodes

- Interference range ($r_{I}$)
  - Range within which receiver nodes will be interfered with by a third node so that the packet is lost
  - Depends on the distance from the sender
Hidden node

- ...or: a node DOES transmit when he SHOULD NOT do so

- C cannot sense A’s transmission, so his transmission (to B or elsewhere) interferes with A’s
RTS/CTS as a hidden node countermeasure

- Mitigates the hidden node effect in infrastructure WLANs
  - the sender node advertises his intention to send data with a small RTS packet
  - it reserves the medium for the time required to transmit the data
  - the receiver replies with a CTS packet which is heard (with a high probability) by the hidden node

- Less effective in WMNs
  - the interfering node not always within the transmission range of the receiver
  - the exchange of RTS/CTS may worsen the interference in the network
Exposed node

- ...or: a node DOES NOT transmit when he SHOULD

- B’s transmission to A is sensed by C, since B is within its carrier sense range
- C does not transmit to D although C’s transmission does not interfere A and B’s transmission does not interfere D
Three ranges and hidden/exposed nodes

$R_H$: hidden node zone

$R_E$: exposed node zone

$d$: Tx-Rx distance
Three ranges and hidden/exposed nodes

- $R_H$: hidden node zone
- $R_E$: exposed node zone
- $d$: Tx-Rx distance

- Not possible to eliminate both
  - Decrease of $R_H$ results in increase of $R_E$
  - ... and vice versa
Interference range - single interferer

Received power at distance $d$:

$$P_r(d)[dB] = P_r(d_0)[dB] - a \cdot 10 \log(d / d_0) \quad \text{or} \quad P_r(d) = P_r(d_0) \cdot (d / d_0)^{-a}$$

$d_0$: reference distance  $\alpha$: path loss exponent

SINR at receiver:

$$SINR = \frac{Pr(d)}{Pr(I) + N_0} \approx \frac{Pr(d)}{Pr(I)} = \frac{Pr(d)}{Pr(d) \cdot (I / d)^{-a}} = \left( \frac{I}{d} \right)^a$$

Interference has an impact as long as:

$$SINR \leq \beta \Rightarrow ... \Rightarrow I \leq d \cdot \beta^a \Rightarrow r_I = d \cdot \beta^a$$
Interference areas - a more realistic view

- the interference range depends on the number of interference sources*

- it is possible to define interference zones \( A_{j,m} \), where \( m \) : minimum number of required interferers to have an impact on receiver \( j \)

- Ranges of zones are a function of the Tx-Rx distance

CSMA/CA: How many can transmit simultaneously?

- Only 6 nodes around the central one can transmit simultaneously (1\textsuperscript{st} tier)

- Only 12 nodes around the central one can transmit simultaneously (2\textsuperscript{nd} tier)

- Collisions may arise depending where the Rx is
Interfering links

- Interference is used within 802.11x context as a shortcut for the hidden node and exposed node phenomena
  - definition: a link $AB$ interferes with link $CD$, as long as the throughputs of the two links $T_{AB}$ and $T_{CD}$ when they are simultaneously used are smaller than when they are individually active

- Link Interference Ratio (LIR) vs. Broadcast Interference Ratio (BIR)
  - LIR: the interference measure, $0 \leq LIR \leq 1$
    \[
    LIR_{AB,CD} = \frac{T_{AB,CD}^{AB} + T_{AB,CD}^{AB,CD}}{T_{AB} + T_{CD}}
    \]
  - BIR: the actual metric, measured with scalability in mind
    - each node first broadcasts individually –measure $T_{AB}$ and $T_{CD}$
    - nodes then broadcast in pairs –measure $T_{AB}^{A,C}$ and $T_{CD}^{A,C}$
    \[
    BIR_{AB,CD} = \frac{T_{AB}^{A,C} + T_{CD}^{A,C}}{T_{AB} + T_{CD}}
    \]
Conflict graphs

- Graph $G(V,E)$ where
  - Set of vertices $V$ is the set of network links $\sim N(N-1)$ for number of nodes $N$
  - An edge is added between two vertices as long as $\text{BIR} < e$
    - $e \equiv$ threshold defining what we consider “interference”

- Once the conflict graph is at hand it is possible to get significant improvements in the system throughput via theoretical centralized routing and scheduling*
  - Performance gains pertain even under the distributed scheduling function of 802.11b

Implications on network throughput/ capacity

Wired network

Assume 3 streaming CBR flows of 128kb/s each traverse the network
No cross-section of the flows’ paths

What is the network throughput?
Implications on network throughput/ capacity

Wireless network

Assume 3 streaming flows of 128kb/s each traverse the network of 802.11a/b/g links (minimum Tx rate 1Mb/s)

What is the network throughput now?
Self-interference: the aftermaths of CSMA

- Even a single flow interferes with itself!
  - Nodes B and D do not transmit, since they sense the medium busy
  - Node C is hidden from A and E from C, i.e., collisions at B and D

- Bidirectional traffic (e.g., TCP ACKs) and use of RTS/CTS only aggravate the phenomenon

- Simulations have shown that the throughput in a node chain decreases down to 1/7 of the throughput in the 2-node chain for > 10 nodes
Getting some capacity bounds

- Gupta and Kumar provided first some bounds [1]
  - per-node throughput $\lambda(n)$ is $O\left(\frac{1}{\sqrt{n}}\right)$ under optimal placement of destinations, scheduling, routing
  - $\lambda(n)$ is $O\left(\frac{1}{\sqrt{n \log n}}\right)$ under random selection of destinations and uniform nodes
    - quite pessimistic!

- Some more optimistic views
  - Mobility can be exploited to improve throughput as long as delay is not a concern [2]
    - Two-hop routing scheme lets throughput scale
  - More empirical studies have shown that the throughput is a function of traffic pattern locality [3]

Tonio will tell us more on this on Wed Nov 14th...


Quick and dirty proof of the $1/\sqrt{n}$ law (1)

- assumptions
  - uniform node density $d$ over a square network area of size $A$ so that the node density remains constant, i.e., $n = d \cdot A$
  - nodes choose random destinations for sending data
  - each node transmits its own traffic and acts as relay for the traffic of other nodes

- hence
  - Total per-hop capacity $C$ is proportional to the area $A$, i.e., $C = k \cdot A = k \cdot n/d$
  - $C$ also satisfies the equality $n \cdot \lambda \cdot E[\text{hop}] \leq C$, where $\lambda$: per node throughput and $E[\text{hop}]$: mean number of hops for each source–destination pair
  - combining the two expressions for $C$, it comes out that $\lambda \cdot E[\text{hop}] \leq k/d = c_1$, i.e., $\lambda_{\text{max}} = c_1/E[\text{hop}]$
Quick and dirty proof of the $1/\sqrt{n}$ law (2)

- How does $E[\text{hop}]$ vary?
  - For the given scenario and a square area, the number of hops is proportional to the $\sqrt{A}$, i.e., proportional to the $\sqrt{n}$ [1]
  - hence, $\lambda_{\text{max}} = O(1/\sqrt{n})$

Node mobility

- Relevant to MANETs

- Links and routes break as nodes move
  - network topology is more dynamic

- Classical routing approaches (proactive) do not fit well
  - No real need to maintain continuously information about the network, unless there is continuous data transmission

- Standard end-to-end transport protocols (e.g. TCP) have problems
  - Interaction of path change with TCP flow control results in low protocol throughput
  - This is on top of the problems TCP faces due to the MAC dynamics (hidden/exposed node phenomena, flow self-interference)
Energy constraints

- Higher performance requires more intensive processing
  - Results in higher energy consumption
  - Big problem for small devices (handhelds, PDAs) but also for mobile laptops

- Transmission wastes much more power than reception
  - Need to minimize failures in transmissions and retransmissions

- Battery lifetime
  - new bottleneck in these systems – no analogue of Moore’s law here
    - battery power doubles every 35 years...
  - mobile users now need more some extra hours of battery duration than another couple of GHz processor speed...
Energy consumption

- Much effort from industry on this – both short-term and longer-term
  - Energy-friendly design of devices
  - Power management tool
  - New power sources (e.g., fuel cells)
Co-operation

- So far we identified a couple of problems in the way the system works
  - they have to do with performance-related matters

- Well, it can really get worse...How?
  - We took for granted that all nodes cooperate in the network. What if they do not?
Node misbehavior: routing

- drop all kind of packets

- drop all or some packets of other nodes, while forwarding its own (selfish node)

- forward packets but after
  - reordering them
  - delaying them variably
  - both actions may cause problems to the layer above (e.g., TCP)

- send falsified routing messages
  - route updates
  - stale route advertisements

- decrease the TTL of packets so that they do not reach the destination
Node misbehavior: MAC layer

- Change MAC protocol parameters
  - back off parameter the usual suspect
  - Increase the NAV value in the RTS/CTS packets to occupy the medium for more time
  - Shorten the duration of wait intervals defined by the standard, to get first access to the channel

- Selectively scramble frames sent by others
  - CTS frames: CTS loss is followed by idle interval, which can be occupied by the selfish node
  - ACK and DATA frames: transmission time is not saved but the senders will end up with higher backoff values

- hardware misconfiguration
  - reported disobedience of wireless cards to the 802.11 standard*

Security attacks

- At high level the threats are the same with a wired network
  - Messages can be intercepted, modified, delayed, replayed or fake messages can be inserted
  - ...but both the wireless and the highly distributed operation of the system make things worse
    - delays detection and treatment of attacks, increases dependence on routing

- Vulnerability differs according to the type of network –existence of administrative restrictions
  - most challenging scenario: community mesh

- Attacks can be carried out from isolated nodes or colluding nodes (cheaters)
Security attacks

- Attacks may address different layers
  - Physical layer: damage hardware or jamming
  - Greedy/selfish behavior at MAC and routing level
  - Application layer: inject false or fake information

- Types of attacks
  - Impersonation
    - pretend to be someone else
  - Sleep deprivation
    - keep a node busy to exhaust his battery
  - (D)DoS
    - simpler at MAC layer
  - Sickhole attack and wormhole attack
    - use the routing protocol to advertise best path to the victim nodes
Two notes on the paper presentations and the exercises
Paper presentations - sth to check


- Some of the recommendation are more relevant to the reviewing task, yet good insight to the reviewers’ expectations from certain paper sections

- Proposes a three-pass approach in attacking a paper
  - First pass: abstract, intro, section-subsection headings, conclusions, and a look at the references
  - Second pass: read the paper without insisting on proofs, check figures and diagrams, write down notes on the important points of the paper (~1h)
  - Third pass: go through the paper in detail (~5-6hs, more depending on familiarity)
Paper presentations and exercises - things to know

- The expectation is that everyone takes a good read of the papers presented
  - the exercise has questions/tasks from both the lecture material and the papers to be presented
  - in the exams there will be questions from the papers

- Duration of presentations ~ 20mins
  - a list of questions will be sent to Tonio and Samuel
    - the presentations should also address those questions
  - the same questions will be discussed in the end of each presentation
    - the class will identify the answers, as given in the presentation, and comment on their correctness
  - of course, the class is welcome to pose additional questions