Wireless in Automation - Summary

Manuel Waibel

June 19, 2023

Contents

1 Overview

Process: complete set of interacting operations of a system by which material, energy or information is transformed, transported or stored.

Technical Process: complete set of operations in a plant

Plant: complete set of technical equipment and facilities for solving a defined technical task. A plant includes apparatus, machines, instruments, devices, means of transportation, control equipment and other operating equipment.

1.1 Wired vs. Wireless

Wired	**Wireless**
High bandwidth	Low-medium bandwidth
High performance	Higher latency
Robust	Interference
Reliable	Unreliable by nature
Installation expensive	Installation cheap
"Unlimited" resources	Low power, memory
Static network	Mobile network
Security?	Security!

1.2 Multiplexing

1.2.1 Time Division Multiple Access (TDMA)

Channel occupies whole frequency for defined time slot.

- **Advantage**
  - Only one carrier per time slot
  - High throughput
- **Disadvantage**
  - Precise synchronization required

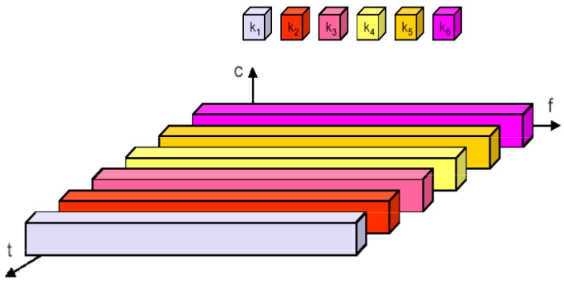

Figure 1: Time Division Multiple Access

1.2.2 Frequency division multiplex access (FDMA)

Total bandwidth separated into different frequency segments.
Channel occupies frequency segment.

- **Advantage**
  - No dynamic coordination
  - Also for analog signals
- **Disadvantage**
  - Inflexible
  - Waste of bandwidth in case of unequal load

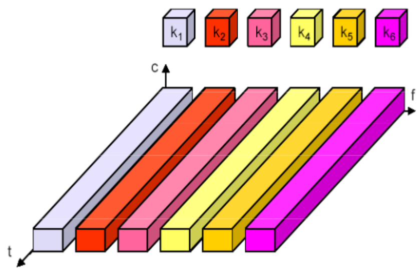

Figure 2: Frequency division multiplex access

1.2.3 Time and Frequency multiplexing

Combination of time and frequency multiplexing

- **Advantage**
  - (Quite) secure
  - protection against interference

– Higher user data rates

- **Disadvantage**
  – Precise coordination

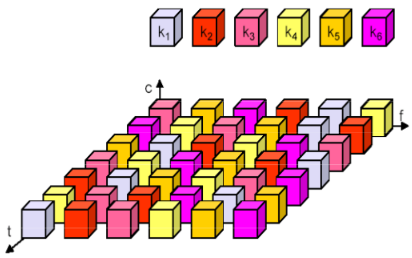

Figure 3: Time and Frequency multiplexing

1.2.4 Code division multiplex access (CDMA)

Each sender has unique orthogonal code → all senders can transmit at same time

- **Advantage**
  – Efficient use of bandwidth
  – No coordination or synchronization
  – Protection against interferences
- **Disadvantage**
  – User data rate limited
  – Complex because of signal generation

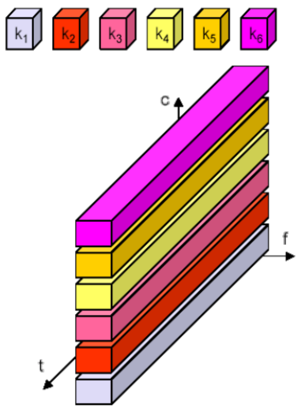

Figure 4: Code division multiplex access

2 IEEE 802.15.4, ZigBee, LongRangeWireless, Visual and audio communication

2.1 IEEE 802.15.4

- Defines the physical and the data link layer of the network stack.
- On top of this protocol lay protocols like ZigBee, WirelessHART or 6LoWPAN.
- It is an open standard, which is kept simple to ensure longevity and flexibility.
- It has fixed communication channels, which mean there is no frequency hopping possible.
- Either in star- or peer-to-peer topology
- Devices have a 64 bit extended address and a 16 bit short address

  64 bit address is unique in all of the network

  16 bit address is only unique within the local PAN
- Short range
- Low cost
- Low power consumption

2.1.1 Full-Function Device (FFD)

- Implements the full communication stack
- PAN coordinator and end device
- Can communicate with other FFDs or RFDs
- Externally powered

  Because of the complete communication stack and the use of the radio almost all the time

2.1.2 Reduced-Function Device (RFD)

- Implements only subset of communication stack
- Only end device
- Can only communicate with other FFDs
- Can be battery-powered

2.1.3 Communication

- Beacon enabled

  Synchronizes network (communication)

- Non-beacon enabled

  No synchronization

  Beacon on request

  Only CSMA/CA

Indirect data transfer:

- Star topology
- A device will request data from its coordinator

  Coordinators will not send unrequested data

- Power saving: devices can switch off

Direct data transfer:

- Device communicates with any other device (peer-to-peer)
- Power saving only in beacon enabled mode

2.1.4 Limitations

- Unbounded latencies

  Because of CSMA/CA

- No guaranteed bandwidth

  Not suitable for real-time networks

- Intrinsically unreliable
- Default MAC parameters are not optimal
- Acknowledgements are optional
- Prone to radio interference
- Cheap radio transceivers not suitable for harsh environments

→ in 2012 a new amendment was approved: IEEE 802.15.4e

2.2 ZigBee

Used in many home automation devices.

2.2.1 Device types

- **Coordinator**

  Full-Function Device (FFD)

  Externally powered

- **Router**

  FFD

  Externally powered

- **End device**

  FFD or RFD

  Can be battery powered

- **Green Power Device**

  Power harvesting - no battery power needed

2.2.2 Topologies

Star
Central ZigBee Coordinator and ZigBee End Devices are attached.

Tree
Central ZigBee Coordinator with attached ZigBee Routers. Routers then have End Devices attached as "leafs".
The routers are only connected to the coordinator, but not under each other.

Mesh
In the Mesh topology multiple routers are connected with each other. One of devices is the central Coordinator. Attached to some routers are the ZigBee Devices.

2.2.3 Routing

Broadcasting

- Every <u>routing</u> device forwards a broadcast message
- Passive Acknowledgement

  Device expects forwarded message from all its neighbours (except from the device it received the message)

Many-to-one Routing

- Usually used in sensor networks.

  A single node collects the data from multiple sensor nodes.

- Forwarding path is recorded

  Nodes build a routing table

Source/One-to-many routing

- Uses routing tables of all other nodes to build routing table of network

  Message is sent out and the response is the routing table/traceroute of the (last) node

  → Node now knows how to reach all other nodes.

Mesh routing/ Ad-hoc On-demand Distance Vector-Routingalgorithm (AODV) protocol
A wants to send to node B

1. A initiates a router request (broadcast)
2. All receiving node update their *route discovery table* and forward it to their neighbours
3. B send a (directed) *Route Reply* to A

   B uses the shortest path back to A
4. Routers update their *routing tables*
5. After communication the nodes drop their *route discovery table* and store the *routing tables*

2.2.4 ZigBee application Framework

Devices have applications, which have application objects.
Application objects implement **clusters** (e.g. On/Off cluster).
Clusters consist of **attributes** (e.g. On/Off - type boolean) and **commands** (e.g. On, Off, Toggle)

2.3 LoRaWAN Technology & Narrowband - IoT (NB-IoT)

2.3.1 LoRaWAN

Long Range wireless protocol with low energy consumption (40km line-of-sight with 100mW of power).
LoRa is "free-to-use" and you don't rely on any public infrastructure or license. You can

acquire a development kit and are ”good to go”, **but** the devices are quite expensive.

Duty cycle[1] is very small: 1% → data rates are very low

Example applications are in smart agriculture or smart cities.

2.3.2 NarrowBand IoT (NB-IoT)

- Depends on a network infrastructure provider

  - Dependency

  + Maintenance Support

- Relatively low cost per device

- Easy deployment

  Integration into cellular system

- Deep penetration (indoors or underground)

2.3.3 Comparison

- Dedicated infrastructure

  LoRa needs dedicated gateways, NB-IoT does not

- Frequency spectrum

  LoRa works on an unlicensed frequency spectrum

  NB-IOT services are synchronized and they are provided over licensed frequency bands (costs are not insignificant)

- Data rates

  NB-IoT outperforms LoRa by 20x

- Network coverage

  LoRa more suited for rural areas, NB-IoT for urban locations

- Ecosystem

  LoRa is older and better established, NB-IoT is still very new

[1] The duty cycle determines how long a device is allowed to send. The smaller the cycle the less active time the device is allowed to have (e.g if a device has a 50% duty cycle, that means that is it allowed to be active 50% of a timeframe - see figure `https://cdn.sparkfun.com/assets/f/9/c/8/a/512e869bce395fbc64000002.JPG`).

2.4 Non radio-frequency communication

2.4.1 Visible light communication

Use visible light to transmit information (e.g. IDs, acoustic signals, traffic light information, ...).

2.4.2 Ultrasonic audio communication

Transmit information via audio channel (17.5 - 22kHz).

\+ Only low-end hardware needed and possibility for retrofitting.
\+ Estimate the distance
\- Prone for disturbances.
\- Physical proximity neccessary

3 6LoWPAN, Energy and various Protocols and Wireless M-Bus

3.1 6LoWPAN

IPv6 was considered to be infeasible for most ”embedded” devices:

- bigger addresses cause bigger overhead

  Minimum MTU of 1280 bytes

- Using TCP connections consumes a lot of power

  Devices have to be connected constantly and cannot turn off their antennas

- Conventional IP routing is not easily applicable to mesh topologies

6LoWPAN then managed to adapt IPv6 in IEEE 802.15.4:

- IPv6 header compression
- Packet fragmentation (into smaller packets) and re-assembly
- Adaption of IPv6 neighbour discovery

3.1.1 Applications of 6LoWPAN

- Home and building automation
- Healthcare automation
- Industrial automation
- Smart meetering
- Real-time environmental monitoring and forecasting

3.1.2 6LoWPAN Packet

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 1 0 0 0 0 0 1|Version| Traffic Class |       Flow Label     ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... (FL cont.)  |         Payload Length        |  Next Header  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Hop Limit   |                                               |
+-+-+-+-+-+-+-+-+                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |                                               |
+-+-+-+-+-+-+-+-+                                               +
|                                                               |
+                       Destination Address                     +
|                                                               |
...
```

Figure 5: 6LoWPAN Format

- Dispatch byte (top left corner - `01000001`)
  - Indicates "what kind of traffic" it is
  - e.g. `01000010` - 6LoWPAN_HC1 compressed IPv6 packet
- Compression via omitting unused/redundant header fields
  - Flags indicate what is omitted and how
  - e.g. Flag to indicate link-local prefix (FE80::/64) address - address can be omitted
  - IP version header field can be omitted because it is always IPv6
  - Best case header size is 2 bytes instead of 40!

3.2 Energy

3.2.1 Energy conversion

EnOcean is a protocol which supports very low energy telegrams.

Example:
A button which if pressed produces a small amount of energy (e.g. via a piezo crystal). This is then enough energy to send a very small telegram (size of 3 bytes) to a light source to turn the light on/off.
$\rightarrow$ no battery or external energy source needed.

Because the messages have to be so small, there is no room for security. If security measures are added, more energy is needed.

3.2.2 Energy distribution

Radio Frequency Identification (RFID) absorb radio-magnetic field to be powered.

Wireless Interface for Sensors and Actuators (WISA) uses the same principal as RFID, but the energy used is way larger.

3.3 Wireless M-Bus

Used for smart grids.
Remote reading of different meters (gas, electricity, water, ...).

4 Deterministic Wireless

"Deterministic" in wireless protocols usually refers to how the wireless channels are used. With frequency hopping for example, the frequency to use is calculated via a simple algorithm.

4.1 WirelessHART

- Wireless protocol for industrial automation
- Extension to wired HART protocol
- Partially based on IEEE 802.15.4
- Deterministic communication
- Mesh architecture
- Security is mandatory

4.1.1 Device types

- Field device
  - Routing capabilities
  - Send and receive data
- Adapter
  - Connection to an existing wired HART network
- Gateway
  - Connects HART network to the plant automation network
  - Not necessarily wireless

  - Unique clock source for the whole WirelessHART network

- Access Points
  - Provide access to the wireless network
  - Connected with the Gateway (maybe via Ethernet or WiFi)

- Network Manager
  - Unique (exactly one Network Manager in the network)
  - Knows all of network and communication

    based on this it manages Scheduling and Routing

- Security Manager
  - Management and distribution of keys

5 WLAN, Bluetooth and various Protocols

5.1 IEEE 802.11x

WiFi is part of IEEE 802.11x (x = a, b, g, n, ac, ad, ax)
Depending on the flavour the protocol operates on different frequency bands (partly overlapping between standards: 1 GHz - 5 GHz or 60 GHz) and supports different bitrates (6 Mbit/s - 11 Gbits/s).

Typically has star topology (every device is connected to a central access point).

Access points are identified by beacon frames.

Authentication:
A device can/will associate itself with a APs SSID, so it can hop between APs that share the same SSID.

Encryption:
Authentication and encryption are independent.

Power saving mode:
Intended for battery powered node and marked by flag.

1. Node will choose sleep duration (typically 0.5s) and and sends empty frame to AP (with power save bit = 1).

2. AP will buffer all intended packages for this node.

3. On wake-up node will again send empty frame with power save bit = 0

4. AP will send all buffered data

IEEE 802.11 in Automation:
Not used in typical automation systems, but can be used in:

- production planning

  e.g. for maintenance

- data acquisition

  e.g. with mobile devices and existing infrastructure that support this protocol

- Applications with high throughput demands

  e.g. Video surveillance

- Network bridges or pipelines for other technologies

Power saving should not be a big factor, when using this protocol though (since it does it rather poorly).

5.1.1 IEEE 802.11p

Aka *WAVE*, is from the same working group as the WiFi standards IEEE 802.11x, but is actually something completely different.

It is used for vehicle communication (e.g. with ITS - intelligent transport system) and operates in the frequency band of $5,85$ to $5,925$ GHz.

It deviates from the conventional WiFi principles:

- data exchange is possible without association and authentication

  while driving there is no time to authenticate with multiple different access points

- adds timing advertisement, half the channel width

  ?

It does not have a lot of implementations (yet).

Downsides:

- High energy consumption
- Easily impacted by interference
- High traffic in P2P scenarios due to star topology
- Large protocol stack

5.1.2 IEEE 802.11ah

Aka *HaLow* uses 900 MHz band, which results in higher range and lower energy usage.

It introduces ”grouped stations”, which act as relays (mesh like - 2 hops max).
It also has wake/doze periods to save energy (similar to radio duty cycles).

It has quite a low through put (100 Kbit/s) but a longer range (1km).

It's applications are in IoT, Smart Metering and M2M (Machine-to-Machine) communication.

5.2 Bluetooth

Less throughput and range than WiFi, but more energy efficient (can be used with battery powered devices).

Downside: very vulnerable to interference

Layers:

Application
RFCOMM/SDP
L2CAP
Host Controller Interface (HCI)
Link Manager
Link Controller
Baseband (ACL, SCO, eSCO)
Radio

5.2.1 Radio layer

- Bluetooth networks are called ”Piconets” and have a star topology (primary-secondary).
- The primary can wake up secondaries to communicate.
- Up to 8 active devices (3 bit Piconet address).

  1 primary and up to 7 secondaries
- ”Scatternets” are pooled/connected Piconets.

5.2.2 Baseband layer

Different types of connections:

- Asynchronous Connection-Less (ACL)
  - Connectionless, packet oriented
  - Low priority
  - No bandwidth guarantees
- Synchronous Connection-Oriented (SCO)
  - Synchronous P2P
  - Primary assigns time slot to secondary
  - No integrity checks
  - Bandwidth guaranteed
- Enhanced Synchronous Connection-Oriented (eSCO)
  - Integrity checks
  - Higher throughput than SCO

5.2.3 Link Controller

Responsible for creation and management of connections.

Scans:

- Inquiry and Inquiry Scan
  - Find unknown devices
  - Devices open for connections regularly switch to "Inquiry Scan" state
- Page and Page Scan
  - Creaton of an ACL connection
  - Address must be known (from inquiry or previous connection)

There are energy savings happending in this layer:

- Connection-Hold

  Primary and secondary agree on a "timeout" and both shut down for some time
- Connection-Sniff

  Primary and secondary negotiate a Sniff-interval
- Connection-Parking

  Secondary gives IP its Piconet address (if for example turned off for some time) → address becomes available again.

5.2.4 Link Manager

Manages connections:

- Creation of ACL, SCO or eSCO connections
- Closing of connections
- Configuration of e.g. time slots
- Distribution of Piconet addresses
- Enabling/Disabling energy saving modes
- Control adaptive frequency hoping (AFH)
- Pairing
- Security checks

  Bluetooth <= 2.0 uses PIN for authentication

  since Bluetooth 2.1 various pairing protocols for different applications & private/public key with elliptic curve Diffie-Hellman

  Authorization: restrict services and access

5.2.5 Host Controller Interface

E.g. via USB, UART or SD (embedded PCs with SD-interface)

HCI commands (host → controller)
Events (controller → host)

5.2.6 Logical Link Control and Adaptation Procotol (L2CAP)

Create multiple logical connection over one physical connection → Protocol Service Multiplexer (PSM)
BUT only for ACL connections!
SCO and eSCO connection are created directly over HCI → no multiplexing

5.2.7 RFCOMM/SDP

Virtual serial interface for data transfer.

Bluetooth profiles:

- Serial Port
- OBEX File Transfer

- Dial-Up

  e.g. phone provides internet access for laptop over Bluetooth

- Human Interface Device (HID)

  e.g. for keyboards

Services are listed in the Service Database.
Services are found over the Service Discovery Protocol (SDP)

5.2.8 Bluetooth in Automation

Pros:

- Wide spread
  - Automated Guided Vehicles (AGV)
  - Wireless Sensor and actuator networks
  - Home and building automation
- Often already "on-board"/supported by devices

Cons:

- Large stack with large overhead
- Energy intensive (<= 3.x)

  Continuous polling through primary node

  Fixed in >= 4.x

- Low range
- Small networks
- Just star topology available (<= 3.x)

  Mesh capabilities announced in 2017

- Not an open standard

5.3 Z-Wave

- Focuses on home automation
- Mesh networking with source routing
- Maximum of 232 devices

- Device classes
  - Controllers

    Aware of entire topology

    Configure secondaries

    Handle security and routing
  - Secondaries

    Only reception and acknowledgement

    Routing secondary: Data relaying along predefined routes
- Stardard device classes for ”basic” interoperability (like in ZigBee)

  Light controller

  ...

5.4 KNX-RF

KNX-RF devices cannot be used with normal wired KNX group addresses (because group address might not be unique over RF e.g. if neighbour uses same group addresses) → fix:
extend group addresses: 6 octets serial number + 2 octets standard group address
→ every device knows serial numbers of sending devices, which are part of the same group

5.5 Insteon

Dual-mesh network:
Uses both wireless and wired media (power line)

Broadcast based transmission scheme → flooding of messages → no routing required

Telegrams: 3 byte address + 14 byte user data
Hop limit: 0-3