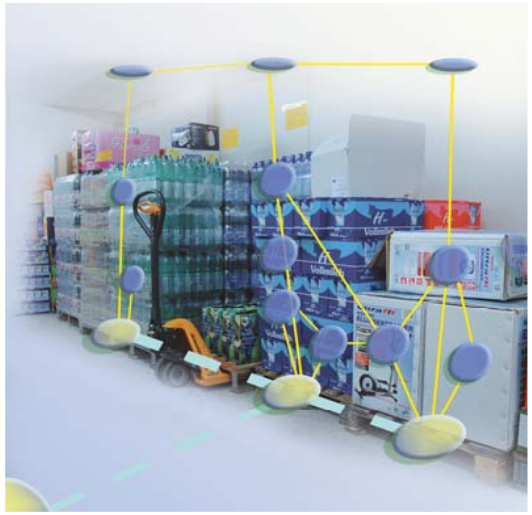


Wireless Sensor Networks: Applications, Architectures and Protocols

German contribution to first face to face meeting of the JTC1 Study Group on Sensor Networks,
Shanghai, 25. – 27. June 2008

Prepared and presented by Dr. Alexander Pflaum
Contact: alexander.pflaum@atl.fraunhofer.de

Background

Main target of the meeting in Shanghai is to compile standardisation requirements for wireless sensor networks.

Call for contributions concerning different sensor network issues (right part of slide)

Call for Contributions to the First Meeting of JTC 1 Study Group on Sensor Networks

The first JTC 1 SGSN meeting has now been announced in SGSN N002, and the JTC 1 SGSN is about to start the process of gathering contributions for consideration at its first meeting. The JTC 1 SGSN Convenor invites you to contribute to the first JTC 1 SGSN meeting in Shanghai, China, 25-27 June 2008 by submitting to any of the categories below.

- the current definitions, visions and requirements for target applications of Sensor Networks within JTC1 and outside JTC1 in connection with different application areas (e.g. home, medical informatics, transport informatics, industrial communications, RFID etc) as well as JTC 1 SCs roles in these application areas
- the unique characteristics of Sensor Networks and the commonalities and differences with other networks
- the system architectures of Sensor Networks in terms of functionalities
- the entities that together comprise Sensor Networks and their characteristics
- existing protocols that can be used for Sensor Networks and the elements of protocols that are unique to Sensor Networks
- the scope of infrastructure that can be considered to be a Sensor Network
- the types of data that need to be handled (acquired, processed, transported, stored, rendered etc) by Sensor Networks and any specific QoS attributes required by those categories
- the interfaces that need to be supported by Sensor Networks
- the services that need to be supported by Sensor Networks
- aspects such as security, privacy, identification that may be relevant to specific Sensor Networks
- other activities in international standardisation bodies and consortia and fora where specifications related to Sensor Networks are being developed.

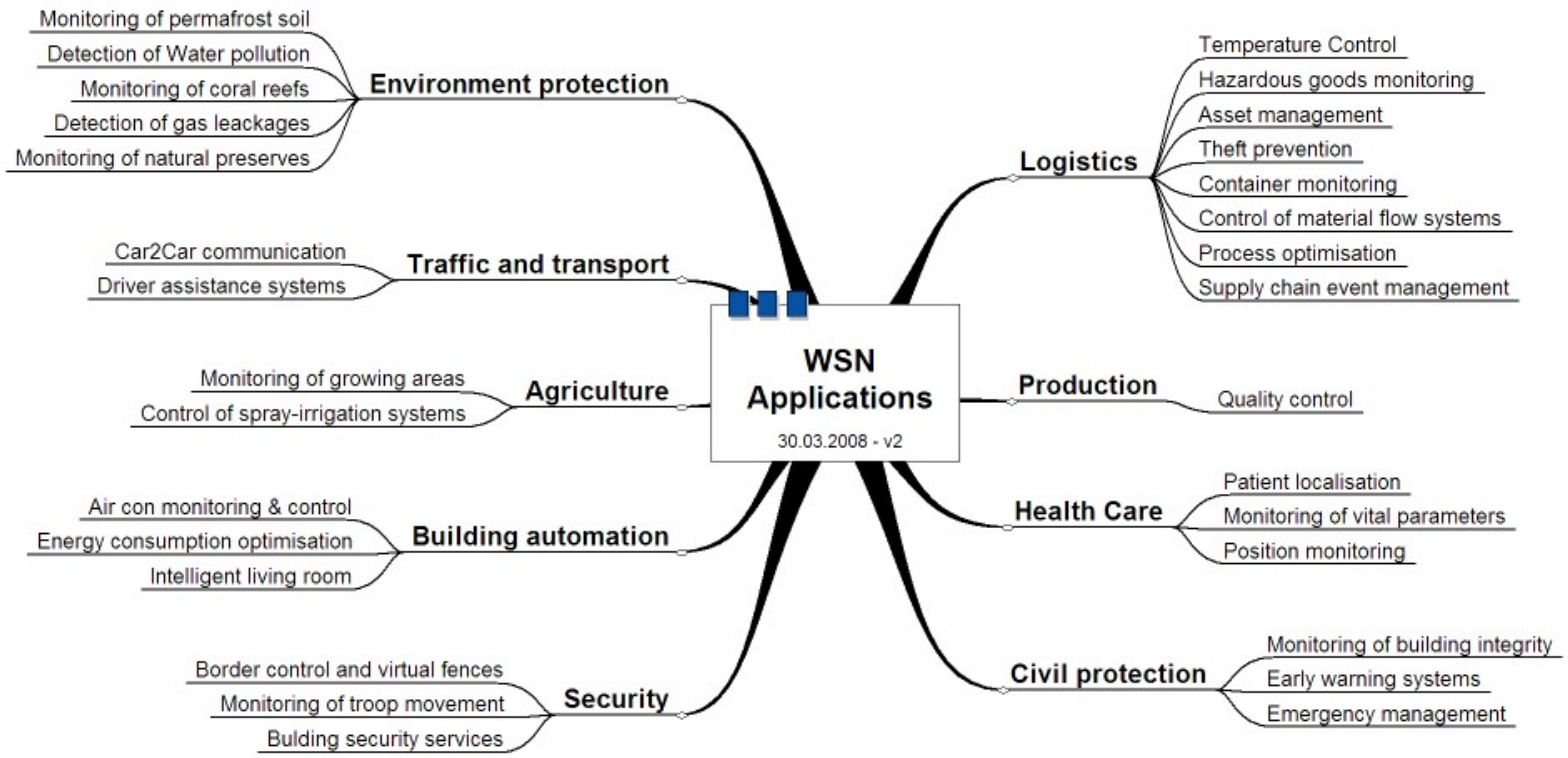
The above categories are described as per the Terms of References for the SGSN which were approved by JTC 1.

Content

- Target applications of wireless sensor networks
- Unique elements of sensor networks
- Basic system architectures and services to be supported
- Interfaces to be supported and data types to be handled
- Protocols and their unique elements
- Remarks concerning standardisation issues

I.1 Target applications of wireless sensor networks

Source: Study on existing applications of wireless sensor networks, Engineering Center for smart Objects in Logistics, 2007 (does not claim to be complete)

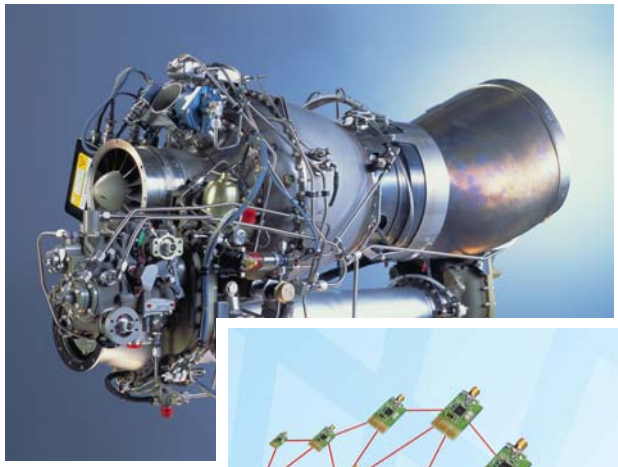


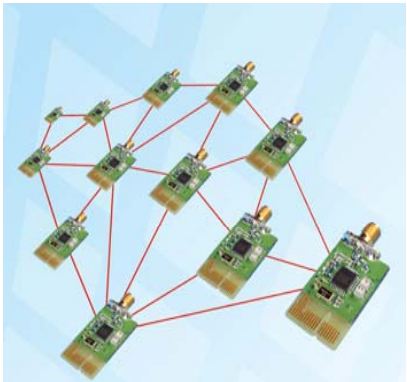
I.2 Examples for Target Applications of wireless Sensor Networks: Theft Prevention System for expensive Goods in Distribution Systems

Source: Courtesy of Fraunhofer ATL, Fürth

- Definition and Vision:
  - Packages on a pallet are equipped with sensor nodes that detect manipulations and monitor the physical presence ot their neighbour nodes.
  - In case of intrusion or theft an alarm message is generated and routed to a security service provider.
  - Sensor nodes support logistical processes and prevent from theft
- The more important requirements:
  - Size of a smart card
  - Latency time less than 5 seconds
  - Price of sensor node less than 2 € (estimated value, actually their is no business case for this application)
  - Cooperative operation with existing RFID technology

I.3 Examples for Target Applications of wireless Sensor Networks: Monitoring of Engine Conditions





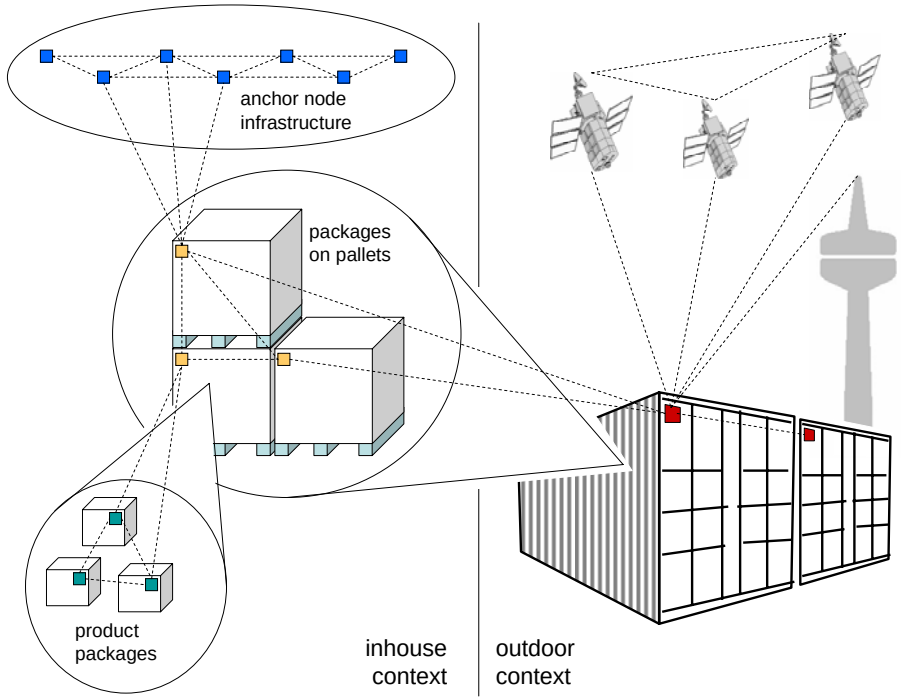
Source: Courtesy of Fraunhofer IIS, Erlangen

- Definition and Vision:
  - Miniaturized and energy autonomous sensor nodes identify and monitor the state of critical parts of an engine
  - They can additionally be used for identification in logistics processes as well as for documentation of maintenance activities.
- The more important requirements:
  - Integration into parts if possible
  - Robust and insensitive to high temperatures (operation in extremely hazardous environment)
  - Short latency time
  - High reliability and redundancy
  - Passive operation if possible (at least in long-term)

I.4 Examples for Target Applications of wireless Sensor Networks: Temperatur Monitioring for Blood Bags

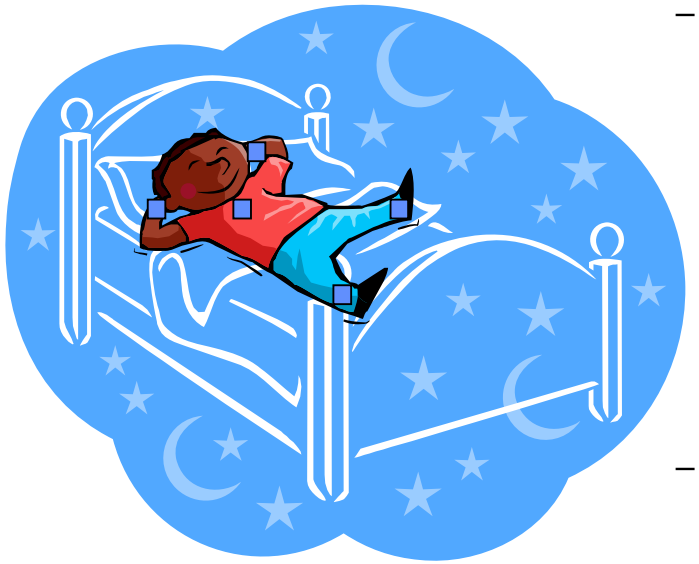
- Definition and Vision:
  - Miniaturized sensor nodes with a temperature sensing function are connected to blood bags
  - Logistical infrastructure (fridges and other storage devices, transportation media etc.) are equipped with anchor nodes for localisation and information routing
  - In case that the cool chain is interrupted somewhere in the network an alarm is generated and routed to an internal service provider
- The more important requirements:
  - Compliance with EMC regulations (clinical environments)
  - Robustness and reliability (acid cleaning agents)
  - Localisation resolution less than a few meters
  - »Realtime« localisation (only a few sec latency acceptable)

I.5 Examples for Target Applications of wireless Sensor Networks: Monitoring the Integrity of global Distribution Systems



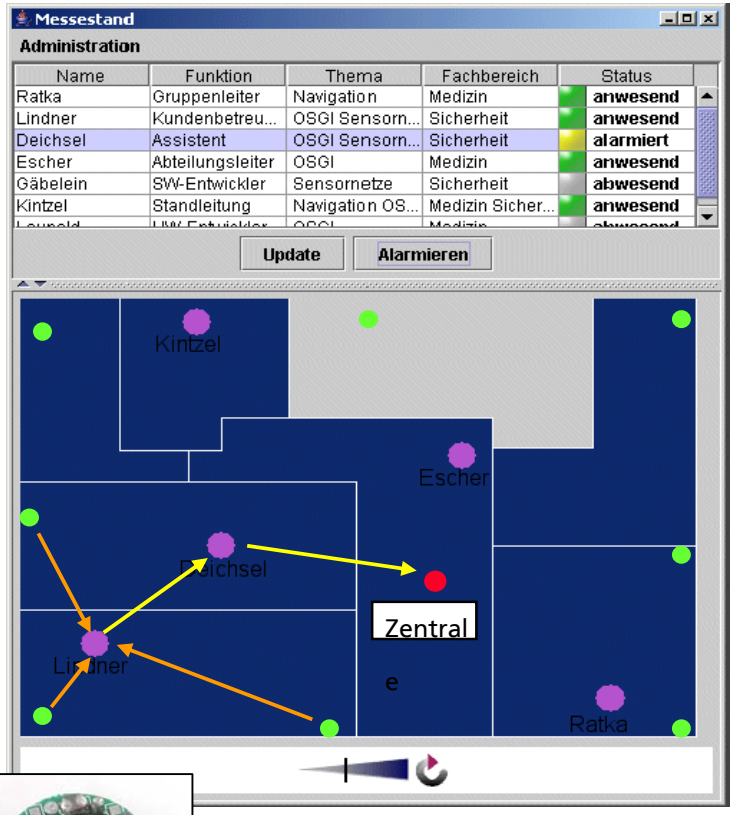
- Definition and vision:
  - Sensor nodes are attached to items on different hierarchical levels (products, pallets, containers)
  - System enables total transparency of worldwide supply chains without integration of existing tracking & tracing systems for different object types
- The more important requirements:
  - Same requirements of product and pallet nodes like in the theft prevention case
  - Protocols have to support hierarchical clustering of nodes
  - Leveling of energy consumption on container level necessary

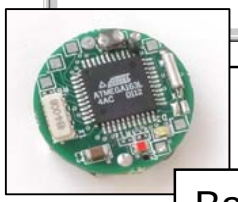
I.6 Examples for Target Applications of wireless Sensor Networks: Context specific Position Monitoring for Patients



- Definition and vision:
  - Intelligent sensor nodes are connected to extremities of the body, a central unit to the belt.
  - Sensor nodes are able to determine the relative position (relative to the other nodes and the central unit) as well as their 3-dimensional orientation in space.
  - If the position and orientation does not meet the normal conditions in a given context (walking, lying in bed etc.) an alarm message can be generated
- The more important requirements:
  - Small nodes which can be integrated into clothing
  - Localisation resolution less than a few centimeters
  - Orientation detection
  - Protection of the personal sphere of the patient

I.7 Examples for Target Applications of wireless Sensor Networks: Tracking of single Persons in large Areas or Buildings

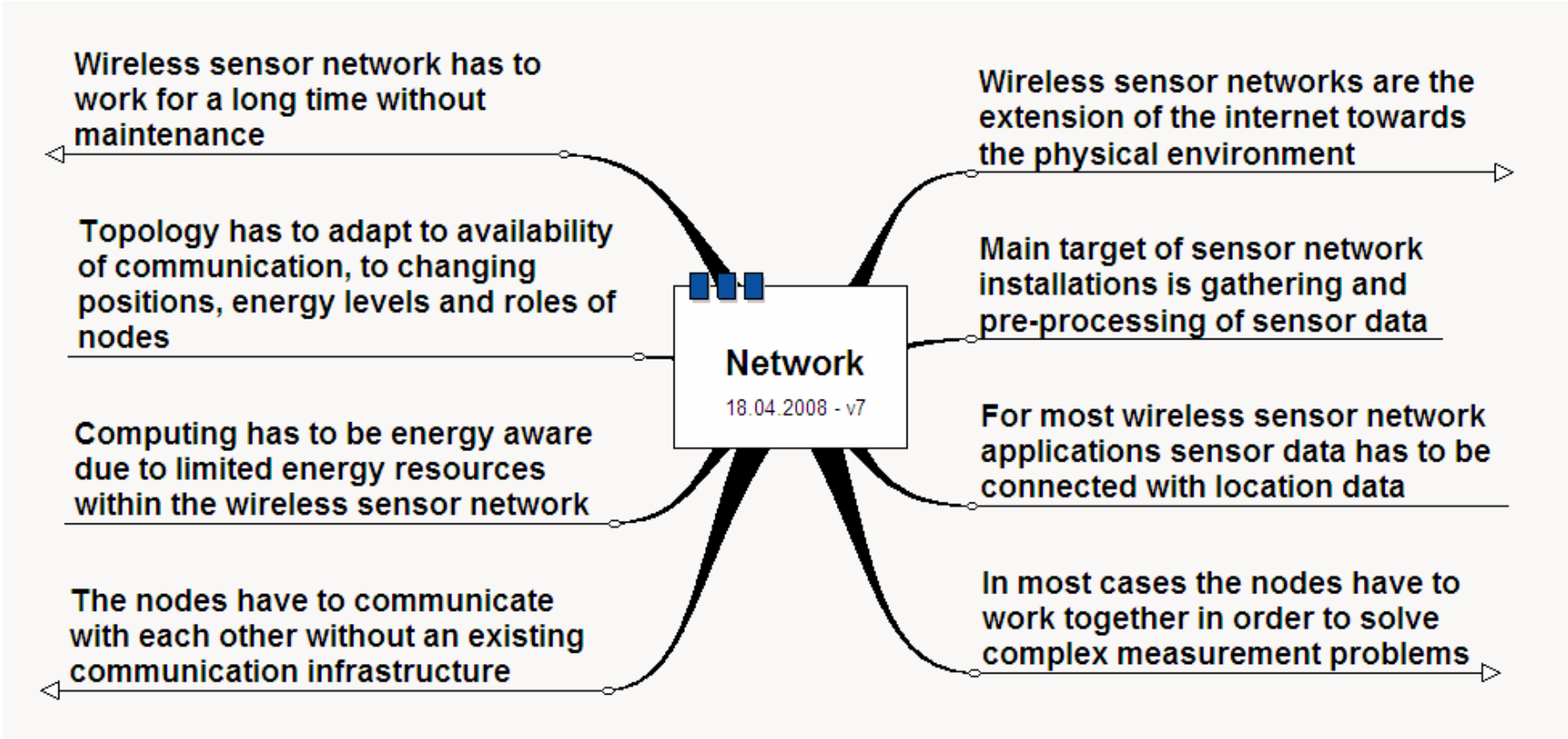




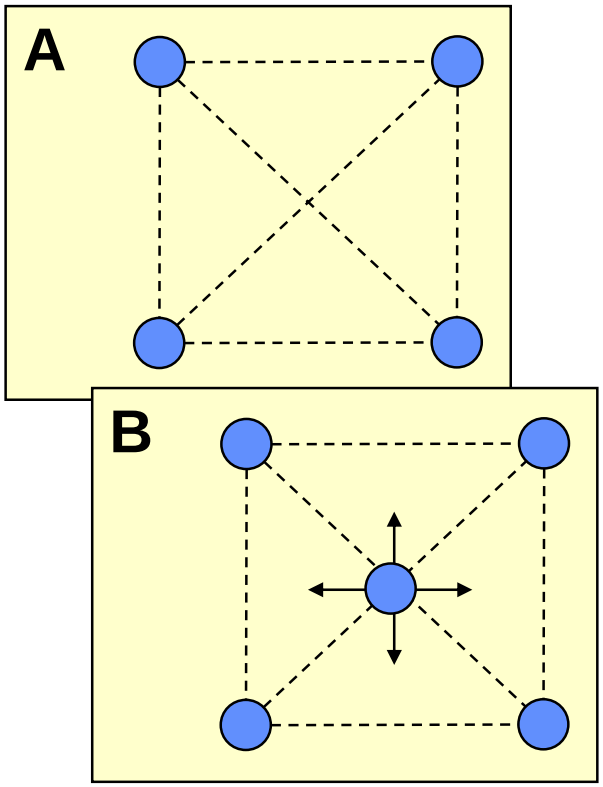
Badge

- Definition and vision:
  - Persons are equipped with small sensor nodes which are able to determine their own position using different localisation mechanisms.
  - Network of anchor nodes in a buildung delivers necessary beacon signals and routes location information to a central IT-System.
- The more important requirements:
  - Scalability of the overall system (large buildings)
  - Availability and robustness (in case of security applications)
  - Realtime location (difficult in large buildings with complex network structures)
  - Low energy consumption (long operation times without maintenance processes)

2.1 The wireless Network itself: Unique Characteristics

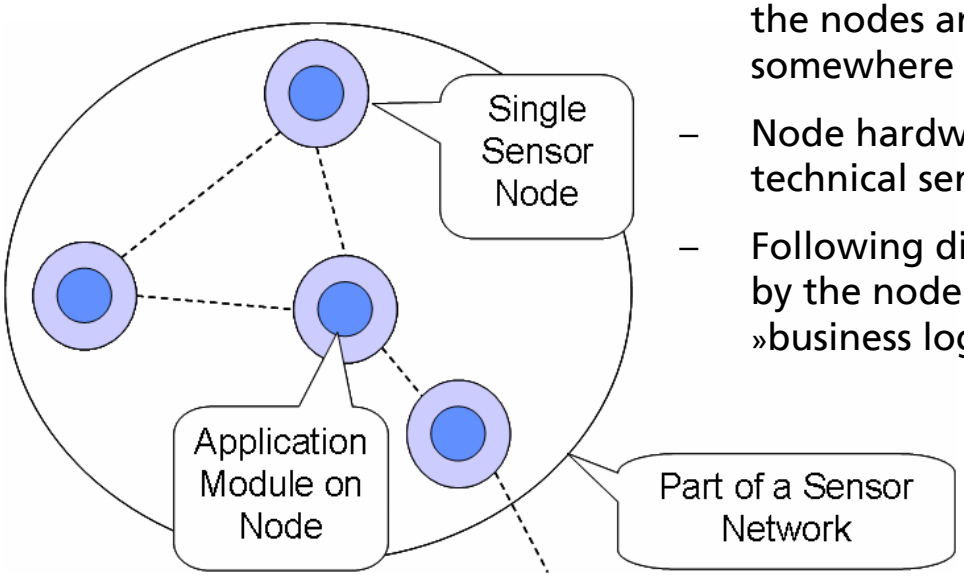


3.1 Basic System Architectures: Entities that comprise a Sensor Network and their Characteristics



- In general two different types of nodes within a sensor network:
  - Stationary nodes which are attached to parts of the infrastructure (walls, fences, ceiling, trees etc.)
  - Mobile nodes which are attached to moving objects (cars and other vehicles, logistical objects like pallets, containers etc.)
- Characteristics depend on the application! No general characteristics apart from size and energy efficency for the mobile nodes!
- Two types of applications have to be taken into account:
  - Applications which are based on stationary nodes (A)
  - Applications where networked mobile nodes flow through a network of stationary nodes (B)

3.2 Basic System Architectures: Services to be supported by Sensor Networks – The main Idea behind the »Service Issue«



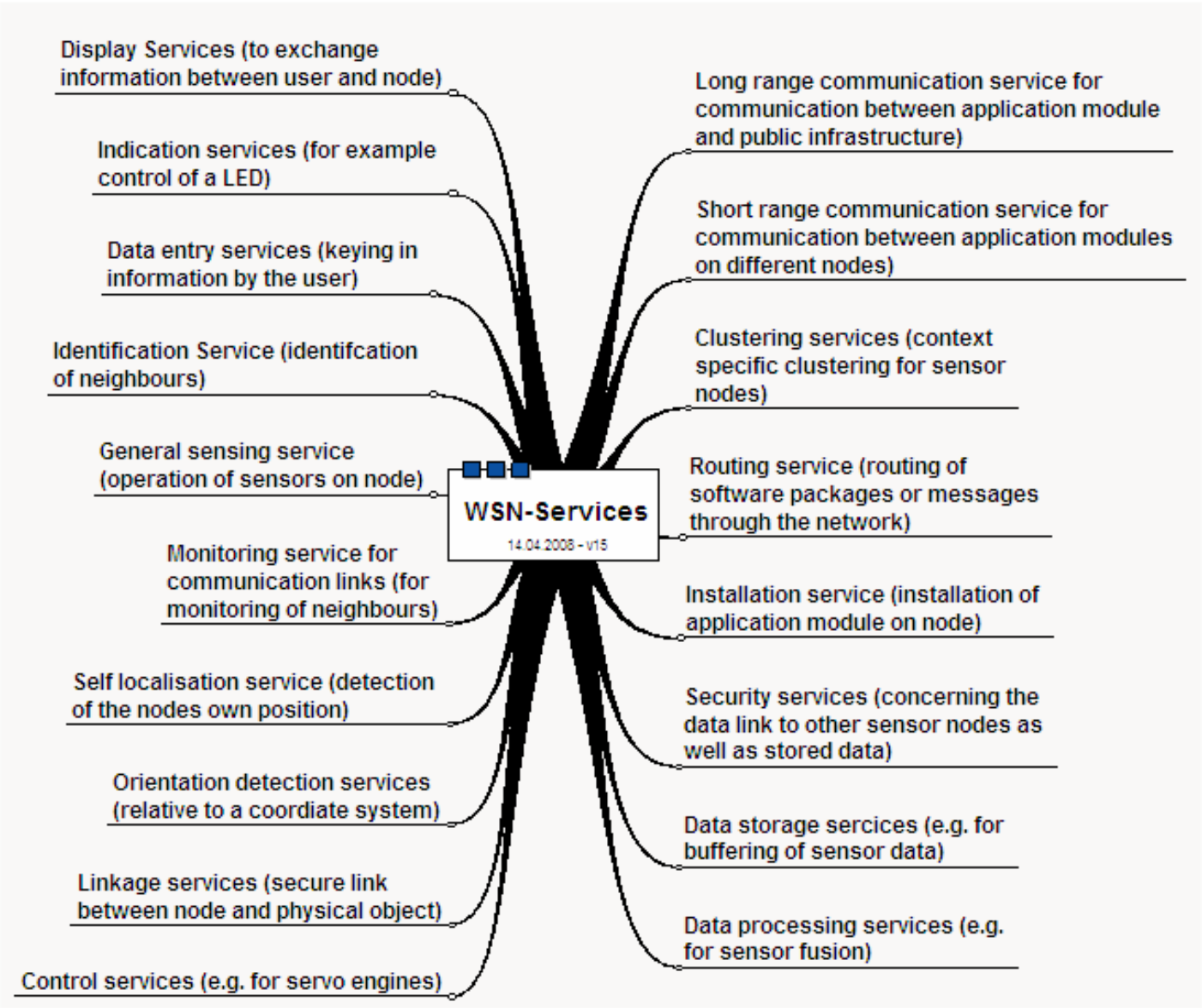
- Sensor networks are embedded into applications and more complex »services« for the end consumer or customer
- Application software is distributed (application modules on the nodes are connected to a central application module somewhere in the IT-backend of the company)
- Node hardware and »middleware« on the node deliver more technical services to the application module on the node
- Following discussion focuses the services which are delivered by the node itself in order to support application modules or »business logic« installed on the node

3.3 Basic System Architectures: Services to be supported by WSNs

Services in the mindmap are needed to support the different applications that have been described before!

Others might be necessary for other applications (therefore list does not claim to be exhaustive).

The services might also be understood as application specific »functions« of sensor nodes and networks.

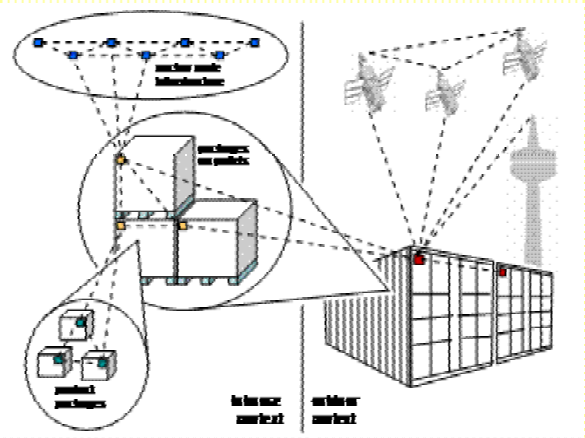


3.4 Basic System Architectures: Application specific and hierarchical Structures define the functional Architecture of a Network

There is no generic architecture in terms of functionalities!

Application defines distribution of functionalities to sensor nodes!

Example:

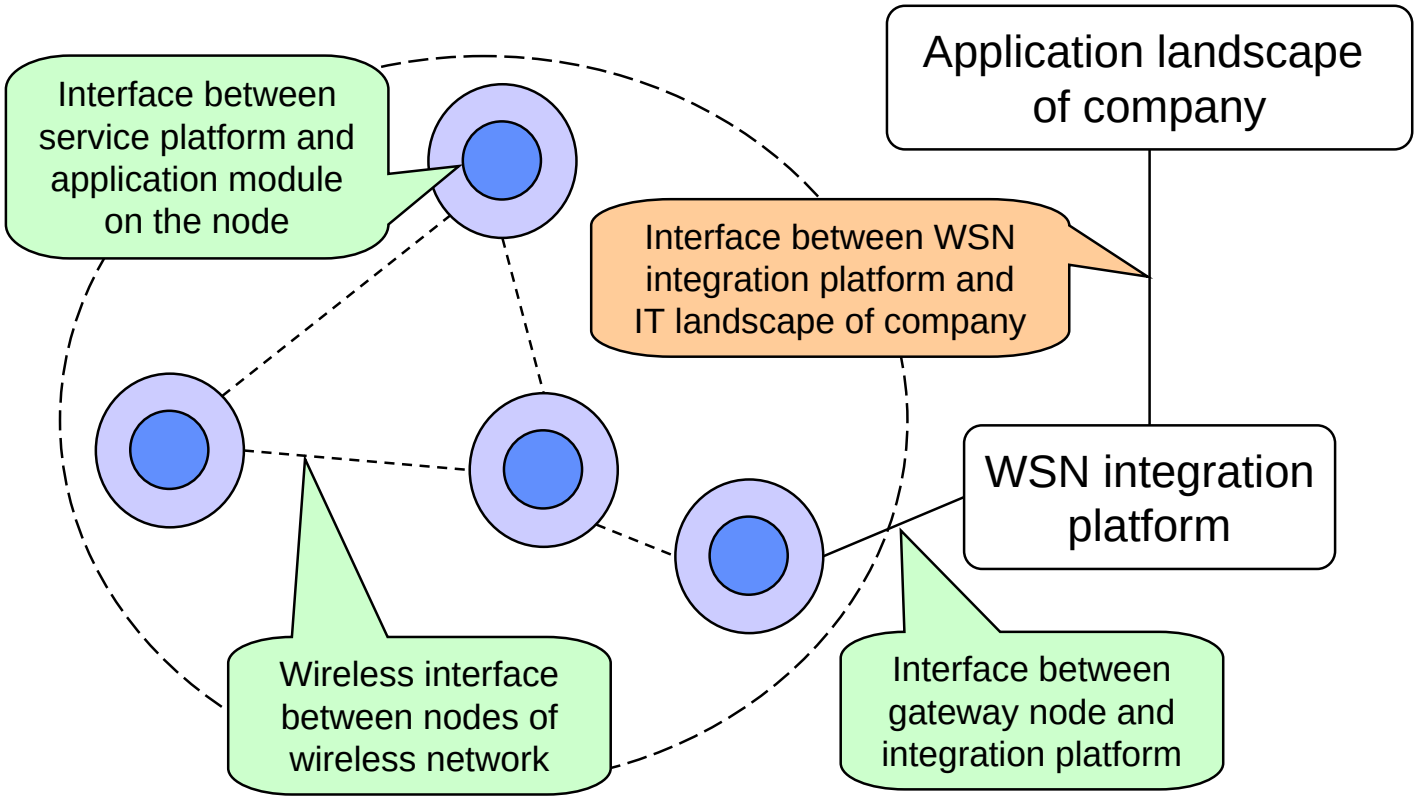


	Product node	Palett node	Container node	Anchor Node
Application specific services				
Long range communication				
Short range communication				
Installation services				
Security services				
Data storage services				
Data processing services				
Control services				
Linkage services				
Orientation detection services				
Self localisation service				
Neighbourhood monitoring servce				
Sensing service				
Identification service				
Data entry service				
Indication service				
Display service				
Network function				
Clock master				
Gateway to backend network				
Anchor services				
Network router				

4.1 Interfaces and Data Types to be handled in the wireless Sensor Network

Data types:

- *Identification number of node*
- *Sensor data, position and context information*
- *Business Logic or business rules / software agents*
- *Private or personal information*
- *Configuration data and network managament information*



5.1 Sensor Network Protocols: A few existing Standards and a growing Number of proprietary Application-specific Protocols

Source: Courtesy of Fraunhofer ATL, Fürth

- Two different types of protocols are used:
  - Standard or quasi-standard protocols like Zigbee, Bluetooth, WLAN (for high end applications) or TinyOS
  - Whole bunch of proprietary protocols like »Slotted MAC« of Fraunhofer IIS in Nuremberg and others
- Problem is that requirements of certain applications could not be met using existing standards
- Due to that number of proprietary and highly application-specific protocols is growing

Theft prevention as an example: Thin smart cards needed, more than three month lifetime without charging, less than five seconds latency time in a highly dynamic network-environment!

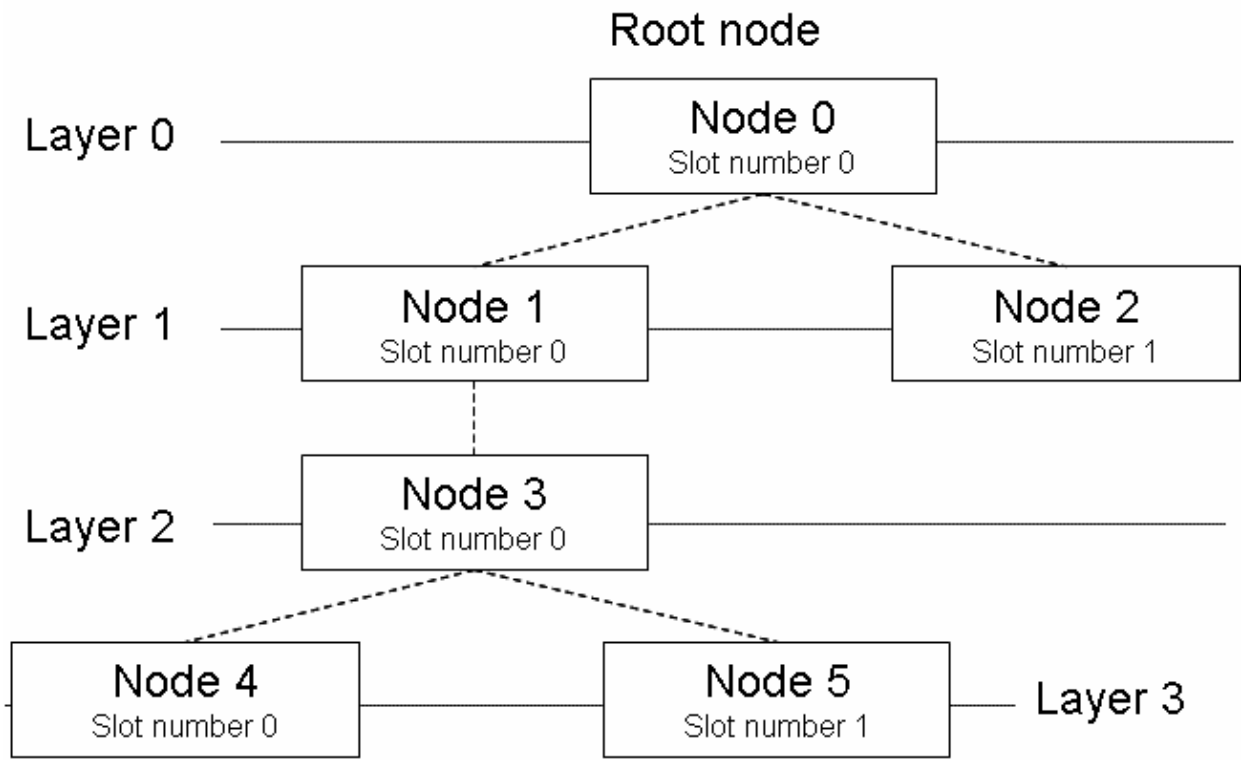
5.2 Sensor Network Protocols: Reduction of Latency time as one of the more important Task for Researchers

Picture on the right shows a tree-structure which is typical for a multi-hop network!

For the theft prevention system the situation becomes critical (latency time!) when

- *an alarm is generated on the lower network layers (many hops to root) and*
- *when many items with sensor node are on the palett (many layers)*

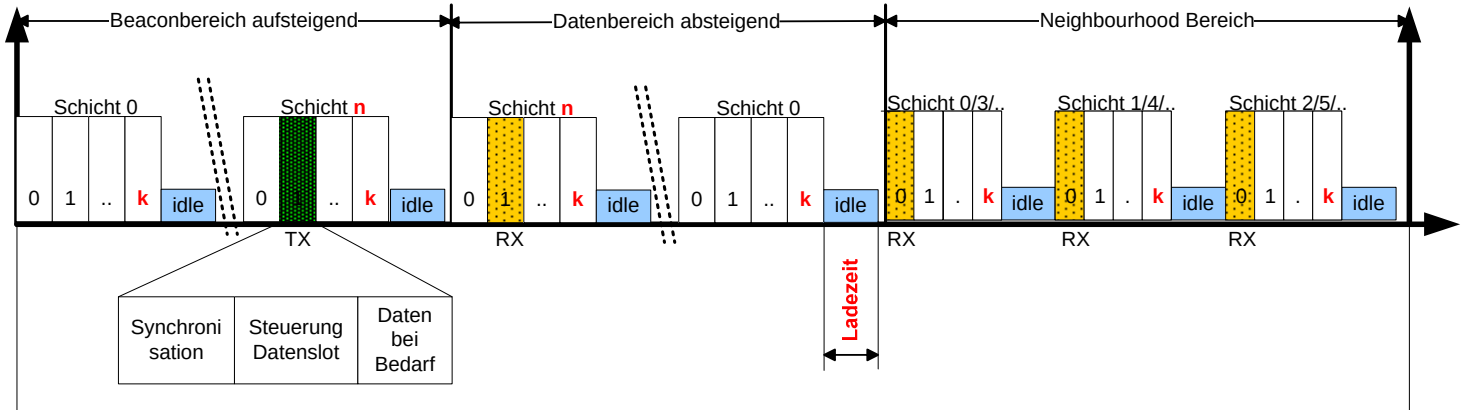
Zigbee and Bluetooth do not meet requirements and can not be used!



5.3 Sensor Network Protocols: Reduction of Latency time as one of the more important Task for Researchers

In case of the theft prevention system the answer was a proprietary protocol that combines the efficiency of Time Division Multiple Access and as well as the scalability and flexibility of other protocols.

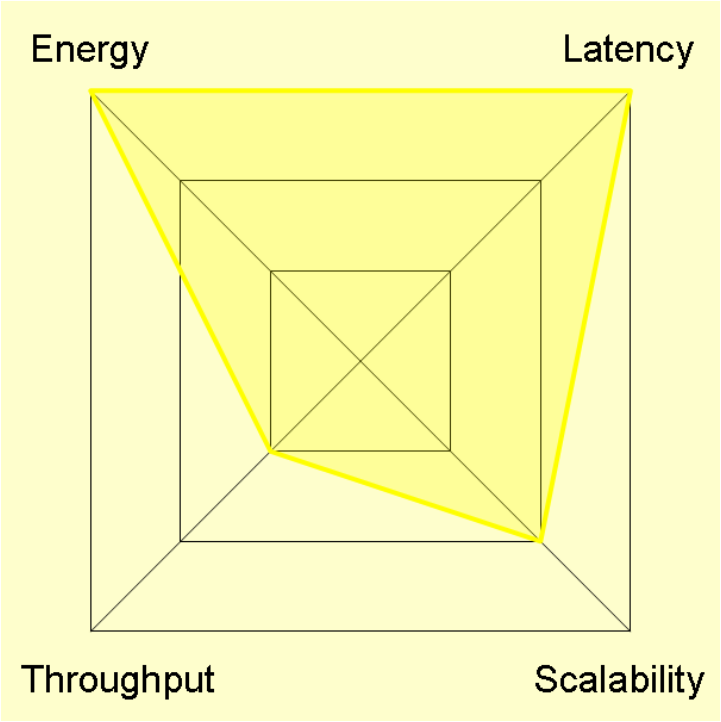
Latency time can be reduced by a smart configuration of time slots.



Three different domains for communication:

- Beacon domain for communication along the branches of the tree coming from the root
- Data domain for communication along the branches of the tree towards the root node
- Neighbourhood domain for communication between nodes which are physically neighbours

5.4 Sensor Network Protocols: Necessary »Trade-off« between different Targets seems to be the main Problem



- Main targets for designing a sensor network protocol:
  - Low energy consumption (lifecycle time)
  - Short Latency time (data extraction)
  - High data throughput (sensor information)
  - High scalability (number of objects)
- Seems to be a simple optimization problem but there is a conflict if all targets should be reached equally!

Thesis: Most critical target is »low energy consumption«. With high energy supplies latency time, throughput and scalability are less critical. Following that line of thinking besides application orientation energy efficiency is the most important characteristic of sensor network protocols.

6.1 Remarks concerning Standardisation Issues

- Large variety of different WSN applications in different areas! Due to different requirements profiles a generic standard (one size fits all) doesn't seem to be possible.
- Solution might be the identification and description of different application classes. Standards could than be developed for each class.
- Wireless sensor networks differ heavily from other existing networks. It will therefore be difficult to transfer elements of existing standards but in exceptional cases it might be possible.
- Application modules require a lot of different services to be supported by the sensor node. In order to push the implementation of the technology all these services need to be identified, described and – if possible – standardized.
- There is no generic system architecture in terms of functionalities. Basic architecture as well as distribution of system functions to nodes and backend depend on specific requirements of a given application. Again clusters or classes of similar applications could be identified.
- Exactly the same is true for the routing and communication protocols. Energy efficency which is needed for most applications requires a specific adaptation of existing protocols to the application which has to be supported by the sensor network.
- Last but not least: Sensor networks will operate in the same environments like RFID-systems, standards have to meet each other.

End of Presentation