Everything about Real-Time networks

Important definitions

- Contention window: The set of numbers a backoff time is chosen from
- **Response-time**
    - Tiden det tar fra en av inputene endrer seg til at den tilsvarende responsen kan føles.
- Event triggered.
    - Event triggered=> Max end-end delay.
    - Need to know order of events => Possible synchronisation.
- Temporal consistency
    - If t_a and t_b represent the time wich the values of two (Possible external variables) were acquired
    - Absolute=> $|\, t - t_a| \leq A$ Where t_a is the time where the sample was taken and A is a threshold. (Freshness)
    - Relative $|\, t_a - t_b| < R$
- Spatial consistency: Copies of information among a set of nodes are identical.
- LAN: A data link that uses the same physical layer and medium access protocols
- Data link: Two end-points, and the communication channel between them which allows for data exchange.
    - data link (IEC 8802.2) – "an assembly of two or more terminal installations and the interconnecting communication channel operating according to a particular method that permit information to be exchanged. In this context, the term terminal installation does not include the data source and the data sink".
-
- Trafic: $\{\, T_i, D_i, C_i\}$
    - C_i: Length of message
    - T_i
        - Periodic traffic model => Period of transfer
        - Sporadic model => min. interarrival time.
    - D_i: Rellative period from arrival (or period time)
- **QoS** (Quality of Service)
    - Transfer delay bounds
    - Transfer delay variations (jitter)
    - Throughput
- Flow control:
    - Technique for regulationg the amount of data that is transferred by two data that work at different speeds, so that no-one is overwhelmed.
    - Link layer: Feedback-based => Sends data frames after having received acknowledgement from the user.
    - Network & Transport layer: Rate-based => Built-in mechanism for limiting rate of transmission without needing acknowledgement.
    - Sliding window: Multiple transmission without receiving ack.
- Coexistence

    - Internal: Measures the capability of different networks that operate on the same technology (i.e. Two separate BLE clusters)
    - External: Measures the ability that operates on one technology to operate in the presence of networks on other technologies.
- SIFS: short interframe space: Number of ms from a wireless interface has received frame until it is able to send a response frame.
-

Not important definitions

- MSDU: MAC Service Data Unit
    - IP-package + some LLC-data (=>The link layer's "Pyload"(?))
- Admission control:
    - A check before a connection is made to see if the current resources are sufficient for the proposed connection.
- Data circuit: Common path between two or more physical enteties with the nececari facilities for transmiting bits on it.
- Segment: Data circuit when the nodes are connected through wires
- Cell: data circuit, but over wireless
- Real subnetwork: Equpment+ media that can transfer bits for data transfer. (Mest be an autonomous whole)
    - Subnetwork: Abstraction of real subnetwork.
- Errors can both be bursty (Interference), or lasting (Fading)
- **Drop**: The piece of cable that goes from a node to the common on the main cable (the bus)

Wired networks

- Høyere line-speed => Større overhead av request-response protokoller.
- TNS (Time-Sensitive Networking)
    - Forsøk på å gjøre eternett Real-time
- Errors are well modeled by packet error rate with no correlation

Both kinds of networks

- Protokoleler:
    - Asynkrone=> Energieffektive ved lav trafikk + gode for coexistence
    - Synkrone: Høy utilization, og bra ved god trafikk. Men Sliter med mobility?
- Bridges: (Basically switches)
    - But software based, not hardware-based.
    - Can only have one spading tree instance (Not like switches)
-

Data link layer:

- Often dependent on physical medium
- Flow control
- Frame-synchronisation
- Management of access to medium

Network layer

- Stateful: Manage separate state for each flow. Operations are performed per low
- Stateless:

Transport layer

- ISO transport layer QoS parameter
  - Connection establishment [max] delay
  - Connection establishment failure probability; Connection release delay
  - Transit delay: Time data is submitted to when it is delivered. (Accessible to the other application (?))
  - Transfer failure property, Throughput,

Misc.

- RBER (Residual Bit Error Rate): Probability that a bit is erroneous, but not detected as wrong.
- Gateways: When protocols on the application latera are different on both sides.
  - Connecting a CAN-network to the internet using HTTP
- We look at things in bit-rate, not baud rate in this course.
- CDMA (Code division Multiple access):
  - Like a combination of TDMA and FDMA
- TDMA => All nodes are on the same frequency
- FDD & TDD ((Frequency- & Time-) Division Duplexing) : Each direction uses a different band, or same band, but at different time-instances.
- Reservation => May only be conflict in the requests. + Interesting for QoS
- Send Data with Response (SDR)
  - Client-application puts a piece of data to the layer 2 protocol, and when somebody sends an ACK-request, the data can piggyback on the ack.
- ISO: International Standard Organisation
- Session layer => Check-points. Presentation layer => Compression
- **Failure models:**
  - Sporadic failure model: Faults are always separated by a mii
  - Probabalistic failure model: Fault=> max length error frame,

CAN (Controller Area Network)

- Limited to 30 stations (In principe)
- Just the Data Link and the physical layer.
  - Twisted pair, single wire, drop is limited to 20cm.
- Synchronizes by using signal edges
  - Uses bit-stuffing: After 5 signs of the same type, an opposite is inserted.
- Logical 0 is dominant.
- Single 11 or 29 bit identifier used for each frame
  - Used to identify payload (Usually)
- CSMA with collision detection
  - If node senses the bus is different from what it put on there, it withdraws.
  - Dominant bit overwhelms the recessive one.
  - Several ways of checking errors: Ack, Frame check (structure), CRC, checking adherence to bit-stuffing. Checking for difference between the bit sent and the one received.

- Fault-confinement
    - Error active:
        - Normally takes part in the conversation.
        - Can send error active flags (6 dominant, consecutive bits)
    - Error passive
        - Takes normal part in conversation (With some restrictions)
        - Can only send error passive flags (6 consecutive recessive bits)
    - Bus off
        - Can't send or receive any frame
        - Can only exit by user command
    - Error flags will trigger from the other nodes => Last 6 – 12 bits
- Nodes filter messages according to their interest (All is broadcast)
- All messages are acknowledged (Including by those who are not interested) => Ack does not mean the intended recipient got it.
- Automatic retransmission if: Lost arbitration or disturbed by errors during transmission.

New Analysis

- Busy period length $t_m = B_m + \sum_{\forall j \in hep(m)} \left\lceil \frac{t_m + J_m}{T_j} \right\rceil C_j$
- Number of instances of message m that becomes ready for transmission before the end of the busy period

$$Q_m = \left\lceil \frac{t_m + J_m}{T_m} \right\rceil$$

- The longest time from the start of busy period to instance q (q=0 is first one) starting transmission is

$$I_m(q) = B_m + qC_m + \sum_{\forall j \in hp(m)} \left\lceil \frac{I_m + J_m + \tau_{bit}}{T_j} \right\rceil C_j$$

l-Time Networks – CAN 32

©2016 J.-D. Decotignie

-
    - This comes from the fact that messages can not be pre-empted.
- CAN is unfair
    - Lower identifier frames get priority.
    - But we can see if the network complies with the requirements if we need all the needs of the networks (

WordFIP

- For real-time traffic broadcasted in cyclic manner.
- Only variables have identifiers
- No retransmission or acknowledge for real-time traffic.
- MAC handled by unique distributor
- Response time bounded by 10 and 70 bit times.
- Periods should be multiples of some base value.
- Twisted pair or optic fibers + different speeds, etc.
    - Speed: 31 Kbps – 2.5 Mbps
    - Optical: Restricted to using point-to point and active optical stars.
- Non-real-time traffic uses client-server model.

- Ways to tell temporal validity and spatial consistency in the protocol.
- Centralized medium access control (bus arbiter)
    - 2 kinds of transfer services: Variable transfer and message transfer.
    - Several Bas can be in backup, but only one active.
- Signalling requests is done in the response to a periodic variable invitation (From the bus arbiter)
    - BA will later pool the requesting station to get the list of identifiers for the requested messages/variables
- Temporal behaviour: Central polling => Guaranteed transaction time.
    - No retransmission in case of errors. (except for messages with ack)
        - May need oversampling to handle packet-loss.
- Bounds can be derived for periodic traffic

Ethernet

- Senses cable while transmitting => Backoff if collision + (Double backoff window)
- Coax-cable or fiber + bridges(switches).
- Minimal access-delay, but not real-time
- Switch-buffers may overflow
- MAC-bridges have 8 priority levels
- Adding another MAC to get QoS has been relatively inefficient.

EtherCat

- Non-standard hardware
- Integration with CANopen (and SERCOS (?)), very fast
- Incompatible with eternet, restrictive topology
- Master sends a package. Each node relays it, but there are also fields in the dtagram where they can add inputs themselves.
- Node to node communication only via master
- Has short-circuting.

SERCOS III

- Real-time communication.
- Dedicated hardware, but compliant with 802.3u Fast Ethernet
- Ring or line topology. (Master dirves vommunication.
- Two channels:
    - Main channel => Real-time, (And there is a secondary channel)
- Uses regular IP with no encapsulation.
- A node may be connected to a regular Ethernet network
- Guaranteed cycle time.

Other Ethernet-implementations

- Ethernet IP with time synchronisation
    - Can be mixed with "Pure" Etehernet
    - Only statistical guarantees+Cycle time is not constant+ jitter is uncontrolled.
- Ethernet Powerlink
    - Synchronous part is made of slots.
    - Compliant with CANopen

    - (This one seems kind of disastrous; Model does not accunt for errors, sensitive to timing errors, low effichiency, special hardware, incompatible with ethernet)
- Real-time Ethernet
    - Number of nodes only limited by physical considerations
    - Compliant with 802.3 (All variants) (+ On normal hardware)
    - Cycle-time in multiples of milliseconds.
    - Only client-server and single polling cycle + configuration must be centralized.
    - Difficult to calculate guarantees
- Apparently switched ethernet can be sufficient for RT if priorities in swithes are being used (?), but bad in therms of topology
    - And suffers in terms of delay variations.
    - Traffic smoothing

Wireless

- Radio coverage is not circular, and signal strength is loosely related to distance.
- 3 catoegories of links
    - Connected, Transitional, disconnected.
        - Transitional=> Unrelieable and asymmetric, even for static nodes.
- Other sources to packet errors that collision => Often not good to retry right away.
- Packet transmission => Sender & receiver must be synchronised.
    - => Packet overhead (Varies with sender interval)
- Forward error correction can be used to lower apparent FER (Frame Error Rate)
- Several layers can play a role in QoS
- Fading: The signal becomes worse because of positioning and some other factors:
    - Multipath propagation
    - Shadowing from obstacles
    - Attenuation

Bluetooth

- Max 1 master 7 slaves
- Frequency hopping spread spectrum: hoping sequence based on master identity and clock phase
- TDD: Time Division Duplexing
    - Each 625 μs slot is used alternatively by a master and a slave (Frequency hop at each new slot)
- Access code, Header, Data
    - Intra and inter piconet scheduling is not specified. Local inside the node is FIFO (probably)
- Reduced traffic
    - Slave needs to listen only at T_{sniff} intervals, for $N_{sniff\_attempts}$ slots.
        - Each time a packet is received the time may be extended.
- Parked mode: may be unparked by master beacon, or by slave in the access window after beacon. (almost no limit to number of parked nodes)
- Suports synchronous traffic. (Asynchronous is interleaved)
- Piconet: Group of max 8 participants

- Scatternet: set of piconets in the same geographical area (a node may participate in more than one piconet)
- Link manager:
  - LM data has higher priority than user data (max response time 30 seconds)
  - LM does setup, control and security of links.
    - Authentication
- **Cons: No real-time** capacity for data, point to multipoint, short distance, limited capacity (#devices & throughput), 10.24 s connection time.
- **Pros:** Low interference, power management is possible, device discovery protocol, no planning, low cost authentication and encryption.
- **QoS**
  - On ACL (Asynchronous Connection-Less) links:
    - Token bucket algorithm
      - Mean throughput with some peaks
    - Only lower priority that eSCO
    - May be subject to admission control
      - A check before a connection is made to see if the current resources are sufficient for the proposed connection.
    -
  - On SCO (Synchronous Connection-oriented) links:
    - Constant bit rate
    - Error correction may be done by using retransmission
    - Only one link per slave

Bluetooth extensions

- Versions:
  - 1.2 : QoS + better flow management
  - 2.0: 3Mbps
  - 3.0: Suport for high speed alternate physical layer
  - 4.0: Low energy version (BLE, BT Smart)
  - 5.0: Long range, high duty cycle, BLE mesh.
- BLE:
  - No carrier sense before transmission
  - Fast interactions with channel diversity and random waits.
  - No temporal guarantees
- BLE 4.2 (BT Smart)
  - **Pros**: Good coexistence, fast advertisement, security, can be implemented on resource limited devices.
  - **Cons:** No RT-guarantee, limited throughput (<= ~80-90Kbps)
- Bluetooth 5
  - Long range, 2Mbps
  - Lower duty-cycle, connection-less broadcasting.
  - Bluetooth mesh (2017)
    - Mesh networking based on publish-subscribe

IEEE 802.11 (Wireless LANs)

- Only layer 1 and Mac
- 2 operating modes (3 in total)

  - Ad hoc network or DCF (Distributed Communication Function)
  - Coordinated by a single access station per cell (Point Coordination Function (PCF))
- CSMA/CA + connection-less period (PCF)
- A large family with
- Each frame contains time needed to transmit remaining traffic
  - Used to update the Network Allocation Vector (NAV)
- Transmission of long frames =>
  - Segmentation to avoid long retransmission.
  - Whole frame is transmitted without other transmissions (blocking time)
    - But collisions can't be detected => Avoid sending long frames.
- Point Coordinator Function (PCF)
  - Connection-oriented, but supports connection-less.
  - The access point AP takes on the role of "Point coordinator"
  - Transfer according to polling list. AP(beacon) ->all, AP(poll)->STA, STA(ack, data)->AP
    - Possible with station to station transfer (the ack is not addressed to AP, but to another station)
  - QoS limitations (throughput, delay, jitter)
    - DCF: Best effort, no traffic differentiation
    - PCF:
      - Centralized traffic
      - Strong requirements on response time (SIFS ~$10\mu s$
- A number of possibilities for QoS. Room left for improvement

EDCA

- Extended DCF Access (EDCA)
- Provides QoS support in ad hoc mode without an access point
- Trafic discrimination based on
  - Time STA senses channel before transmit or backoff
  - Length of contention window.
  - How long a channel can transmit if it got the channel
- Can have admission control
- Can't use the channel more than a given limit TXOP
- Has block acknowledgement
  - Up to 64 dataframes in a row can be sendt without ack.
- Direct link protocol
  - From QSTA to QSTA. Setup goes through QAP

Wireless sensor networks (IoT)

- Some characteristics of radio transmission
  - Can't be powered over transmission line
  - Longer turn and switching times
  - The normal stuff
- Light transmission
  - Sensitive to heat, requires line of sight, Health concerns
- Both suffer from interferences, security, limited ability to detect collisions, and lower distances.
- Error recovert:
  - Forward error correction codes are used to lower apparent FER

- Expected Features of WSNs
    - Self-organized, no infra-structure, battery operated (low energy), multihop transmission, small and low cost, low data rate, large number of nodes, sensor information needs temporal consistency,
- Reliability => Multiple paths, no single point of failure, node redundancy
- There are several topologies
    - Multi-hop to sink
    - Infrastructure: All nodes are connected to an AP (of several), that is on a bus to sink
    - Hybrid: (Mix of the two)
- There is not a guarantee that if a node can receive from somebody, that they will be able to send to them
- The world is not flat.
- MAC must take multihop into consideration for WSANs
- Sources of energy waste in MAC
    - Idle listening
    - Overhearing: Can become important in dense ad hoc networks. Limits scalability in infrastructure sensor networks.
    - Collisions: Retransmissions cost energy
    - Over emitting: Sending when nobody is listening
    - Protocol Overhead: There must be a frame header and signalling to implement MAC
- S-MAC:
    - Nodes have a listen/sleep periodic schedule
    - CSMA/CA protocol with RTS/CTS to avoid collisions
    - A starting node listens for a neighbour schedule; If it finds one, it adopts it, if not it selects one randomly. If it hears two schedules, it will adopt both
    - No guarantees.
    - Power consumption not linked to traffic, but to duty cycle.
    - Mitigates overearing, collisions and idle listening.
- TMAC:
    - Same as SMAC, but a node goes back to sleep as soon as there is no traffic.

802.14.4 (Improperly called ZigBee)

- Lower layer of many solutions (ZigBee, WirelessHART)
- MAC: CSMA/CA + Contention-less period
- 2 operationg modes (Peer-to-peer and star)
    - Station to station without coordination (ad hoc network or DCF)
    - Coordinated by a single base station per cell
- Duty cycle
- Power save mode: Nodes go to sleep as soon as there is no traffic for a given time.
- Trafic indicator map: Coordinator indicates downlink traffic in beacon. Nodes may wake up according to what they feel like.
- Star with beacon can give guarantees with Guaranteed Time Slots (GTS)
- Peer-to-peer has no guarantees and rather high idle listening.
- Multihop with beacons uses a lot of energy for relaying nodes.
- The TDMA requires tight time-synchronisation
    - & Slot time must accommodate for longest packet.
    - LMAC can guarantee RT if no errors.

- Each node owns a slot in a frame and must transmit in it (payload + control data). All nodes must listen for the control data of all neighbours. The gateway starts the network.

Others

- WiseMAC (Wireless Sensor MAC)
  - Multi-hop, low average data rate, and high latencies re tolerated, but power consumption should be low.
  - A wakeup-radio and a main radio.
  - Wake-up preamble minimized by exploiting knowledge of sampling schedule of direct neighbours.
  - Samples every T_w => tradeoff between delay and energy consumption
  - Minimum preamble length: If L seconds between communications, and the clocks drift Θ per second. $T_p = \min(4L\Theta, T_w)$
    - T_w: Time between samples.
  - Sampling schedule information is inserted in every ack
  - Medium reservation <= Avoid collisions when using short preambles.
  - ∃ "More"-bit in header to be able to transmit in bursts.
  - Data frame repeated in preamble if the preamble is large.
    - Reduce FER, mitigate overhearing
  - Receive-thresholds for wake-up <= Not wake up due to noise.
  - Carrier sense range larger than interference range <= Reduce hidden node problem at cost of capacity.
  - ∃ Medium reservation preamble.
  - WiseMAC is single channel
  - RTS/CTS requires broadcast communication => Long preamble
  - Adaptive to traffic=> For energy efficiency
  - The radio has a switch or setup-state before it can enter Rx, Tx
  - Suports sporadic, periodic and burst-y traffic.
- BMAC
  - Same as ALOHA with preamble sampling.
  - Supposed to be generic MAC where you can change parameters on upper layers
- SCP-MAC
  - Periodic preamble sampling
  - Neighbours are synchronized (Like SMAC)
  - Collision mitigation and adaption to traffic (optimized for multihop)

Low-Power Listening (LP)

- Radios make preambles by repeating packets (They can't do it "properly"(?))
- In case of noisy environments, one can adjust the level for wakeup, or change the preamble to something that doesn't occur as often (as in WiseMAC)
- Broadcasts are not acknowledged
- Broadcast can't have any timing info => Long preamble.
  - This overhead can be reduced by sending the packet "back-to-back" with the "more bit" (?)

Pure TDMA

- Good from safety point of view, but does not scale, is not flexible and hardly supports fluctuating links.
- Energy efficient and good on high loads
- Adaptable case: Nodes only have to send a synchronisation message every K rounds
- All nodes send and receive 1 message every L rounds
- Asynchronous protocols can avoid collisions by supressing arbitration in some cases (“More bit”)
- Margin is needed between slots for desync, for retries and to accommodate for the longest packets.
- Asynchronous methds get the same results, but without the synchronisation job.

More stuff

- Infrstructure-mode:
    - Several star topologies. Center is unconstrained by energy.
    - WiseMAC still works (Also PTIP and PSM)
    - PSM: Sensors wake up regularly to receive traffic indication map
    - WiseMAC:
        - Sensor nodes sense the network to detect preamble
        - AP learns the sampling schedule of the sensor nodes (through ACK-messages) & send messages at the right time mith minimized preamble.
    - PTIP: Sensor nodes periodically poll the AP to check for potential data packets.
        - If high latency is OK, this is energy-efficient.
    - In Wireless Sensor Networks (WNS), communication is often the largest source of consumption.
        - Might be useful to switch between protocols depending on traffic.
    - Routing has a large effect on consumption in WSN

Industrial Wireless networks

- Time-Synchronized Channel Hopping (TSCH)
    - Fixed duration time-slots long enough to send packet and get ack.
    - No superframe, no regular beacon, general topology.
    - LLDN: Low Latency Deterministic Networks (Star topology with single coordinator.
        - Send beacon on fist slot of superframe. All others are assigned to nodes.
        - No akc in slot, but in next beacon.
    - DSME: Deterministic and Synchronous Multi-channel Extension
        - Multi-channel, multi-superframe, mesh extension to GTS
        - Group ack,
        - 2 cannel diversity modes (channel adaption & channel hopping)
        - 16 slots in superframe. Slots can be reserved for group acks

Wireless HART

- Full solution (Not just MAC)
- Security manager, Network manager (Possible with redundancy), gateways (access-points)

- 802.15.4 physical layer and PDUs
- TDMA MAC; entirely configured by network manager
- Mesh with route redundancy+ all field devices are possible routers
- Prioritized traffic is possible
- TDMA: One or more superframes of a fixed number of slots.
- Channel hopping at each slot.
- Timetables:
    - For per
- There is a counter for slot number since startup
- There may be several nodes in one slot if they are in different superframes. Transmit has priority over receive.
    - Shared slots are handled with CSMA/CA
- Timetables:
    - For periodic:
        - Specifies transger period on a connection
        - End-to end latency assumed not to exceed 1/3 of period
    - For sporadic: Specifies max end-to-end latency.
- If a node receives from two slots at the same time, it selects the one with the lowest ID.
- All superframes start at time 0 + N*T   (T = Period)
- A data transfer has 1 slot +1 slot for retry + 1 for retry on another path for 2^{nd} retry
- There is a management superframe (6400 slots)
    - Keep_alive, join requests/responses, ad hoc requests,
- Addressing: Source+dest
- No encryption, but there is authentication.
- QoS: Priorities (Command, process data, Normal, alarm), timeout.
- Network layer => end-to-end security.
- 4 types of routing: graph (relay knows next hop), source (

“Words of wisdom”

- Traffic is rarely constant=> Fixed assignment is often overkill.
- The industry does not like probabilistic approaches
    - Certification

TODO

- Actually learn 802.11 (And what RT-requirements it can fulfil)