Ubiquitous Computing Spring 2013

Dominic Langenegger

August 20, 2013

1 The vision of Ubiquitous Computing

Vision is increasing number of further shrinking devices per person. A path to the **Internet of Things**. Possible to have information everywhere and always because of cheaper, smaller hardware with wireless communication at almost no cost.

Small, leightweight, cheap, mobiel processors, sensors and wireless communication modules in many everyday objects (embedded computing), embedded in the environment (sensor networks) and on your body (wearable computing).

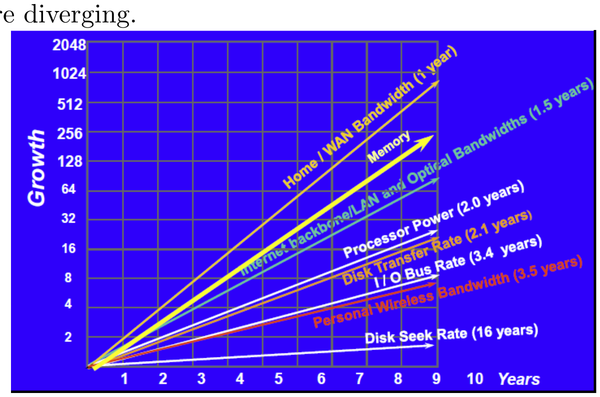
2 Technology trends

2.1 Moore's Law (1965)

> Processing and storage capacity double every 18 months.

Exponential growth/shrinking can also be observed in the size of transistors (down from 10μm 1971 to 22nm 2012), power efficiency, price per computing power, price of RAM and magnetic storage, disk storage density.

In general, the most important technology parameters double every 1-3 years. The problem however is, that the fabrication costs doubled approximately every 4 years. Main drawbacks in future technology are that Moore's Law does not apply to all technologies (e.g. batteries) and especially that the exponent of growth (growth factor) is not equal for all technologies and therefore diverging.



Examples of divergences are:

- Processor-Memory performance gap (RAM to slow)
- Battery-Computing Power (batteries way to low on capacity)

2.2 Limits of Growth

The predictions for the future see a limit and a clear end to Moore's Law. It is very likely that alternative technologies must be explored to further increase technology power. (i.e. Molecular-, Organic-, Quantum-level and others)

The 5 technical drivers of Ubiquitous Vomputing are:

Moore's Law
Increasing computing power and decreasing device size.

New Materials
e. g. semiconudctors, fibers, flexible substrates (displays etc.), E-Ink

Progress in Communication Technologies
Fiber optics, wireless (NFC, RFID, Bluetooth, LTE), opportunistic carriers (powerline, body area networks)

New Architectural and Software Concepts
like Spontaneous Networking (e.g. Universal Plug and Play UPnP)

Better Sensors
Miniaturized cameras, microphones, biometric sensors, location sensors, passive radio frequency (RF) sensors (use piezoelectric and pyroelectric materials), RFID

3 Radio Frequency Identification (RFID)

Identify objects from distance to associate specific actions or attributes with the object or authenticate it. (or a person)

Uses RF-transponder (Transmitter-responder) and wireless energy supply by induction or electromagnetic field with range of up to 10 m. Small amounts of data (up to about 100 bytes) can be stored using ROM (Read Only Memory) or EEPROM (Electronically Erasable Programmable ROM) and chips are very cheap and therefore disposable.

Medium range features include collision detection (typically 30 items/s) and read-write memory (EEPROM, SRAM). High end features are complex functions like cryptography used in smartcards.

RFID systems are typically classified based on different features:

- Power Supply
- Operation Frequency
- Communication, Coding and Modulation
- Anti-Collision Protocols
- Memory Structure and Data Access

3.1 Power Supply & Operation Frequency

Tag need energy to power microchip and transmit data back to reader. Passive tags have no internal battery and entirely use energy transmitted by reader while active RFID tags contain an internal battery which increases range (up to 100m) and lowers environmental influences (no interference with metal, liquids etc.) while coming at a higher price and bigger size.

There exist two coupling methods for wireless energy supply:

Inductive Coupling (magnetic field)
Magnetic field generated by reader induces voltage in the coil of the transponder. Frequencies typically $100 - 135kHz$ (LF) or $13.56MHz$ (HF). Works in the near field for low power usage. Note that EEPROM needs much more energy than ROM.

Electromagnetic Coupling
Coupling in the far-field on $868, 915MHz$ (UHF) and $2.4Ghz$ (micro wave)

The magnetic **near field** is an energy storage field of strength $\mathcal{O}(\frac{1}{r^3})$ while the electromagnetic **far field** is an energy propagating field of strenght $\mathcal{O}(\frac{1}{r})$. The boundary lies at $\frac{\lambda}{2\pi}$ where their amplitude is equal. Some values are 5 m at 10 MHz and 5 cm at 1 GHz. Typically RFID operates in the near field.

3.2 Communication Principles

The reader may periodically turn of its field to allow transponders to send in-between. However this needs a capacitor on transponders to store energy.

3.2.1 Encoding Schemes

NRZ 1 = high, 0 = low
Manchester Coding 1 = low-to-high transition, 0 = high-to-low (IEEE 802.3 or reverse for old convention)
Pulse Pause Coding (PPC) 1 = short period to next pause, 0 = long period (similar to morse code)

3.2.2 Data Transfer

Typically Amplitude Shift Keying (ASK) on the reader's field used to send from reader to the tag.

From the tag to the reader there are several common principles:

Capacitive Coupling very short distance (mms), electrical field
Load Modulation near distance magnetic field, resistor generates sub-carrier subject to modulation (ASK, FSK, PSK)
Backscatter long range, electromagnetic field, reflection of high frequency signal (like radar) with change of reflection properties by resistor in parallel to transponder antenna

3.3 Collision Problem

Broadcast of reader leads to many simultaneous replies which interfere. While a transponder typically can't hear signals from other transponders, they still should have exclusive access to a shared channel during a short period of time. Therefore collision detection and avoidance have to happen at reader and be fast and reliable.

FDMA
channels limited, expensive readers, however possible for small, fixed number of transponder

TDMA (stochastic)
ALOHA random re-sends → bad because optimum throughput at only 18% occupation
Slotted ALOHA maximum throughput 37% when only sending at well-defined slots with additional syncing by reader
Adaptive Rounds Slot count dynamically altered based on load
Reservation ALOHA Competition phase using ALOHA and phase with reserved slot transmission (no collision). However causes extra delays

3.3.1 Capture Effect

Throughput improves if transponders closer to the reader. They win because of their stronger signal because a weaker one may not be strong enough to cause interference. **Weak Collisions** can occur if this leads to collision going unnoticed.

3.3.2 Tree Walking Anti-Collision

With manchester encoding, collisions can be located if two different signals differ in the same bit. (Leads to illegal high during whole bit period)

Algorithm 1: Tree Walking Cnti-Collision Algorithm

```
Data: Set T with transponders
Result: t ∈ T that can send collision free
Broadcasts "sync";
while no collision detected do
    Request ID of all t ∈ T;
    Determine leftmost bit b that yields a collision;
    if No collision then
        break;
    end
    Broadcast "mute all with v(b) = 0";
    All t ∈ T with v_t(b) = 1 proceed to next round;
end
Request data from unique x ∈ T;
Send "halt" to x: won't compete until next "sync";
move up tree and repeat;
```

This is an example of a deterministic TDMA approach (in contrast to the stochastic ones introduced above)

3.4 Data Access

There exist factory programmed read-only tags and read-write tags with a unique ID plus some additional read-write memory. The latter usually has way worse performance for writing than reading. In special cases RFID can also be used with structured memory and access security features.

3.5 Application-Driven Selection Criteria

For the needs of a particular application a system is chosen based on the following criteria:

Read Range Antennas, environment, data rate, frequency and transmission power; whereas the latter 3 typically are regulated and standardized.

Data Transfer and Detection Rates Low and High Frequency about 5 kb/s and UHF 50 kb/s. Detection rate (time to identify tag) depends on transfer rate, length of tag ID, anti-collision algorithm (typically between 20 (LF,HF) and 300 (UHF) tags per second)

Suspectivility to Noise and other Error Sources Interference, collisions, absorption, tag misalignment and detuning

Cost depends on size and complexity of chip; production volume and technology; antennas and assembly

Tag Form Factors Size and form

	LF	HF	UHF	MW
Type of coupling	Near-field (inductive)		Far-field (electromagnetic wave)	
Typical frequency	134.2 kHz	13.56 MHz	868 MHz (EU) 915 MHz (US)	2.45 GHz
Typical read-range	~ 1.5 m	~ 1.0 m	Passive: < 3 m (0.4 W transmission power of the reader), < 5 m (2 W), < 10 m (4 W) Active tags: ~ 100 m	
Typical data-rate	5 kb/s (ISO 15693/14223)		50 kb/s (ISO 18000, Part 6, Mode A)	
Detection-rate	10-30 tags/s		100-500 tags/s	
Environmental influences	- Shielding - Conductive materials (e.g. metal)		Shielding, Absorption, Reflection, Refraction (metal, liquids)	
Collocated tags	Antenna detuning of closely located tags		Distortion of radio patterns due to antenna coupling	

3.6 RFID vs. Barcodes

No line of sight required, longer identification range, more data, (nearly) simultaneous reading, write and delete access, fraud difficult. However comes at higher cost and is unreliable under certain conditions.

3.7 RFID Future

Highest potential currently seen in retail (10000 billion $ per year), postal services (650), books 50 and drugs 30. RFID is subject to continuous adoptions due to Government regulations (e.g. animal identification, biometric passports), industry leaders adopting their standards, and cost of RFID equipment.

3.7.1 Electronic Product Code

To identify single object instances rather than whole object classes. Decouple identity from data and only store the EPC on the RFID tag and all additional information in external databases. The goal is to replace the wide spread 13-digit EAN 13 bar codes (European Article Number) with 96 bit EPC RFID tags.

Standardized interfaces and data formats enable cross enterprise business processes and decentralized information sharing.

Object Name Service (ONS) is used to resolve EPC to URI where the URI points to something that provides more information on the product or that triggers an operation (e.g. web page, EPC information service, WSDL to webservice)

3.8 Reception in Public

Many concerns about privacy and infrastructure. Solutions include kill-feature (deactivate tags at sales point) but this often doesn't satisfy skeptical customers, vendors might want after-sales services and manufaturers want to add additional product functionality.

RFID Kill stations can only change the writable part of the memory and the manufacturer's unique ID in the ROM is not "killable".

3.8.1 Infrastructure Concerns

Include security of data and controlling access, interoperability between various solutions, access to historical data (not only processing current events), cost and complexity of managing, policy issues and more.

3.9 Applications

Electronic Articel Surveillance (EAS) Products in super market (first introduced in 1966)

Ski Ticketing

Debit System, Wireless Payment

Car Immobilizer (Anti-Theft device)

Automatic Toll Collection

E-Ticket and E-Passports

Logistics Real time inventory and product tracking

4 Smart Cards

Portable and secure container for secret data providing a secure execution environment for cryptographic algorithms. Used e. g. in mobile phone subscriber information (SIM), credit and debit cards, public telephony, healthcare and enterprise security (encryption etc.).

Memory Cards Cheap (< 1) but not smart, container for data (usually with PIN access control for parts of the memory), low level of security for use in prepaid cards, loyalty cards and disposable applications

Processor Cards True "smart cards" with internal microprocessor and RAM to perform internal calculations so secret data never leaves card (e.g. private key). Can contain true random generator but has much higher price. Typically up to 256 kB ROM and 128 kB EEPROM.

4.1 Random Number Generation

Pseudo random number is generate based on some logical CPU states (e.g. registers) that are incremented by a clock or a crypto algorithm such as DES.

True random number generator can be in hardware and exploit physical characteristics with varying performance depending on how long it takes to build up a sufficient level of entropy.

4.2 Communication

Communication is initiated by the reader (terminal) as client with the card as server. The communication protocol is half-duplex with typically 9.6 kbit/s (up to 115) and either byte- or block-oriented. Newer generations of smart cards communicate via the USB protocol using two originally unused connections on the chip. This allows speeds of up to 1.5 Mbit/s full duplex.

4.3 Smart Card System

Simple and small (3 – 30 kB) **Operating System** without user interface, interrupts or multiprogramming. Highly dependent on the hardware and primarily optimized for security. Offers API to operating system functions like access to file system, cryptographic functions and I/O. Most important OSes are *JavaCard* and *MULTOS*.

The **File System** is held as a tree in EEPROM allowing different types of files (e.g. fixed vs. variable sized records) and access control. There exist several file access commands for creation, deletion, writing, reading, appending, locking, invalidating and seeking that can then be performed on the card without further request-reply cycles with the client.

4.3.1 JavaCard

JavaCard is a stripped down Java VM on the card which is directly programmable in Java (subset: no threads, cloning, strings, large data types or dynamic class loading) and offers a standardized interface to the card (Java Card API). Applets can be loaded dynamically into the card.

This allows for very easy application development on a high level and increased flexibility because the software can be loaded/replaced at any time. A major disadvantage is however the worse performance, as the execution time is about four times slower than for native code.

Multiple applets are prohibited from interaction with each other by a applet firewall to guarantee security. Only the terminal can select applets to be loaded for execution.

4.4 Subscriber Identity Module (SIM)

SIM is a security module for accessing mobile phone networks to enable separation of phone and service marketing. It is currently the largest market for smart cards and the execution platform for mobile applications.

Used to store unique **International Mobile Subscriber Identity** (IMSI), encryption key, current location, service provider, preferred language and other relevant information.

4.5 Contact-less Smart Cards

As described in ISO 14443, smart cards using external energy sources similar to RFID with the capability for contact-less interaction do exist. They have a range of a few centimeters, are more expensive and provide improved security compared to RFID tags because they have direct cryptography support.

4.6 Security Issues

With direct hardware access no such thing as 100% security exists. However the price/protection ratio must be considered. While smart cards are relatively secure due to support for terminal, card and user authentication, the right tools can help in breaching security and gaining access to stored data.

This can be achieved by reverse engineering the logic circuits or the ROM content using microscopes and similar equipment. It is even possible to set bits with UV pulses of X rays to specific memory locations. A possible use could be to manipulate the random generator to always yield the same number or manipulate the DES algorithm.

Simple attacks include forcing glitches by clock bursts (rapid increase in clock frequency) or voltage glitches to learn secret keys or bypass security checks. More sophisticated attacks try to retrieve keys by side-channel information like power consumption, heat and timing during encryption. This type of attacks is applicable for almost all crypto algorithms and smart cards with simple requirements of a digital oscilloscope, a smart card reader and a PC.

4.6.1 Countermeasures

There exist **hardware** countermeasures to power and timing analysis like reducing and balancing power consumption, increasing noise, vary execution time of instructions and randomly modifying internal clock speed. **Software** countermeasures include adding random instructions to desynchronize, limit number of executions for algorithm and the elimination of all correlation between timing and data or key.

In general this includes scrambling of the data bus and memory cells, checksums on memory contents, encryption of memory content, redundant computing and bus data and the use of dual logic. (10 = low, 01 = high → always uses the same amount of power) **Active Shielding** uses sensors (e.g. reacting to light or increased clock rate, i. e. temperature) and performance analysis to detect a potential attack. If an attack is detected, critical parts of the EEPROM can be overwritten.

5 Wireless short-distance communication[1]

5.1 Comparison to fixed Networks

Wireless networks typically have way higher loss rates due to interference, fading etc. and are restricted to regulations of resources (frequency bands). They typically achieve lower transmission rates and are less secure due to the publicly shared transmission medium. However they have great mobility support and need less infrastructure.

Major challenges of mobility include varying transmission quality, disconnection management, handover, location transparency, service discovery, authentication and security.

5.2 Multiplexing

There are four basic multiplexing methods that are usually combined to achieve a real-world compatible solution:

- Space Division Multiplexing Access
- Frequency Division Multiplexing Access
- Time Division Multiplexing Access
- Code Division Multiplexing Access

In FDMA two versions are commonly distinguished: Fast and Slow Hopping. While in **Fast Hopping** several frequencies per bit are used, **Slow Hopping** sends several bits per frequency.

An example of the combination of TDMA and FDMA is the widely used GSM protocol for mobile phones.

5.3 Bluetooth

Bluetooth 802.15.1 is for short-range (typically up to 10m) medium bandwidth (< 1 Mb/s) data transfers in spontaneously created small networks. It operates in the 2.4 GHz frequency band on 79 channels with 1600 frequency hops per second (625μs intervals).

Two basic modes (baseband link types) exist: One for synchronous, timing critical transmission like voice and one for asynchronous transmissions like data.

Bluetooth devices can form a so called piconet of up to 8 devices with 1 master that determines clock and frequency hopping pattern (based on its device ID). All communication always goes over the master, there is no possibility for direct slave-to-slave communication. Because a slave can participate in multiple piconets at once (but at most in one actively at any time) it is possible to form scatternets of multiple overlapping piconets where slaves in multiple piconets serve as bridges.

The further development of the Bluetooth standards (currently version 3.0) tries to achieve higher data rates with lower power consumption for a cheaper price. Since Bluetooth 2.1 (2007) pairing between devices became much simpler and with Bluetooth 3.0 (2009) WiFi can be used on the physical layer to enable for much higher transfer rates.

5.4 802.15.4

For even smaller, cheaper and less energy consuming communication devices like smart watches, remote controls or sensor networks, IEEE 802.15.4 provides a suitable solution. It is designed to allow building multi-month (or even year) battery life personal area networks with support for latency-critical applications. Nodes can operate in a master-slave fashion or peer-to-peer in mesh networks and transfer data with up to 250 kbit/s. The standard only defines the physical and MAC layer.

ZigBee is an upper layer protocol based in IEEE 802.15.4 that defines the network and application layer and implements mesh topologies using multi-hop and ad hoc on-demand distance vector routing.[2]

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) sends IPv6 packets over 802.15.4 using aditional header compression and packet fragmentation. It supports both mesh-under (link layer) and route-over (IP layer) routing.

6 Location

Geographic location is of interest for mobile devices, people and everyday objects. Location Information can be interesting for positioning, navigating, logistics and location-based (context aware) services. Some examples include emergency services (locate assistance and caller), traffic information, navigation, mapping, weather information.

Commonly the **geometric** and the **symbolic Location Model** are distinguished. While the first is based on a reference coordinate system, only the latter is human-friendly because it uses special topology and is typically hierarchically organized (e.g. postal address). Reverse mapping from the symbolic model to the geometric is however not always unique due to common names.

[1] For more detailed information about wireless network basics and the Bluetooth protocol please consult [1].
[2] http://en.wikipedia.org/wiki/Distance-vector_routing_protocol

6.1 Location Technologies

There exist various different location technologies each approaching different issues like cost, accuracy, scalability, indoor/outdoor, private/public or active/passive.

Important terms for location technologies are Reference Value, Estimate, Resolution, Precision/Variance, Location Value, Probabiliby Density and Accuracy/Error.

While in relative positioning only change is measured (e.g. velocity, acceleration or height), absolute positioning can be more complex:

Triangulation measures angles to reference point
Angle of Arrival (AOA) used in aviation

Trilateration measures distances to reference point
Time of Arrival (TOA) as delay between sending and receiving either one-way (synchronization needed, e.g. in GPS) or round-trip (e.g. Radar).

Multilateration compares relative distances
Time Difference of Arrival (TDOA) e.g. used to locate mobile phone from multiple base stations with known positions

In GSM multiple of these techniques can be used with different accuracy. While the Cell of Origin (COO, Cell identity) has relatively low accuracy, TOA (500 m and TDOA 150m) are relatively accurate. Other methods are AOA and Signal strength comparison with cell shape database (fingerprinting). The combination of multiple methods can give even better results.

6.2 Global Navigation Satellite Systems (GNSS)

GNSS include the famous **Global Positioning System** (GPS) but also its Russian version *GLONASS* and the Chinese brother *COMPASS*. The European Union is currently building its equivalent *Galileo System*.

GNSS use Trilateration in three dimensional space with 3 satellites plus a fourth satellite for clock synchronization in TOA.

To improve accuracy over the typical $5 - 15$m, **Differential GPS** uses fixed reference stations to cancel out some error sources. It is also possible to use pseudo-satellites on ground (so called "Pseudolites") to improve accuracy in difficult terrain or indoors.

Wireless Assisted Satellite Navigation **A-GSP** uses additional data through the mobile phone network. These include but are not limited to cellular network properties, database of WiFi access points, time synchronization and list of visible satellites and their position. (where the latter mainly increases locating speed)

6.3 Indoor Positioning Systems

For indoor positioning a high accuracy can only be achieved by using dedicated infrastructure like:

Infrared-based Systems short range, room-level, limited by line of sight

Radio Frequency bacons cell-level granularity

Ultra Sound TOA, TDOA (synchronize via RF channel) with accuracy of a few cm but very poor scale

Ultra Wide Band Reference stations in corner, up to 20cm accuracy

Magnetic, Optical and others for specialized applications

Nowadays there is often no longer a need for a new dedicated infrastructure because we can used already existing infrastructure like WLAN base stations or phone beacons (DECT). Additionally there is only very small communication overhead when using fingerprinting with existing infrastructure.

6.4 Trends

As always: smaller, cheaper and more accurate...

7 Outlook

7.1 Energy

The capacity of batteries is often measured in **energy per gram** where top notch Lithium-Ion batteries come at about 720 J/g. The efficiency of battery technology is improving only slowly over time while other hardware continuously uses more energy. (However the number of instruction per energy is luckily decreasing due to better power management)

7.2 Augmented Reality

Huge potential with first products appearing on market like Google Glass and various smart phone apps. Augmenting the user's view of the environment by extending his senses and make him more secure and smart. (Human Empowering)

7.3 Economic and Social Impact

Ubiquitous Computing can lead to higher efficiency, more convenience, increased safety and opens many new business opportunities. However there are a lot of critical voices about social and economic value, general user acceptance and privacy. Smart things may behave unexpectedly, humans may no longer have full control and self-determination. Over all not only the smart objects but also mankind increases their dependability on a correct infrastructure and each other.

References

[1] Dominic Langenegger. Advanced computer networks - summary. 2013.