

PA197 Secure Network Design

1. Introduction

Eva Hladká, Luděk Matyska

Faculty of Informatics

16. 2. 2022

Content

- 1 Course Introduction
 - Course Organization
- 2 Course Goal
- 3 Basic network architectures and functions
 - data transmission
 - end to end argument
 - routing
 - switching
- 4 General requirements on the security and reliability
 - implication towards the architecture design
 - ISO/OSI vs. TCP/IP Model
- 5 Redundancy principle
- 6 Wireless ad-hoc/sensor networks

Course Organization

- Structure: 2/2/2 credits
 - f2f lecture every Wednesday, 10-12 am (but also see later)
 - 3 Games: Adaptive Game, short CTF, long CTF

Rules of engagement – Lectures

- Lectures are pre-recorded and made available in IS MU a week before the real-time session
 - With the exception of this first one
- Scheduled time will be used as an interactive seminar
 - F2f unless forbidden
 - Your questions
 - More detailed discussion around selected topics
 - Questions through Sli.do
 - Examination questions/subjects
- Examination will be in an **Open Book** format
 - IS MU
 - The first (mandatory) examination on 18th May at 10 AM (we may discuss a different timing in that day/week)
 - Other terms as needed (for those who can't make it for serious reason)

Rules of engagement – Games and points

- Adaptive cybersecurity game, home assignment (up to 5 points) – April
- Short Capture the Flag (CTF), 2 hours (up to 10 points) – May
- Long CTF, 10 hours of a cyber game plus report to be provided afterwards (up to 20 points) – May or later
- Examination (65 points) – 18th May
- **Total of 100 points** (65 Exam, 35 Games)
- Attendance at all games is mandatory (you can't pass otherwise)
- To pass you need at least **65 points**
 - The actual grading will be defined after the examination (to collect sufficient statistically relevant data)

Resources

- Slides and recordings are available in IS
 - Also the recordings from the interactive sessions will be made available
- Recommended literature
 - Some papers and RFCs are referenced directly in the slides
 - Graig Hunt: TCP Network Administration. O'Reilly Media, Third Edition, 2002. ISBN-10: 059600297
 - Lee Allen: Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Packt Publishing Ltd. 2016. ISBN13 (EAN): 9781784395810
 - Holger Karl, Andreas Willig: Protocols and Architectures for Wireless Sensor Networks. Wiley-Interscience. 2007. ISBN-10: 0470519231

Course Goal

- To present basic network architectures and functions
 - data transmission
 - end to end argument
 - routing
 - switching
 - ...
- General requirements on the security and reliability
 - implication towards the architecture design
- Network architectures from the security point of view
 - reliable design also in
 - ad-hoc/sensor networks

Basic network architecture and functions

- Data transmission
- End to end argument
- Routing
- Switching

Data Transmissions—Introduction

- **The main goal:** to ensure a transmission of bits (= the content of passed frames) between sender and receiver
- Several standards (RS-232-C, CCITT V.24, CCITT X.21, *IEEE 802.x*) defining electrical, mechanical, functional, and procedural characteristics of interfaces used for connecting various transmission media and devices, e.g.:
 - parameters of the transmitted signals, their meaning and timing
 - mutual relationships of control and state signals
 - connectors' wiring
 - and many many others

Services - Data Transmissions

- *Bit-to-Signal Transformation*
 - representing the bits by a signal – electromagnetic energy that can propagate through medium
- *Bit-Rate Control*
 - the number of bits sent per second
- *Bit Synchronization*
 - the timing of the bit transfer (synchronization of the bits by providing clocking mechanisms that control both sender and receiver)
- *Multiplexing*
 - the process of dividing a link (physical medium) into logical channels for better efficiency
- *Circuit Switching*
 - circuit switching is usually a function of the physical layer
 - (packet switching is an issue of the data link layer)

Signals

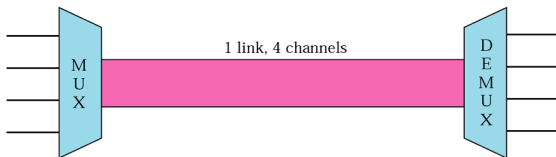
- Data are transferred (via transmission media) in the form of (electromagnetic) *signals*
 - the data have to be converted into the signals
- *Signal* = a function of time representing changes of physical (electromagnetic) characteristics of the transmission media
- Data that have to be transferred (0s and 1s) – *digital* (binary)
- Signals spread through the transmission media – *analog* or *digital*
 - some media suitable for both analog and digital transmission – wired media (coaxial cable, twisted pair), optical fibre
 - some media suitable just for analog transmission – ether (air)

Transmission Media

- Provides an environment for the functionality of physical layer
- Basic distinction:
 - *guided (wired) media*
 - provide a conduit from one device to another
 - twisted pair (LANs, up to 10 Gbps), coaxial cable, optical fibre (backbones, hundreds of Gbps), etc.
 - *unguided (wire-less) media*
 - transfer an electromagnetic wave without the use of physical conductor
 - the signals are broadcasted (spread) via ether (air, vacuum, water, etc.)
 - radio signals, microwave signals, infrared signals, etc.

Multiplexing

- *Multiplexing* – a technique of sharing an available bandwidth by concurrent communication channels
 - the goal is to maximize the utilization of the media
 - applied especially for optical fibres and non-wired media



- For analog signals:
 - *Frequency-Division Multiplexing (FDM)*
 - *Wave-Division Multiplexing (WDM)*
- For digital signals:
 - *Time-Division Multiplexing (TDM)*

End to End (E2E) argument

How to provide demanded functionality in computer networks?

- **End-to-End (E2E) argument**
 - application demanded functionality is possible to provide with knowledge and by application
 - \Rightarrow if it is possible, communication protocol operations have to be defined by realization only in communication system end nodes or in the closest distance
 - in lower system levels protocol function should be implemented only if performance increases.
 - suitable for applications demanding higher degree fidelity transported data and some latency is tolerated.
- **Hop-by-Hop (HbH)**
 - repeating specific functionality on the each two-point connection is possible to obtain increasing performance
 - it requires storing state information on inside network nodes \Rightarrow limited scalability
 - useful for applications, where minimal latency is more important than transported data fidelity (e.g. real-time applications)

Routing

- The main goal of routing is:
 - to find optimal paths
 - the optimality criterion is a *metric* – a cost assigned for passing through a network
 - to deliver a data packet to its receiver
- The routing *usually* does not deal with the whole packet path
 - the router deals with just a single step – to whom should the particular packet be forwarded
 - somebody “closer” to the recipient
 - so-called *hop-by-hop* principle
 - the next router then decides, what to further do with the received packet

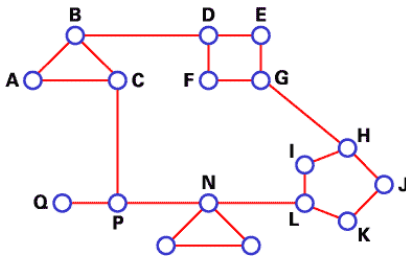
Routing – basic approaches

The basic approaches distinguished by the routing table creation/maintenance:

- *static (non-adaptive)*
 - manually (by hand) edited records
 - suitable for a static topology and smaller networks
- *dynamic (adaptive)* – these respond to network changes
 - complex (usually distributed) algorithms
 - e.g.:
 - *centralized* – a centre controls the whole routing
 - *isolated* – every node on its own
 - *distributed* – nodes' cooperation

Routing – mathematical view

- The routing can be seen as a problem of graph theory
- A network can be represented by a graph, where:
 - nodes represent routers (identified by their IP addresses)
 - edges represent routers' interconnection (a data link)
 - edges' value = the communication cost
 - *the goal*: to find paths having minimal costs between any two nodes in the network



Routing – routing algorithms' required features

Required features of any routing algorithm:

- accuracy
- simplicity
- effectiveness and scalability
 - to minimize an amount of control information ($\approx 5\%$ of the whole traffic!)
 - to minimize routing tables' sizes
- robustness and stability
 - a distributed algorithm is necessary—network composition and topology changes in time!
- fairness
- optimality
 - *“What should be treated as the best path?”*

Routing – basic approaches to distributed routing

Basic approaches to distributed routing:

- *Distance Vector (DV)* – Bellman-Ford algorithm
 - *info about the whole network to my neighbors only*
- *Link State (LS)*
 - *info about my neighbors to the whole network*

Routing – Distance Vector

- Bellman-Ford algorithm
 - the neighboring routers periodically (or when the topology changes) exchange complete copies of their routing tables
 - based on the content of received updates, a router updates its information and increments its *distance vector number*
 - a metric indicating the number of hops in the network
 - i.e., “*all pieces of information about the network just to my neighbors*”

Routing – Link State

- The routers periodically exchange information about states of the links, to which they are directly connected
- They maintain complete information about the network topology – every router is aware of all the other routers in the network
- Once acquired, the Dijkstra algorithm is used for shortest paths computation
- I.e., *“information about just my neighbors to everyone”*

Packet Switching

- Packet switching refers to protocols in which messages are divided into packets before sending and each packet is transmitted individually. Once all packets forming a message arrive at the destination, they are recombined into the original message.
- Packet switching operation
 - data are transmitted in short packets, typically an upper bound on packet size is 1000 bytes.
 - each packet contains part of the user's data and some control information.
 - the control information should at least contain
 - destination address
 - source address
 - store and forward – packets are received, stored briefly and sent to the next node.

Packet Switching – Advantages

- Line efficiency – single node to node link can be shared by many packets over time and packets queued and transmitted as fast as possible
- Data rate conversion – each station connects to the local node at its own speed
- Packets are accepted even when network is busy
- Priorities can be used

Switching Technique

- Virtual Circuits
 - pre-planned route is established before any packets sent
 - call setup before the exchange (handshake)
 - all packets follow the same route and arrive in sequence
 - each packet contains a virtual circuit identifier instead of destination address
 - no routing decision required for each packet
 - clear request to drop circuit
- Datagrams
 - each packet is treated independently with no reference to packets that have gone before.
 - packets may arrive out of order
 - packets may go missing
 - up to receiver to re-order and recover from missing packets
 - more processing time per packet node
 - robust in the face of link or node failures

Circuit vs. Packet Switching

- Performance
 - propagation delay
 - transmission time
 - node delay
- Packet switching evolution
 - X.25 packet-switched network
 - router-based networking
 - switching vs. routing
 - frame relay network
 - ATM network

Switching vs Routing

- Switching

- path set up at connection time
- simple table look up
- table maintenance via signaling
- no out of sequence delivery
- lost path may lost connection
- much faster than pure routing
- link decision made ahead of time, resources allocated then

- Routing

- can work as connectionless
- complex routing algorithm
- table maintenance via protocol
- out of sequence delivery likely
- robust: no connections lost
- significant processing delay
- output link decision based on packet header (at every node)

General requirements on the security and reliability

- Dual network basis
- Communication protocols
- ISO/OSI and TCP/IP models

Dual network basis

- Physical and software base
- Physical base: links and physical equipment
 - not a primary subject of this lecture
- Software base: protocols and applications
 - subject of this lecture

Network (Communication) Protocols I.

- Motivated by the need to communicate among several entities (at least two)
 - *entity* = anything capable of sending or receiving information
- The form/method of the communication must be known to all the participating entities
 - they have to **agree on a protocol**

Network (Communication) Protocols II.

- The **protocol** defines “*What*” the subject of communication is, “*How*” the communication has to behave and “*When*” does it behave
- They define:
 - *syntax* = structure/format of data (the order in which they are presented)
 - *semantics* = refers to the meaning of each section of bits (how should a particular pattern to be interpreted)
 - *timing* = when data should be sent and how fast they can be sent
- Examples of network protocols:
 - UDP, TCP, IP, IPv6, SSL, TLS, SNMP, HTTP, FTP, SSH, Aloha, CSMA/CD, . . .

Network Protocol

- **Network Protocol** is a set of rules that define
 - the format of the messages exchanged among two or more communication entities
 - the order of such messages
 - the actions performed during sending/receiving that messages

Standardization

- Definition of norms/standards describing various actions, activities, forms/methods of communication, etc. (not only in IT)
- Main goals:
 - quality
 - security
 - compatibility
 - interoperability
 - portability
- Standards fall into two categories:
 - *de facto* – standards that have not been approved by an organized body but have been adopted as standards through widespread use (they are often established originally by manufacturers)
 - *de iure* – standards legislated by an officially recognized body

Standardization organizations in IT

- ISO, ITU-T, ANSI, IEEE, IETF (*RFCs*), IEC, etc.

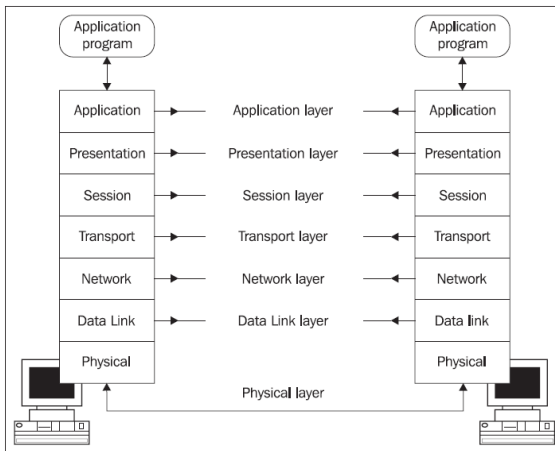
ISO/OSI Model I

- **7-layer model** proposed by OSI to ensure compatibility and interoperability of communication systems developed by various vendors
- The purpose of layered architecture:
 - each layer is **responsible for particular functionality**
 - it adds some control information to the data in order to do its job
 - each layer **communicates just with its neighbours**
 - each layer uses the services provided by the lower layer and provides its services to the higher layer
 - the functionality is **isolated** in the particular layer (once a layer changes, just the neighbouring layers have to adapt to such a change)

ISO/OSI Model II

- “Logical” communication
 - between the peer layers on the communicating entities
- Physical communication
 - the data must pass through all the lower layers
- The layers are just an abstraction – the real implementations are more or less different
- 7 layers not really accepted/implemented \Rightarrow TCP/IP model

ISO/OSI Model vs. TCP/IP Model



L1 – Physical Layer

Introduction I.

- Provides the functionality for an interaction with transmission media
- Provides services for the *Data Link Layer*
 - the Data Link Layer passes/obtains data to/from the Physical Layer in the form of 0s and 1s organized into *frames*
 - the Physical Layer transforms the streams of bits (from frames) into *signals* spread through the transmission media
- Controls the transmission media; for example, decides about:
 - sending/receiving the data (signals)
 - data transformation (coding) into signals
 - the number of logical channels simultaneously transferring data from various sources

L1 – Physical Layer

Services

- *Bit-to-Signal Transformation*
 - representing the bits by a signal – electromagnetic energy that can propagate through medium
- *Bit-Rate Control*
 - the number of bits sent per second
- *Bit Synchronization*
 - the timing of the bit transfer (synchronization of the bits by providing clocking mechanisms that control both sender and receiver)
- *Multiplexing*
 - the process of dividing a link (physical medium) into logical channels for better efficiency
- *Circuit Switching*
 - circuit switching is usually a function of the physical layer
 - (packet switching is an issue of the data link layer)

L1 – Physical Layer

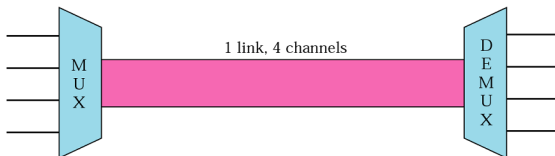
Signals

- Data is transferred (via transmission media) in the form of (electromagnetic) *signals*
 - the data have to be converted into the signals
- *Signal* = a function of time representing changes of physical (electromagnetic) characteristics of the transmission media
- Data that have to be transferred (0s and 1s) – *digital* (binary)
- Signals spread through the transmission media – *analog* or *digital*
 - some media suitable for both analog and digital transmission – wired media (coaxial cable, twisted pair), optical fibre
 - some media suitable just for analog transmission – ether (air)

L1 – Physical Layer

Multiplexing

- *Multiplexing* – a technique of sharing an available bandwidth by concurrent communication channels
 - the goal is to maximize the utilization of the media
 - applied especially for optical fibres and non-wired media



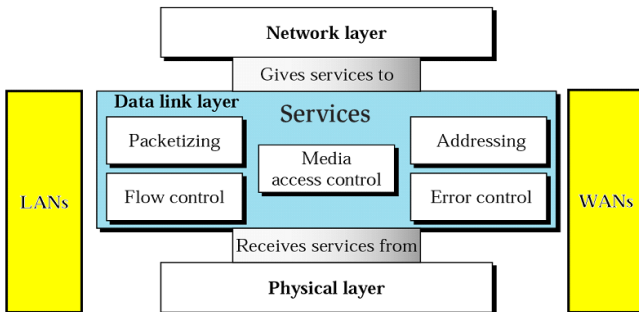
- For analog signals:
 - *Frequency-Division Multiplexing (FDM)*
 - *Wave-Division Multiplexing (WDM)*
- For digital signals:

L2 – Data Link Layer

Introduction

- Receives **packets** (being passed from the Network Layer) and transforms them into **frames**
- In cooperation with the Physical layer ensures the transmission of frames between communicating devices interconnected with a (*shared*) *transmission media*
 - i.e., just the local (inside a segment) delivery (LAN)
- Ensures the transmission reliability between these devices
- Ensures the flow control in order to avoid receiver congestion
- Controls the access of the devices to shared media (Medium Access Control)

L2 – Data Link Layer



L2 – Data Link Layer

properties

- *Framing*
 - the incoming packets (being passed from the Network Layer) are encapsulated into *frames*
- *Addressing*
 - provides the addresses of physical layer entities – *physical/MAC addresses*
 - frames contain source and destination addresses of communicating entities

L2 – Data Link Layer

control

- *Error Control*
 - it's not possible to eliminate the errors occurring on the physical layer
 - L2 layer ensures the required level of reliability of the data link (error detection and correction)
- *Flow Control*
 - prevents the receiver congestion
 - *stop-and-wait* mechanism, *sliding-window* mechanism, ...
- *Medium Access Control – MAC*
 - necessary in environments, where the transmission media is shared by several entities
 - eliminates or mitigates collisions caused by multiple (concurrent) transmissions

L2 – Data Link Layer

Error Control

- A concept of redundancy is used
 - sender adds bits whose value is a function of transmitted data
 - receiver calculates the same function and if the values differ, it detects (tries to repair) an error
 - when using error detection only (or if the error is non-repairable), the receiver may request the sender to repeat the transmission
- *Error Detection, Automatic Request for Retransmission (ARQ)*
 - error detection and transmission repetition guarantee
 - suitable for little-lossy transmission media
 - even/odd parity, *Cyclic Redundancy Check (CRC)*, etc.

L2 – Data Link Layer

Error Control

- *Forward Error Correction (FEC)*
 - error detection and attempts to data correction (using redundant data)
 - suitable for lossy transmission media (especially with high transmission latency)
 - e.g., *Hamming code*
 - for details see *PV169: Communication Systems Basics*

L2 – Data Link Layer

Medium Access Control (MAC)

- The functionality responsible for coordination of multiple devices' access to shared transmission media
- *The goal:* the elimination of collisions caused by concurrent transmissions (emissions)
 - i.e., concurrent transmissions to a shared transmission environment
- Medium access protocols:
 - *random-access protocols* – Aloha, CSMA/CD, CSMA/CA
 - *controlled-access protocols* – based on reservations, polling, tokens, etc.
 - *channelization protocols (multiplex-oriented access)* – FDMA, TDMA, etc.

L3 – Network Layer

Introduction

- Provides services for the *Transport Layer*:
 - receives *segments* from the Transport Layer and transforms them into *packets*
 - in cooperation with the Data Link Layer ensures the packets' transmission between communicating nodes (*even between different LANs*)
- Logically joins independent LAN networks
 - the upper layers are provided with an illusion of just a single wide-area network (*WAN*)
- Allows unique identification (addressing) of every host/device on the Internet
- Ensures *routing* of passing packets
- In cooperation with the Data Link Layer associates the L3-addresses with the L2/MAC-addresses (and vice versa)

L3 – Network Layer

Services I

- *Internetworking*
 - logical gluing of heterogeneous physical networks together to look like a single network (from the upper layers' point of view)
 - by such an interconnection, an *internetwork* (shortly *Internet*) is created
 - an illusion of a uniform environment provided by a single wide-area network

L3 – Network Layer

Services II

- *Packetizing*
 - segments (payload) are transformed into packets
- *Fragmentation*
 - a technique to solve the problem of heterogeneous MTUs – when a packet is larger than the MTU of the network over which it must be sent, it is divided into smaller fragments which are each sent separately
- *Addressing*
 - the entity addresses used on the network layer – so-called *IP addresses*, unique throughout the whole network
 - packets contain source and destination addresses of communicating entities

L3 – Network Layer

Services III

- *Address Resolution*
 - ARP, RARP protocols
- *Routing*
 - the process of selecting paths in a network along which to send network traffic from a source to a particular destination
- *Control Messaging*
 - providing basic information about unavailability to deliver a packet, about a network/host state, etc. – ICMP protocol

L4 – Transport Layer

Introduction

- Provides its services to the *Application Layer*:
 - obtains data coming from sending application and transforms them into *segments*
 - delivers received segments to the destination application
- In cooperation with the network layer ensures data (segments) delivery between communicating *applications/processes*
 - providing transmission reliability, if required
 - provides them with a logical communication channel
 - an illusion of direct physical interconnection
 - so-called *process-to-process delivery*
- The lowest layer providing so-called *end-to-end* services
 - the headers generated on the sender's side are interpreted “only” on the receiver's side
 - the transport layer data are seen by routers as a payload of transmitted packets

L4 – Transport Layer

Services

- *Packetizing*
 - the data provided by an application are transformed into packets (having a transport header added)
- *Connection Control*
 - *connection-oriented* and *connectionless* services
- *Addressing*
 - the addresses of transport layer entities (= network applications/services) – so-called *ports*
 - the packets contain source and destination ports (an identification of source and destination application)
 - an application is uniquely identified in the network by the pair *IP_address:port*

L4 – Transport Layer

Service II

- *Connection Reliability*
 - *Flow Control and Error Control*
 - provided on the node-to-node principle by lower layers, L4 provides it on the *end-to-end* principle
 - ensures a reliability over *best-effort* service (IP)
- *Congestion Control and Quality of Service (QoS) guarantee*

L7 – Application Layer

Introduction I

- Provides services to *users*:
 - application programs specific for a particular purpose
 - e.g., electronic mail, WWW, DNS, etc. etc.
 - applications = the main reason for computer networks existence

L7 – Application Layer

Introduction II

- Comprises of *network applications/programs* and *application protocols*
 - application protocols (HTTP, SMTP, etc.) are **parts of** network applications (web, email)
 - they are not applications on their own
 - the protocols define a form of communication between communicating applications
 - application protocols define:
 - types of messages, which the applications exchange (*request/response*)
 - messages' syntax
 - messages' semantics (a semantics of particular fields)
 - rules, when and how the messages are exchanged

Redundancy principle in network design

- Basic principle in Nature
 - duplication important viscus in animal's bodies – e.g. kidneys
- Basic principle in networks
 - topology (see topology of CESNET2 network)
 - parts of protocols (CRC on several layers)

Wireless Ad-hoc Networks

Wireless Ad-hoc Network

- A collection of autonomous nodes that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner
 - each node functions as both a *host* and a *router*
 - the control of the network is distributed among the nodes
 - the network topology is (in general) dynamic
 - the connectivity among the nodes may vary in time due to node departures, new node arrivals, and the nodes' mobility
 - \Rightarrow a need for efficient routing protocols that allow the nodes to communicate over multihop paths in an efficient way
- These networks pose many complex issues \Rightarrow there are many open problems for research
 - without a central infrastructure, things become much more difficult

Wireless Ad-hoc Networks

Advantages

- Very fast construction
 - no need to establish wired connections
- Resilient
 - no single point of failure, such as a base station
- Spectrally more efficient than cellular networks
 - every node can communicate with any other node (sometimes even simultaneously), so nodes can make better use of the channel

Wireless Ad-hoc Networks

Problems/Challenges

- Problems arise due to:
 - lack of a central entity for network organization
 - the participating nodes must organize themselves into a network
 - *self-organization* is a must
 - limited range of wireless communication
 - data have to be delivered over a path involving multiple nodes
 - \Rightarrow mechanisms for dynamic path identification and management are required
 - mobility of participants
 - the network nodes may be allowed to move in time and space
 - the network quality depends on the speed to adapt to new topologies
 - \Rightarrow **Mobile Ad-hoc Networks (MANETs)**

Wireless Ad-hoc Networks

Issues

- Among others, the following issues have to be addressed:
 - *medium access control* – no base station can assign transmission resources (it must be decided in a distributed fashion)
 - *routing* – finding a route from one participant to another

Wireless Sensor Networks

Importance of an Energy-efficient Operation

- Often (but not always), the participants in an ad-hoc network (not only sensor network) draw energy from batteries
- It is desirable to sustain a long run time for:
 - individual nodes/devices
 - the network as a whole
 - usually, application demands do not bother with individual nodes, as long as the global application-dependent objective can still be fulfilled
- Employed networking protocols have to take the limited energy into account and behave in an energy-efficient way
 - e.g., use routes with low energy consumption (energy/bit)
 - e.g., take available battery capacity of devices into account
 - How to resolve conflicts between different optimizations?
- Some form of recharging or energy scavenging from the environment is often used to increase the available energy

Wireless Sensor Networks

Required functionality and constraints

- *Available energy*
 - sensor nodes are operated by batteries that provide limited energy for the node
- *Processing power*
 - employed micro controllers usually provide very limited processing performance (due to size and energy restrictions)
- *Memory and storage*
 - the characteristics of the available memory usually correlate with the size of the micro controller
- *Bandwidth and throughput*
 - wireless radio transceivers are optimized for low-energy operation \Rightarrow they provide a relatively small bandwidth to the application

Wireless Sensor Networks

Required functionality and constraints II

- *Reliability*
 - depending on the application scenario, the demands for the reliability (both communication reliability and error-proneness of the hardware) can strongly differ
- *Addressing*
 - typically, off-the-shelf sensor nodes do not have a globally unique address pre-programmed \Rightarrow networking mechanisms must either dynamically allocate unique addresses or even abandon address-based techniques
- *Scalability*
 - a primary constraint – the scalability of employed methods and algorithms

Recapitulation

- *Course organization*
- *Course overview*
 - basic network functions
 - data transmission, E2E argument, routing and switching
 - general requirements on the security and reliability
 - implications towards the architecture design, ISO/OSI and TCP/IP models
 - reliable design of selected networks
 - sensor, mobile