Ubiquitous Computing Summary

Ulla Aeschbacher

14.8.19

Contents

1 Introduction

1.0.1 Ubiquitous computing: Ubiquitous computing is a vision of how we will live and interact with future computing environments. Examples include network embedded systems, wireless sensor networks, wireless communications, distributed systems, mobile devices and human-computer interaction.

1.0.2 Important aspects of Mark Weiser's vision: His vision has a broad background, inspired by social scientists, philosophers and anthropologists. He feels like the most powerful things are those that are effectively invisible in use. For him, ubiquitous computing means that computing doesn't live on a personal device of any sort, but it is in the woodwork everywhere.

1.0.3 Synonyms to ubiquitous computing: There are many synonyms due to different people giving different names to similar visions. Examples are pervasive computing by Lou Gerstner from IBM, ambient intelligence from Emile Aarts from Philips Research and things that think from Neil Gerstenfield at MIT.

2 Vision

2.0.1 *Technical visions slowly become true because of cheaper hardware, smaller hardware, wireless communication at almost no cost and sensors that provide context to objects.*

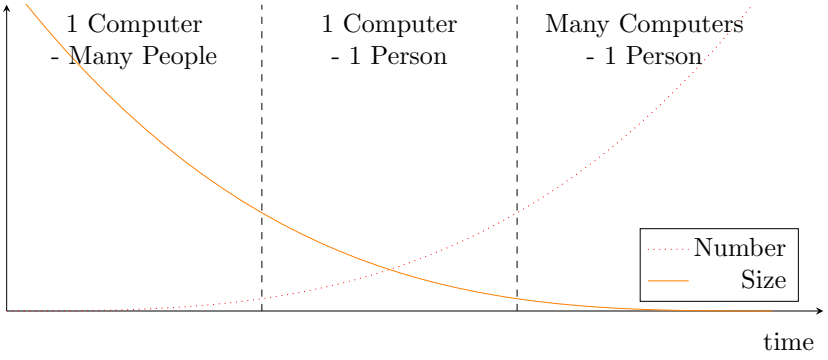

Figure 1: Computing Trend

2.0.1 Technological push and application pull: The technological push is complemented by an application pull because there is value for business, society and individuals.

2.0.2 The evolution of networking:

- Internet: network of computers, TCP/IP
- Web: network of documents, HTTP, HTML
- network of services, XML, WSDL
- network of smart things, JSON

2.0.3 Smart objects: Smart objects are small, cheap and integrated sensors and processors with wireless communication.

2.0.4 Two important smart object paradigms:

- Outsourcing smartness, so that the smart object doesn't need to provide everything itself as long as it can communicate with something that can do it instead.
- Outsourcing the user interface, so that the smart object can be made much cheaper.

2.0.5 Bits vs. atoms: Bits implement all the smart behaviour, while atoms are the physical objects.

2.0.6 Technological paternalism: Paternalism can be considered repressive, by protecting people and satisfying their needs but without allowing them any freedom or responsibility. Technological paternalism is already observed today, for example the beeps in a car if the seat belt is not fastened. The list of potential examples is growing.

2.0.7 Reversal of defaults: Ron Rivest coined this term to describe the current trend where what once was private is now public, what once was hard to copy is now trivial to duplicate and what once was forgotten is now stored forever.

3 Four Ubicomp Drivers

3.1 Moore's Law

3.1.1 Moore's law: Processing speed and storage capacity doubles around every 18 months.

3.1.2 Generalized Moore's law: The most important technology parameters like computation cycles, capacity of memory and bandwidth double every 1-3 years. But batteries and users mind-share do not.

3.1.3 Batteries: The efficiency of battery technology is improving only slowly over time. Considerations to take into account in respect to batteries include size, weight, cost, peak current vs. average current, rechargable vs. disposable, time to recharge, cycle life and ecological concerns. To save and gain energy we can enable power management in hardware units (shut down unused sections, reduce clock frequency and reduce voltage), use power-aware algorithms and harvest energy from the human body or the environment.

3.2 New Materials

3.2.1 New materials: Examples of new materials are organic semiconductors, flexible displays and graphene.

3.3 Progress in Communication Technologies

3.3.1 Progress in communication technologies: Examples of new technologies are fiber optics, wireless 5G and bluetooth.

3.3.2 Near-field communication (NFC): NFC is short-range ($\sim$10 cm) interaction with handheld devices for example contactless payment. There are many advantages like using almost no energy, requiring only small transmitters and receivers, cheapness, security and no addressing or routing needed.

3.3.3 Intrabody communication: Intrabody communication works by sending low-power electrical signals through the human body. This allows wearable devices to communicate and enables touch-selective communication. Some applications are that a car can recognize the driver, a shared device configures itself when being touched, devices identifying users and granting access and micro payments. Issues are the fear of phone radiation, safety concerns, reliability and security.

3.4 Better Sensors

3.4.1 Better sensors: Examples of better sensors are miniaturized cameras and microphones, biometric sensors, temperature and humidity sensors, acceleration sensors and location sensors.

3.4.1 *Sensors are the interface between the real world and the cyber space.*

3.4.2 Piezoelectric Effect: The piezoelectric effect describes the generation of energy resulting from an applied mechanical force.

3.4.3 Surface acoustic wave (SAW based sensors): SAW based sensors need no battery or external power supply, they are powered by external RF interrogation signals or alternatively by physical actuation processes. They reflect the RF signal transmitted by an antenna up to 50 m away. The surface wave is a mechanical wave that propagates on the surface of a body, on piezo crystals for example it propagates at around 3500 m/s.

3.4.3.1 Piezoelectric Transponder: The combination of a transducer and multiple reflectors is called a transponder, from transmitter-responder.

3.4.3.2 How it works: When a signal arrives at the sensor, the transducer converts the electric energy from the RF waves to the surface acoustic wave. Each reflector then sends back parts of the wave thus encoding the response. The wave is then transformed back into an RF pulse sequence by the transducer and sent out. The surface wave is much slower than the RF wave, so a response takes more than 2 μs. This has the nice side effect that RF noise, e.g. reflections by the environment, is not mistaken as the answer by the antenna, because it decays after around 1 μs, so before the answer can arrive.

3.4.3.3 Other SAW based sensors: One can add a second transformer at the end which changes the impedance. It is controlled by a resistor that depends on the sensor value.

3.4.4 Applications:

3.4.4.1 Applications for SAW: Some applications of SAW are temperature sensors, gas sensors, biosensors and tire sensors.

3.4.4.2 Applications for battery-free sensors with transponders: Some applications are identification, temperature sensing, pressure sensing, transport monitoring, product tracking and material flow.

4 Near Field Communication (NFC) & Radio Frequency Identification (RFID)

4.0.1 RFID: RFID identifies objects from a distance. It is a small integrated circuit with a radio frequency transponder. A transponder is a transmitter-responder which generates a response to a received signal. The RFID circuit runs on a wireless energy supply due to a magnetic or electromagnetic field. It contains around 100 Bytes of ROM or EEPROM and costs around 1 cent.

4.0.2 Performance of RFID chips:

- Low end features: read-only memory, tag repeatedly sends out serial number, no collision detection
- Medium range features: read-write memory, collision detection
- High end features: complex functions such as cryptography

4.0.3 Electronic product tag (EPC): The EPC is a standard for logistics and retail applications, managed by an industry consortium. It is a unique identifier for finding information providers about a specific product instance.

4.0.4 Defining features of RFID: RFID systems have four defining features: power supply; operation frequency; communication, coding and modulation, and anti-collision protocols.

4.0.5 Applications of RFID: RFID applications include animal identification and tracking, security gates at exits of shops, self-checkout of a stack of books at a library, car keys, baggage labels and ticketing.

4.1 Power Supply

4.1.1 Power supply: The tag needs energy to power the microchip and to transmit data to the reader. There are two coupling principles: inductive coupling (near field) and electromagnetic wave coupling (far field).

4.1.2 Inductive coupling: We only consider inductive coupling here, where the magnetic field generated by the reader induces a voltage in the coil of the transponder. This typically is around 10 mW at 1 cm and 100 μW at 10 cm. Note that EEPROM needs significantly more energy than ROM.

4.2 Operation Frequency

4.2.1 Operation frequencies: Typical frequency domains are 134kHz (low frequency), 13.56 MHz (high frequency), 868/915 MHz (ultra high frequency) and 2.45 GHz (micro wave). They have different characteristics like sensitivity against metal parts, achievable data rate, national/international regulations and what other services use this spectrum.

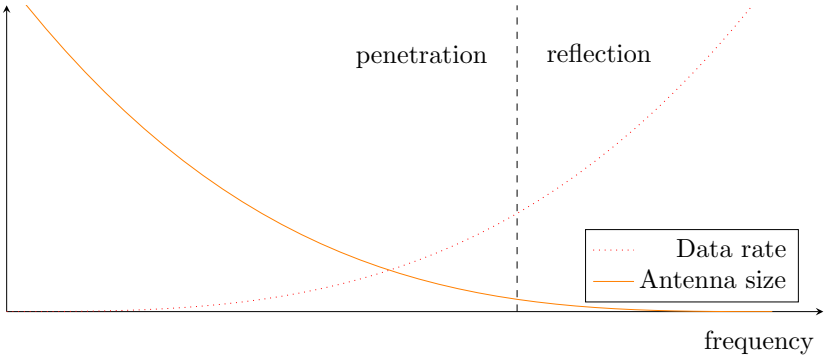

Figure 2: Operation frequencies

4.3 Communication, Coding and Modulation

4.3.1 Communication principles: The field of the reader may be turned off periodically to allow transponders to send in-between. This requires a capacitor on the transponders to buffer energy.

4.3.2 Typical encoding schemes:

4.3.2.1 NRZ: 1 = high, 0 = low

4.3.2.2 Manchester: 1 = high→low, 0 = low→high. This is typically used for tag to reader communication.

4.3.2.3 Pulse pause coding (PPC): 1 = short period to next pause, 0 = long period to next pause. This is typically used for reader to tag communication.

4.3.3 Data transfer from reader to tag: Amplitude shift keying (ASK) is used to switch the antenna driver of the reader on and off. ASK uses a finite number of amplitudes each assigned to an unique pattern of bits. The energy stored in the reader's antenna decays rapidly by cutting it down with clipping diodes.

4.3.4 Data transfer from tag to reader: There are several principles used here:

- Capacitive coupling uses an electrical field and works for very short distances
- Load modulation uses a magnetic field and works for near distances. Magnetic coupling works by turning a resistor in the oscillating circuit of the transponder on and off and thus yielding a small voltage change at the antenna of the reader.
- Backscatter uses an electromagnetic field and works for long ranges. Electromagnetic coupling works by switching a resistor parallel to the transponder antenna on and off and thus changing the reflection properties.

The data rate is typically several kbits/s up to 100 kbits/s.

4.4 Anti-Collision Protocols

4.4.1 The collision problem: The reader broadcasts energy and its signal to many transponders, then all transponders may react simultaneously. They will interfere if there is only a

single shared channel. Ideally a transponder should have exclusive access to the shared channel during the short period where it transmits a few bytes. But transponders usually don't hear the signal from other transponders, only the one from the reader. We want access control and collision detection/avoidance to be fast and reliable.

4.4.2 Capture effect: The throughput improves if transponders closer to the reader "win" because of their stronger signal. Difference in signal strength leads to the problem of weak collisions, where the reader might not notice the presence of a weak signal because of an overwhelming presence of a strong signal and thus collisions might go unnoticed.

4.4.3 Collision avoidance with FDMA: This approach needs many channels in parallel, hence it is only suitable for some particular applications with a small, fixed number of transponders.

4.4.4 Stochastic protocols: Stochastic protocols usually do not detect all tags in one read cycle, there is overall less reader to tag communication and there is typically an ALOHA-based anti-collision algorithm.

4.4.4.1 ALOHA principle: Transponders repeatedly send out their data with random length quiet periods in-between. The data should eventually get through. The higher the load, the more collisions happen. This has a maximal throughput of 18.4%. This is a stochastic TDMA protocol.

4.4.4.2 Slotted ALOHA: Transponders start their transmissions only at well-defined instants (slots). Synchronization is done by the reader who periodically sends out "sync" commands. All transponders then send their serial number in one of the following slots. If the reader gets only one serial number "sn" it sends a "select sn" command. Only the transponder with serial number "sn" responds by sending its payload data. The maximal throughput is then 36.8%.

4.4.4.3 Reservation ALOHA: This protocol has two phases: first a short ALOHA phase where the transponders compete for reservations, then the reserved phase for payload data transmission.

4.4.4.4 Adaptive round algorithm: In this extension of reservation ALOHA the number of slots is dynamically altered, depending on the number of collisions and empty slots.

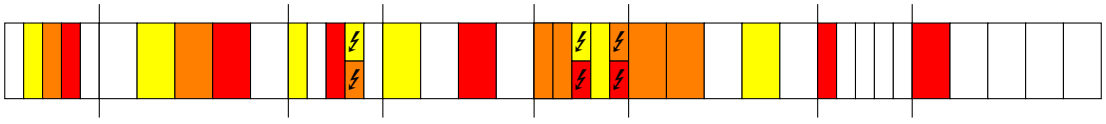

Figure 3: Reservation ALOHA

4.4.5 Deterministic protocols: Deterministic protocols usually detect all tags that are present in a read cycle, but they introduce high reader to tag communication overheads. There is typically a tree-walking anti-collision algorithm.

4.4.5.1 The coding scheme: We use Manchester encoding, so that where two signals that are transmitting over each other differ, it results in an illegal signal and the reader can locate these bits. This requires bit synchronization.

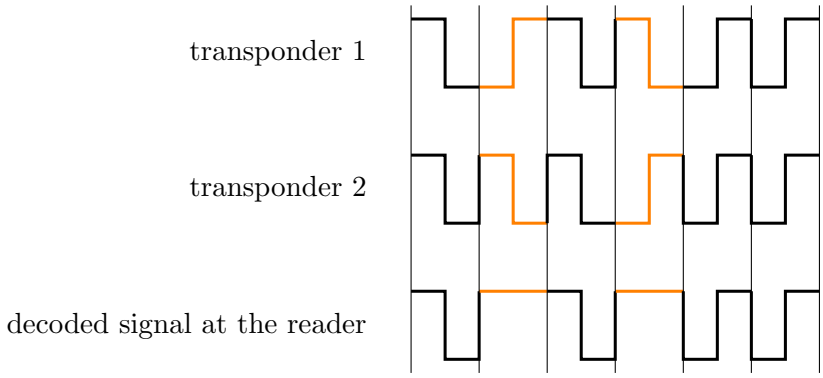

Figure 4: Coding scheme to detect collisions

4.4.5.2 Tree-walking anti-collision algorithm: The reader broadcasts a "sync" to all transponders, then requests the ID number of all transponders. It then determines the leftmost bit b that yields a collision. If there is none, the reader requests data from the unique transponder x, then sends "halt" to x. Then the reader moves up the tree to the next appropriate subtree with a different value of the last b. If there is a collision, the reader broadcasts "mute if value 0 at position b" Only transponders with value 1 at position b move to the next round, all others remain mute from now on.

4.5 Business-relevant and application-driven criteria

4.5.1 Read range: Low and high frequency have a read range of 1-1.5 m, ultra high frequency has a read range of around 10 m. The working area is typically complex.

4.5.2 Data transfer and detection rate: Low and high frequency have a data transfer rate of 5 kb/s, ultra high frequency has a data transfer rate of 50 kb/s. The detection rate depends on the data transfer rate, the choice of anti-collision algorithm and the length of the tag ID. Typically low and high frequency have a detection rate of 10-30 tags/s, ultra high frequency has a range of 100-500 tags/s.

4.5.3 Susceptibility to noise and error sources: This depends on frequency, antenna size and protocol.

4.5.4 Cost: The cost typically ranges from a few cents to a few dollars.

4.5.5 Form factors: This includes things like the coice of paper vs. plastic.

4.6 Strengths and Drawbacks of RFID

4.6.1 Strengths of RFID:

- No line of sight required
- Longer read range
- More bits
- Multiple tags can be read nearly simultaneously
- Write and change data
- Possibility to integrate sensors

4.6.2 Drawbacks of RFID:

- Cost
- Unreliable under certain conditions

5 Smart Cards

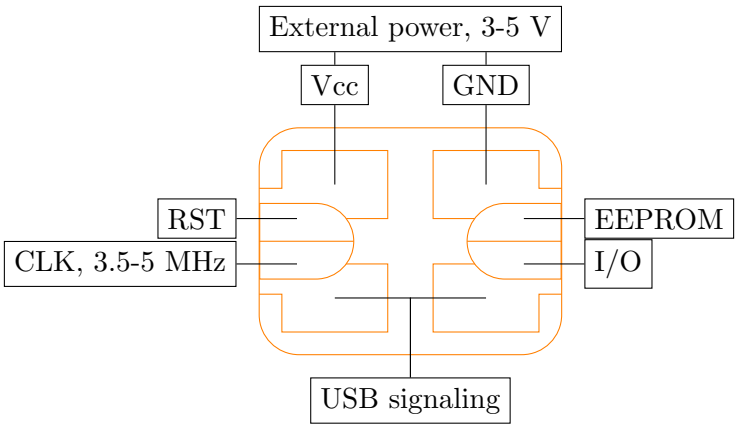

Figure 5: Smart card ISO standard

5.0.1 Main use: Smart cards are portable secure containers for secret data. They are a secure environment for cryptographic algorithms, but they are also interesting for ubicomp technology because they are a cheap, small and disposable computer with security tokens.

5.0.2 Memory cards vs processor cards: Memory cards are just a container for data, usually with access control for parts of the memory. They are cheap (around 1 euro) but not truly smart. Processor cards on the other hand have an internal microprocessor and RAM. They optionally contain a true random generator or hardware crypto-functionality. Processor cards cost 1 - 20 euros.

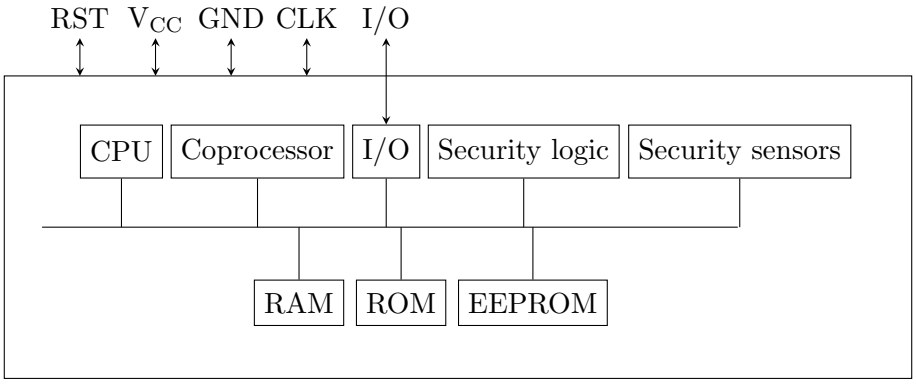

Figure 6: Processor Card

5.0.3 Random number generation (RNG): There are two types of RNGs:

- Pseudo random numbers are typically generated based on some logical CPU states that are incremented by a clock or a crypto-algorithm such as DES.
- True random number generators exploit physical characteristics (i.e. noise).

5.0.4 Communication with the card: Communication between the card reader and the smart card is always initiated by the reader. The card gets Vcc and CLK and does a "reset". Within a few ms, it sends back an "answer to reset" (ATR) containing basic information about the card. Then the terminal sends the first command application protocol data unit (APDU) to the card and the card answers with a response APDU. Encryption and authentication is possible, but slows down the communication by a factor of 4.

5.0.5 Subscriber identity module (SIM): The SIM is the security module for accessing the mobile phone network.

5.0.6 Contact-less smart cards: These smart cards use an external energy source like RFID does. They are more expensive but have better security compared to RFID tags.

5.0.1 *The secret data inside the card must never leave the card and computations must not be observable from the outside.*

5.0.7 Entity authentication:

- Internal authentification: The terminal verifies the card by sending a random number to the card to be hashed/encrypted using a key. The card provides the hash/ciphertext, with that the terminal knows that the card is authentic.
- External authentification: The card verifies the terminal for which the terminal first asks for a challenge which the card provides. The card can then analyze the response to know that the terminal is authentic.
- Card holder authentification: The terminal asks the user to provide the password and sends it to the card for verification.

5.1 Smart Card Components

5.1.1 Smart card hardware: The typical hardware has cheap classical 8 bit and 16 bit processors, a memory management unit (MMU) necessary for multi-application smart cards and 1 - 10 MHz externally supplied power.

5.1.2 Smart card operating system: The typical operating systems is smaller than 100 kB and very simple with no user interface, no external devices, no interrupts and no multi-programming but security is of prime importance. It is highly dependent on the hardware. Access to the operating system functions via an API.

5.1.3 Smart card instructions: There exist several standards that define instructions. Some examples of instruction types are file operations (select, read, write, seek, ...), security (authentication and encryption), application specific operations (e.g. instructions for an electronic purse) and operations for testing.

5.1.4 Smart card file system: Smart cards use a hierarchical file system in EEPROM. There has to be support for different types of files and several types of access control, as well as file access commands like create, delete, write, read, append, lock, invalidate and seek.

5.2 Attacks

5.2.1 Attack classification: There are three kinds of attackers:

- Clever outsiders: they use existing weaknesses in systems
- Knowledgeable insiders: they have access to highly sophisticated tools
- Funded organizations: they have virtually unlimited resources

5.2.2 Leakage: Power consumption, heat, electromagnetic emissions, timing and faulty outputs are all side-channel information that get leaked and can be used in attacks.

5.2.3 Simple attacks:

- Clock bursts: momentarily cause a rapid increase in the clock frequency, this causes instructions to be skipped
- Voltage glitch: momentarily cause a drop in voltage, this causes instructions to be decoded incorrectly
- Acid hacking: gain access to ROM by physically gaining access to see the bits. One could then simply read out from the memory. Another possible use is the manipulation of the random generator so that it always yields the same number. Again another use is to set the bit of an unknown secret key to 0 or 1, the application will then typically return a parity error if the guess was incorrect.

5.2.4 More advanced attacks:

- Power analysis attack: The attacker measures the power consumption to learn the bits of the secret key. When no special counter-measures are taken, this is applicable for almost all crypto-algorithms and smart cards.
- Hamming weight leakage: The attacker learns the number of 1s in each of the seven 8-bit words of the secret key by using an electromagnetic probe. This reduces the brute-force search space from 2^{56} to 2^{40}. (That is a factor of 65'536.)
- Timing attack: Because there is code that is only executed when the bit is 1, the operation will take a bit longer in that case. From this information the attacker can also learn the bits of the secret key.

5.3 Counter-measures

5.3.1 Hardware counter-measures:

- Balance/equalize power consumption
- Increase noise
- Vary the execution time of instructions
- Randomly modify the internal clock speed

5.3.2 Software counter-measures:

- Add random instructions to desynchronize
- Don't let the timing depend on the data or the key

- Limit the number of times an algorithm can be executed

5.3.3 General counter-measures:

- Scramble the data bus and memory cells/addresses differently for each chip
- Use dual logic where 10 = low and 01 = high. They always consume the same amount of power.
- Use a dual CPU where the same operation is performed on two CPUs and then compared.
- Use checksums on memory content.
- Encrypt the memory content
- Encrypt/decrypt the data on the bus with dynamic random keys.
- Use shielding and protection layers

5.3.4 Active hardware counter-measures:

- Use sensors reacting to light, temperature sensors against increased clock rates and resistance/capacity sensors to detect removal of the chips protection layers.
- Watch the current and clock-frequency to detect hardware attacks.
- Do functional tests of parts of the chip.
- Overwrite critical parts of the EEPROM when an attack is suspected.
- Coat the chip with random particles with a high dielectric constant. An array of capacitive sensors detects those properties and uses them as secret random information.

6 Establishing Connectivity

6.0.1 How to connect UbiComp functionality?: We can connect on three levels: on the physical and medium access layer via low-power wireless, on the network level via internet of things (IoT) and on the application layer via web of things (WoT).

6.1 Low-Power Wireless

6.1.1 Wireless communication:

6.1.1.1 Wireless communication benefits:

- Supports mobility
- Less infrastructure

6.1.1.2 Wireless communication drawbacks:

- Typically lower transmission rates
- Restrictive regulation of resources
- Lower security

- Higher loss rates
- Higher power consumption

6.1.2 Energy harvesting: We can harvest power directly from switching events. A spring in a switch outputs enough energy to transmit three identification messages. Other sources of energy include wrist-watches, photovoltaic, piezoelectricity, pyroelectricity, atmospheric pressure changes and other ambient radiation.

6.1.3 Wi-Fi (802.11): Wi-Fi is a power-consuming communication system, therefore there is no wide adaptation in the sensor network and IoT space. Instead they rely on 802.15.4 (a standard for low-rate WPANs) and bluetooth low energy (BLE).

6.1.4 Passive Wi-Fi: Passive Wi-Fi uses backscatter communication to generate up to 11 Mbit/s transmissions and has 3-4 orders of magnitude lower energy consumption. It works by offloading RF componenets to a single plugged-in device in the network, creating a single-frequency tone. Passive Wi-Fi devices communicate by reflecting this tone via a digital switch. Those transmissions can be decoded by all devices within a Wi-Fi chipset. The range is typically 10-100 m.

6.1.5 Interscatter: Interscatter describes the modulation of the reflection of a BLE packet to generate a Wi-Fi packet.

6.1.6 Ultra-low-power communication: The core idea is to exploit energy asymmetries. Every sensor node has very little power but there is a sink node with lots of power.

6.1.6.1 Low-power listening (LPL): Receivers periodically wake up to sample the wireless channel to detect activity from the sender.

6.1.6.2 Low-power probing (LPP): Receivers periodically wake up and send probes and go back to sleep after a short amount of time. The sender listens for probes and sends the payload immediately after receiving one.

6.1.7 Multiplexing: The goal here is to make best use of the precious shared wireless medium.

6.1.7.1 Space division mutltiple access (SDMA): Here we segment space into cells/sectors. We use the same frequencies in different cells. The advantage is its simplicity. The disadvantages are the needed infrastructure investment and handover management.

6.1.7.2 Frequency division multiple access (FDMA): Here we separate the spectrum into smaller frequency bands and allocate one band per channel. The advantage is that there is no need for co-ordination. The disadvantages are the possible waste of bandwidth and its inflexibility.

6.1.7.3 Time division multiple access (TDMA): Here one channel gets the entire spectrum but only for a short period of time. The advantages are that we use only one carrier at at time and that there is higher throughput possible. The disadvantage is the precise synchronization that is needed.

6.1.7.4 Combination of FDMA + TDMA (+ SDMA): A combination has the advantages that it is more robust against selective interference and has better eavesdrop resistance. The disadvantage is the precise synchronization that is needed.

6.1.7.5 Code division multiple access (CDMA): Here we take a narrowband signal and spread it over the available spectrum. All channels then use the same spectrum

simultaneously and statistical methods are used to disentangle the signals. Each channel has a unique code. In DS-CDMA the code is used to chip the signal into smaller pieces, while in FH-CDMA the code is used as a hopping pattern between frequencies. The advantages here are its bandwidth efficiency, that no synchronization is needed and its robustness against interference and eavesdropping. The disadvantage is that more complex signal filtering is needed for decoding the signals.

6.1.8 Low-power wide area network (LPWAN): We want long range, a low number of base stations, a low data rate, low battery and low subscription costs. Examples of LPWAN providers are SigFox and LoRa.

6.2 Bluetooth

6.2.1 Bluetooth: Bluetooth is intended as a WLAN replacement in personal area networks. It is much smaller, cheaper and needs less power, but only has a short range (∼10 m) and up to 720 kb/s. It also needs a complex communication stack to support voice and data as well as bluetooth profiles for different device functions.

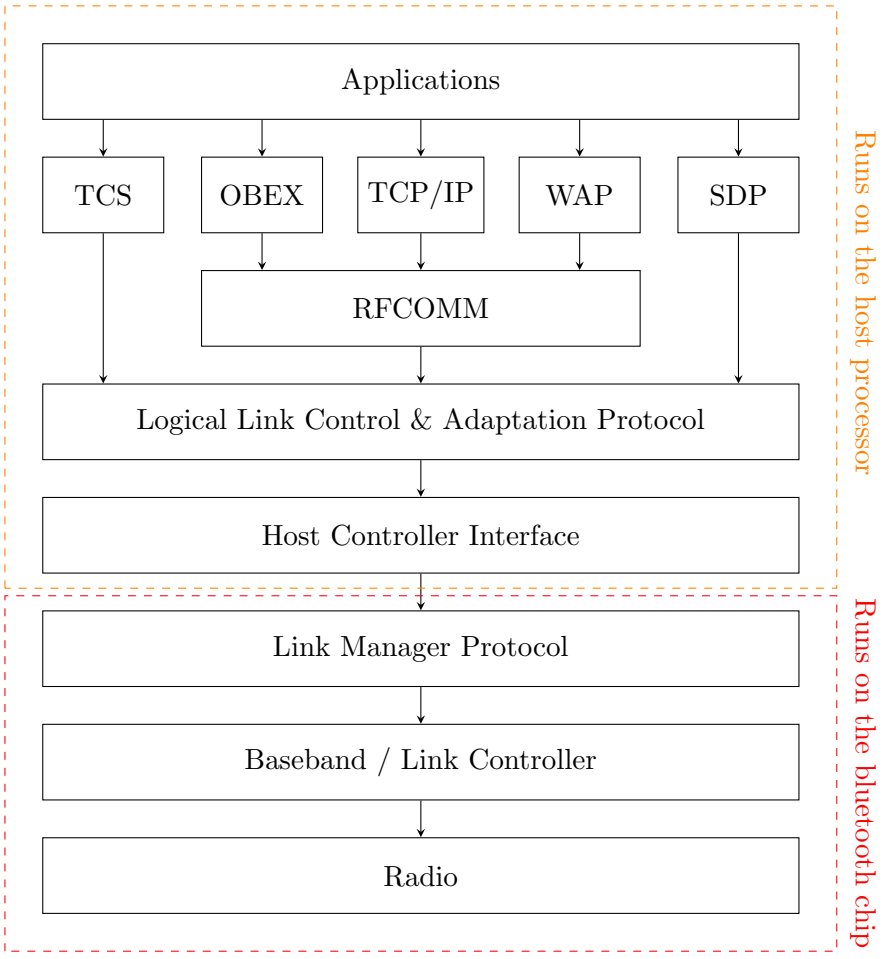

Figure 7: Classic Bluetooth protocol stack

6.2.2 Frequency hopping on the radio layer: If a collision occurs, a packet is retransmitted on a different channel. The specific hopping pattern is not known to outsiders. A common hopping sequence for all cooperating devices is determined by the baseband layer. There are about 1600 hops/s.

6.2.3 Baseband:

6.2.3.1 Addressing: Each bluetooth device has a 48 bit device ID. There is a 3 bit active member address (AMA) when it is active in a piconet and an 8 bit parked member address (PMA) when it is not active. A piconet consists of bluetooth units sharing a single frequency-hopping channel. A single master connects to a maximum of 7 slaves due to the 3 bit address. Communication is point-to-point master-slave or multicast from the master to all of its slaves.

6.2.3.2 Connection states: There are 7 different states:

- Standby: not participating in a piconet
- Inquiry: learn about identity of other devices around
- Page: invitation to a known device to join
- Active: full power mode, listening to all packets
- Sniff: low power mode, wakes up every x ms to check
- Park: low power mode, only listens to sync beacons, not used anymore
- Hold: low power mode, master puts device on hold, slave returns automatically

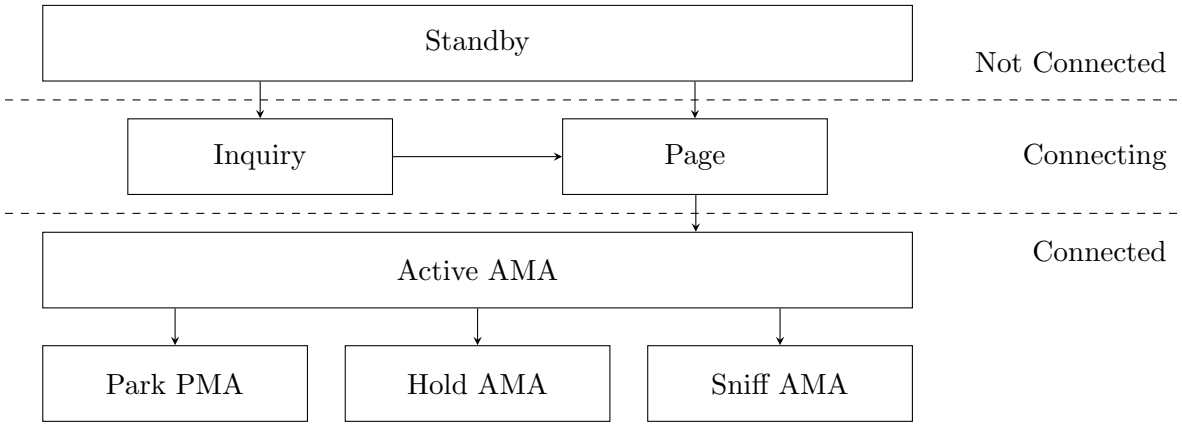

Figure 8: Baseband Connection States

6.2.3.3 Packet Format: 72 bits access code, 54 bits header, 0-2745 bits payload

6.2.3.4 Error Handling:

- Automatic repeat request (ARQ): If the sender does not receive a 1-bit ACK before the timeout, it usually re-transmits the packet until it receives the ACK or exceeds a predefined number of retransmissions.
- Forward error correction (FEC): The sender encodes the message in a redundant way by using an error-correcting code (ECC). This reduces the number of repeat requests but adds overhead.

6.2.4 Link manager: The link manager manages the piconet, authentication (only accept connections from trusted devices), switching of master/slave roles and the tearing down of connections when slaves leave. It also handles the low power modes. Active voice mode uses around 10 mA, active data mode uses around 6 mA and hold/park mode only 60 μA. For comparison bluetooth low energy has a 1 μA average.

6.2.5 Logical link control & adaptation protocol (L2CAP): L2CAP adapts the upper layer protocols to the baseband. It handles the segmentation and reassembly of the upper layer protocol packets and the protocol multiplexing over a single air interface.

6.2.6 Radio frequency communication (RFCOMM): RFCOMM emulates a serial port and thus allows multiple "ports" over a single bluetooth channel. This enables TCP/IP and roughly the same service and reliability guarantees as TCP.

6.2.7 Bluetooth low energy (BLE): BLE has up to 260 Kbps data rate and only sends occasional updates of sensor values. It does not have voice support, has fewer but broader channels, has a faster connection setup and the modulation scheme is optimized for low power usage.

6.2.8 Generic attribute profile (GATT): GATT is the BLE application-layer protocol that reads and writes remote variables, the length of which typically ranges between 20 and 40 bytes. Related characteristics are grouped into services (based on GATT) like "Device information service", "Heart rate profile", etc. The central device is the GATT client while the peripheral devices are GATT servers. Peripheral-peripheral communication is possible through abstractions managed by the central device.

6.2.9 IPv6-based LPWANs: These want direct end-to-end internet integration of resource-constrained embedded devices. Edge routers are used to connect the LoWPAN to the IP infrastructure. An example provider is 6LoWPAN, which transports IPv6 packets over BLE while recognizing and implementing BLE's limits on protocol overhead. A border router connects LWPANs to IP infrastructure, performs (de-)compression and disseminates routing information.

6.3 Internet of Things

6.3.1 Transmission control protocol (TCP): TCP establishes connectivity between processes.

6.3.1.1 Three-way handshake: SYN, SYN-ACK, ACK

6.3.1.2 Sequence number and ack number: These numbers enable the in-order delivery of packets

6.3.1.3 Window: Windows are the limit on packets that can be "in flight" simultaneously

6.3.1.4 Flow control: Flow control makes sure that networks are not overloaded. AIMD is the classic flow control implementation.

6.3.2 User datagram protocol (UDP): UDP is used by applications that do not require the reliability of TCP. It is much more leightweight as there is no connection setup and little overhead.

6.3.3 Representational state transfer (REST): REST provides architectural guidelines for computing infrastructure, including the web. It is a resource-oriented architecture (ROA), meaning that the functionality is integrated into resources, not offered by services.

6.3.4 REST Constraints: REST defines 6 architectural constraints which make any web service a true RESTful API.

6.3.4.1 Uniform interface: You must decide the APIs interface for resources inside the system which are exposed to the API consumers and follow it religiously. A resource in the system should have only one logical URI and that should provide a way to fetch related or additional data.

6.3.4.2 Client-Server: The client application and server application must be able to evolve separately without any dependency on each other. A client should know only resource URIs and thats all.

6.3.4.3 Stateless: All client-server interaction are stateless. The server will not store anything about the latest HTTP request a client made but will treat each and every request as new.

6.3.4.4 Cacheable: Caching shall be applied to resources when applicable and then these resources must declare themselves cacheable. Caching can be implemented on the server or client side.

6.3.4.5 Layered system: REST allows you to use a layered system architecture where you deploy the APIs on server A, and store data on server B and authenticate requests in Server C, for example. A client cannot ordinarily tell whether it is connected directly to the end server, or to an intermediary along the way.

6.3.4.6 Code on demand (optional): When you need to, you are free to return executable code to support a part of your application e.g. clients may call your API to get a UI widget rendering code.

6.3.1 *In REST, there is state in resources and in the client, but not in the transaction. This enables that a series of interactions by a client can be handled by different servers.*

6.3.5 Web resources: A web resource is "anything that you want to talk about", like products, categories, customers, shopping carts, etc. but also client state transitions like next links and paged results.

6.3.2 *In HTTP, verbs stay polymorphic, i.e. we use GET for all types of resources. In contrast RPC-style WS*-web services define operations specific for object types.*

6.3.6 Shared representation model: Every web browser can access every web resource because HTTP works the same for every resource. Interacting with the resource is possible without knowing it beforehand. The representations that are exchanged depend on a shared representation model.

6.3.7 Resource representations: Resources are abstract entities, interaction with resources happens via resource representations. Representation formats can be negotiated between peers and it is communicated which kind of representation is used. When you access a web resource, you see one of its representations your browser negotiates for you. Resource representations contain links to identified resources. Servers guide interactions by providing links. Links are possible state transitions of the client/server application.

6.4 Web of Things

6.4.1 IoT vs WoT: IoT describes the global network of physical objects that communicate using the internet protocol. WoT refers to a specific part of the WWW where physical entities are identified by URLs and interlinked by hyperlinks.

6.4.2 Hypermedia as the engine of application state (HATEOAS): With HATEOAS, a machine API needs no syntactic documentation. Making full use of the WoT (including HATEOAS) for devices and services facilitates the autonomous usage of their interface by machine clients and the creation of flexible mashups across services by different providers. HATEOAS makes systems flexible and robust by decoupling clients and servers as clients discover state transitions at runtime.

6.4.3 HTTP: HTTP is a text-based protocol. HTTP requests indicate the action to be performed and what type of response the client will accept. The advantages are that it is understandable and debuggable. The disadvantage is that it is not very efficient.

6.4.4 The constrained application protocol (CoAP): CoAP is an alternative to HTTP, targeted to constrained nodes and networks. Constrained nodes can be sensors with limited memory and processing power and constrained networks can be slow, unreliable and intermittent. CoAP is optimized for bandwidth and processing efficiency. It is based on UDP and has lightweight security. In CoAP, the client can send an observe to the server, then it will get notifications about resource state changes. There also exists support for multicast. Security in CoAP emulates a 3-way handshake. For low-power devices there is still ongoing work.

6.4.4.1 Message types: There are four message types in CoAP:

- Confirmable (CON): reliable message with retransmission
- Non-Confirmable (NON): best effort transmission
- Acknowledgement (ACK): confirms a CON message
- Reset (RST): used when CON or NON cannot be processed

CONs retransmit after 2-3 seconds. The timeout is doubled after each retransmission. Retransmissions stop when an ACK arrives or after 4 retransmissions failed. CONs and ACKs are matched through the message ID (MID).

7 Location

7.0.1 *Location information is used for positioning, navigation and routing, logistics and location-based services.*

7.0.1 Location models: There are two location models: the geometric model based on coordinate systems and the symbolic model based on names.

7.0.2 Concept of proximity: Co-located objects are objects located in the same environment that can communicate through a physical channel and have correlated sensor readings. This is an important concept in practice, because if something is close it is likely to be in the same place.

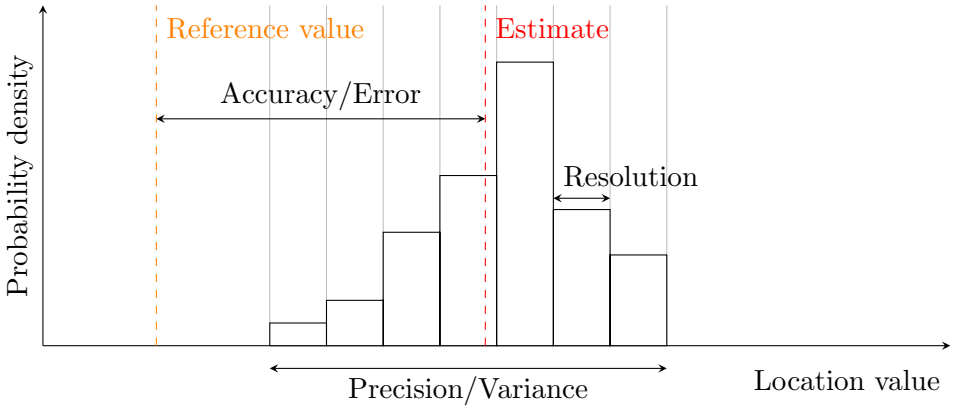

Figure 9: Location Terms

7.0.3 Characterization of location technologies: When choosing a technology, different aspects may be more or less relevant, like cost, accuracy, scalability, indoor/outdoor, private/public and active/passive.

- Tagged (locate a marker) vs. untagged (e.g. vision-based object recognition)
- Positioning vs. containment (e.g. check if inside/outside)
- Relative positioning vs. absolute positioning
- Self-positioning (object knows its position) vs. remote positioning (environment knows objects position)

7.1 Relative and absolute positioning

7.1.1 Relative positioning: We can compute the distance from the previous position by the distance itself (odometer), the velocity (speedometer), the acceleration and the height (barometer).

7.1.2 Absolute Positioning:

- Triangulation: measure the angles to the object from known points at either end of a fixed baseline
- Trilateration: measure the distance from the object to three reference points
- Multilateration: compare relative distances

7.1.3 Angle of arrival (AOA): Uses triangulation, used in VHF ominidirectional range (VOR) for aviation and in the global system for mobile communications (GSM) sector.

7.1.4 Time of arrival (TOA): Uses trilateration, measures the delay between sending and receiving. When using one-way time synchronization is needed, when using round-trip time no synchronization is needed. Used in global positioning system (GPS) and radar.

7.1.5 Time difference of arrival (TDOA): Uses multilateration, three stations compare time difference of signal arrival. Synchronization between stations is required. For the object to learn its own position, the three stations simultaneously emit a signal and the object measures the time difference of their arrival. Because it knows the position of the three reference points, it can learn its own position. Used in mobile phones.

7.2 Location Systems

7.2.1 Global navigation satellite systems (GNSSs):

- Global positioning system (GPS): US project, 31 satellites total
- GLONASS: russian version, 24 satellites total
- Beidon/COMPASS: chinese version, 33 satellites total
- European galileo system: european version, 22 satellites

7.2.2 Assisted GPS (A-GPS): A-GPS uses additional data for the GPS receiver through the mobile phone network. This leads to a reduced time to first fix, higher sensitivity for reception of weak satellite signals, reduced power consuption and higher accuracy.

7.2.3 Positioning via WiFi: Positioning via a database of WiFi access points works particularly in urban areas. It has an accuracy of 15-30 meters.

7.2.4 Indoor positioning systems: These are all positioning systems with dedicated infrastructures:

- Infrared-based systems: these are accurate, have a room-level granularity but are limited by line of sight
- RF beacons: these have cell-level granularity
- Ultrasound: these include TOA and TDOA, have an accuracy of a few cm but scale poorly
- Ultra wide band (UWB): these use four reference stations and have an accuracy of around 20 cm
- Others like magnetic and optical systems, these are often targeted at specialized applications

7.2.5 Location APIs: Location APIs contain support for GPS and mobile/wireless network infrastructure location info, support for periodic location updates/proximity alerts, reverse geocoding (coordinates to address) and forward geocoding (address to coordinates).

8 Societal Implications

8.0.1 Nudging: Nudging is a mild and more accepted version of paternalism.

8.0.2 Relevant technological development:

- Computer vision: recognizing objects, situations, people, etc.
- Artificial intelligence: smart/autonomous systems, self-driving cars, etc.
- Wearable computing: components are distributed over the body and in clothes. They acquire context data and augment the users view of the environment. They have a hands free, intuitive user interface.
- Augmented reality: providing context information, intuitive interfaces, etc.

8.0.3 Hybrid products: Hybrid products are physical items together with an added value provided by embedded ICT. They provide the user with a wealth of background information. The device is sold together with a service which makes it more difficult to imitate.

8.0.4 New business opportunities: Tasks that could not be monitored can now be measured, controlled, managed and priced using embedded sensors and wireless feedback. We can measure the usage of a product or a service and then pay per use. Possible effects are more efficient markets, fairer prices, more adequate supply and better utilization of resources but also more stress for the consumer.

8.0.5 Social risks: Social risks include smart things that may behave unexpectedly, self-determination, increased dependability and privacy concerns.

9 Economical Aspects

9.0.1 Servitization: Servitization defines the departure from just producing physical goods towards a combination of physical goods and services. The desired continued economic sutainability (market pull) and technological innovation (technology push) drive servitization through digitalization. Because there is a large "installed base" and there are usually higher margins in the service business, there is an economic incentive to shift to aftermarket services.

9.0.2 Risk and drawbacks:

9.0.2.1 Risks for service providers: Risks include erosion of economics of scale, availability is king thus penalty clauses directly impact profitability, the temptation to be too ambitious with promises and that the promises to the customers might require additional resources.

9.0.2.2 Risks for customers: Risks include the product/ecosystem lock-in and no legal ownership of the product means there are constraints on the own operations.

	Technology push	Market pull
Sense	New sensor technologies	Necessary to understand own products performance and cost
Connect	New communication technologies	Necessary to ship this data to back end
Analyze	New methods to acquire and process large amounts of data	Necessary to react fast to malfunctions or better forecast them
Control	New materials and softwareization	Even better to upgrade products remotely
Integrate	New architecures/infrastructures to integrate services	Products and services need to be flexible and future-proof

Table 1: Technological push and market pull

9.0.3 High-resolution management: The goal is to support management tasks like planning, leadership and controlling with automated data collection. This also means that digital business model patterns are becoming relevant to physical industries for the first time.

9.0.1 *Traditionally information is not defined and is expected to be free of charge. The IoT business model sees information as a major source for value in the IoT.*

9.0.4 New business model patterns:

- Freemium: A product or service (typically a digital offering or an application such as software, media, games or web services) is provided free of charge, but money is charged for additional features, services, or virtual or physical goods. Examples are LinkedIn, Tinder and Dropbox.
- Digital add-on: Sell asset very inexpensively but customers can purchase higher-margin digital services. Invite third parties to sell add-ons as well. Examples include hardware add-ons like RAM sticks and software add-ons like additional language support.
- Digital lock-in: Limit the product compatibility to prevent counterfeits and ensure warranty. Customers are locked into a vendors world of products and services. Switching to another vendor is not possible without exposing yourself to substantial additional costs. Hence, this strategy protects the company from losing customers to competitors. Examples are Kindle, Gillette and Canon.
- Product as point-of-sales: The product itself takes on a marketing/sales role. An example is a smartphone on which one can then buy apps through the app store.
- Object self-service: The products are smart items that place orders on the internet themselves. One example is Amazons Alexa.