INTERNET OF THINGS – WHITEPAPER

OVERVIEW OF IOT CONNECTIVITY AND PROTOCOLS

A digitizing world in which more and more things are connected is rapidly becoming reality. This is a phenomenon that has been ongoing for the last decades. The IoT hype, the 'always online' culture and internet everywhere has, together with low price electronics, accelerated this process. Industries are aware of this and want to profit from this upcoming (disruptive) industry. The IoT market currently is chaotic. The new technologies and initiatives are rushing to a dynamic market over the coming years. In this paper an overview is provided of today's IoT connectivity and protocols.

The Internet of Things (called IoT) is a topic that is inspiring many people and companies to see endless new opportunities and improvements in both personal lives and in the industry. The term IoT covers a wide range of topics; from complete automated Smart Cities to the simplest heart beat sensor. This makes it difficult to understand what IoT means and how it can be placed into perspective.

The commonly used IoT definition is '*a network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data*'.
The term "Internet of Things" was coined by British entrepreneur Kevin Ashton back in 1999.

Typically, IoT is expected to offer advanced connectivity of devices, systems and services that goes beyond machine-to-machine communications (M2M). It covers a variety of protocols, domains and applications.

The interconnection of the devices will lead to automation in nearly all industries and boundaries between domains will be fading. The network connectivity is key as it allows the "things" to communicate. No connectivity, no IoT. In the market a battle is ongoing to become the de-facto industry standard. Till then new technologies will continue to pop up ….

IoT / M2M difference?

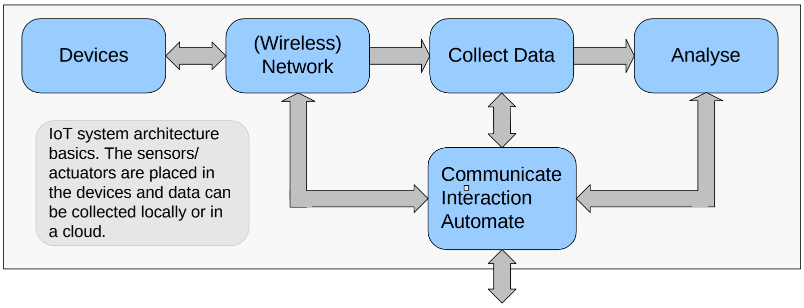
Machine to Machine (M2M) refers to technologies to communicate with other devices of the same type. M2M is a broad term as it does not pinpoint specific wireless or wired networking, information and communications technology. M2M is considered an integral part of the Internet of Things (IoT) and brings several benefits to industry and business in general as it has a wide range of applications such as industrial automation, logistics, Smart Grid, Smart Cities, health, defense etc. mostly for monitoring but also for control purposes. IoT on the other hand connects everything in the physical world, beyond the border of industries.

As a starting point the industry seems to agree on the following critical IoT success factors:

1. Long battery life,
2. Low device costs,
3. Low deployment costs,
4. Low data rate,
5. Support for huge number of devices and
6. Excellent (indoor) network coverage.

The above factors clearly give direction to the development of IoT technology. For example consider LTE technology (as we know it today) in an IoT scenario. One of the showstopper is the high energy consumption (complex LTE) and unneeded high data rates which results in short battery life and high costs. In short it simply offers too much for IoT and needs to be adapted.

The Figure below shows a generic overview of the IoT system architecture. The overview can be intuitively understood by following the data flow.



In the following two Sections an overview is provided of most used protocols and wireless technologies; this describes the (wireless) network as shown in the Figure above.

Wireless network connectivity

The relevant wireless technology standards and initiatives in this paper are discussed from a European perspective. The wired technologies are not in scope of this paper, as the focus is on battery operated wireless devices. Before technologies are described the following important wireless aspects are explained:

Frequency – Determines the radio wavelength. Rule of thumb is that the higher the frequency is the smaller the cell range is and the smaller the antenna can be (important in device form factor). Smaller cells are good for capacity as more capacity is available per surface area. Lower frequencies have a wider range due to propagation characteristics. In this context the term "Sub-1 GHz" is often referred to and means a frequency below 1 GHz.

Licensed / unlicensed spectrum – In the frequency spectrum there are licensed and unlicensed frequencies available. Most of the unlicensed frequencies are ISM frequencies (originally to be used for Industry, Science and Medical purposes other than telecommunications). In the recent years however these frequencies are used for short-range, low power communications standard – e.g. WiFi, Bluetooth, NFC.

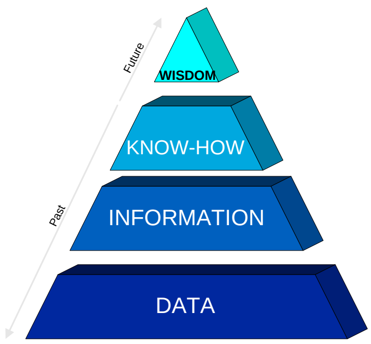
Data rate – Actual data the IoT device needs to transmit / receive per time unit. Industry currently focusses on technology with low data rates (also related to long battery lifetime).

Range and power – As the market wants a battery life of 10 years or more the power consumption must be kept to a minimum. This results in technologies where a trade-off is made between power (less complexity, low data rate) and cell range (lower frequency, sufficient coverage).

The (wireless) network connectivity enables that data is send and received to and from the 'things'. In the IoT world a huge number of things are generating data (Big Data). The data as such is useless and to illustrate this we would like to use the DIKW model. It represents how Data, Information, Know-how and Wisdom are related to each other (see picture on this page).

The network connectivity as described in this paper basically transfers data from A to B – the actual transformation from Data to Information, Know-how and Wisdom is mandatory in IoT networks as Data only adds no value.

- **Data**; Signals from observation and measurements. It is useless due to lack of context and interpretation (know-nothing).
- **Information**; Data is made useful for decisions, it has a meaning and purpose (who, what, where, how many, when) (know-what).
- **Know-How**; Information which is processed, organized and structured in some way or else as being applied or put into action. Normally it contains multiple sources of information over time.
- **Wisdom**; Knowing the right things to do (future), increase efficiency and add value (know-why).



DIKW-model

Obviously the network connectivity layer as described in this paper handles Data only. In the next paper the e2e IoT value chain is described in more details.
In the following sections the IoT technology is summed up with regards to wireless technology (short, medium and long) and protocols.

Short range

The short range wireless technologies considered are capable to reach up to 1000 meter.

NFC

Near Field Communication (NFC) is wireless communication that enable two electronic devices to establish radio data communication with each other by bringing them closer than, typically, 10 cm from each other. It uses the ISM frequency (13.56 MHz) and has a maximum data transfer rate of 424 (kbps). Examples of NFC deployments are: wireless payments systems, identification and access control systems (authentication, authorization) and for tag automation. The short range avoids eavesdropping and reduces other security risks. The NFC technology is often seen as extension or subset of RFID. NFC is nowadays implemented in many smartphones.

RFID

Radio Frequency IDentifier (RFID) technology is used for the purposes of automatically identifying and tracking tags attached to objects. It is based on the wireless usage of electromagnetic fields to transfer data and has a communication range varying from 10 centimeters to a few hundred meters. The range depends on the used tag and reader setup (active / passive combinations). RFID uses frequency ranges from 125 kHz (Low Freq), 13.56 MHz (High Freq) up to 10 GHz (Ultra High Freq). Data rates of 4 kbps for low frequencies up to 640 kbps for UHF.

Some examples of RFID usage: retail product identification (or any object identification), anti-theft tags, access control systems, to track shipping container. Implantable RFIDs for animal tagging (e.g. cats, dogs, cattle) is common practice while tagging via implantable human RFIDs is in an experimental phase.

Bluetooth Smart

Bluetooth Smart (aka Bluetooth Low Energy or BLE) is a wireless PAN technology. Bluetooth Smart technology aims at the IoT market. To reduce energy usage the data rate is reduced while maintaining a similar range (100 meters or more).

It uses the ISM frequency (2.4 GHz) and has a maximum data transfer rate of 1 (Mbps).

Bluetooth (Smart) usage examples are: hands-free car kit, healthcare, fitness, (i)beacons, security and home entertainment industries. Today all latest mobile phones support Bluetooth Smart (i.e. version 4.1)

Beacons

Beacon technology can be seen as small lighthouses enabling Bluetooth devices to broadcast and receive tiny pieces of information within short range. Beacons are based on Bluetooth Smart (4.0). Currently in the market there are 2 beacon technologies available.

- *iBeacon* – proprietary beacon protocol design by Apple based on BLE.
- *Eddystone* - open beacon protocol designed by Google based on BLE. Defined beacon messages format for proximity measurements plus liberty to specify Beacon frames for any applications.

Known beacon examples are: presence detection, retail optimization, anti-lost alarm etc.

ANT(+)

ANT+ is a sub-system of the ANT protocol. It is a proprietary wireless technology with open access. ANT+ is designed to ensure that ANT device data is interoperable (which is not necessarily the case between ANT devices). Conceptually claimed to be similar to Bluetooth Smart, but oriented towards usage with sensors.

ANT(+)uses the 2.4 GHZ ISM frequency. It supports data rate up to 60 kbps and has a communication range of 30 meters.

ANT+ usage examples are: Activity monitors, blood glucose meters, heart rate monitors, light control, temperature sensors.

The ANT+ Alliance is organized by *Dynastream Innovations Inc.*, a subsidiary of Garmin Ltd.

EnOcean

EnOcean is an energy harvesting wireless technology. It generates its energy from slight mechanical motion and other potentials from the environment (e.g. indoor light and temperature differences). This is transformed into usable electrical energy to connect devices. The technology is primarily used in building automation systems.

It uses the sub-1GHz ISM frequency (868 MHz) and has a data rate of 125 kbps. The communication range varies from 30 meters (indoor) to 300 meters (outdoor).

ULE

The Ultra-Low Energy (ULE) is a wireless communication standard (star topology) which is designed to create wireless sensor and actuator networks. It was originated from the DECT technology and also known as DECT ULE. It uses the dedicated 1.8 GHz band and therefore it has no interference from other technologies using the unlicensed ISM frequency (e.g. Bluetooth, Zigbee, Z-wave). ULE handles voice and data simultaneously and has a data rate of up to 1 Mbps. The communication range varies from 70 meters (indoor) to 300 meters (outdoor).

ULE focusses on the Home Automation environment and is used for Home Automation, Home Security and climate control

Z-Wave

The Z-Wave is a wireless communication standard to allow devices to communicate to each other for the purpose of Home Automation.
Z-Wave uses the 868 kHz frequency and has data rates of up to 100 kbps. The communication range varies from 30 meters (indoor) to 100 meters (outdoor).

The Z-Wave usage examples are mainly in the Home Automation area (like motion detector, smoke alarms, door locks etc.)

Digi / XBEE

The company Digi International manufactures a variety of RF solutions. XBee is the brand name for Digi International's family of form factor compatible radio modules. The family of modules consists of a wide variety of radios that support a number of wireless protocols and are certified for worldwide use.

XBee supports the following protocols: 802.15.4, DigiMesh, ZigBee, ZigBee Smart Energy and Wi-Fi.

IEEE 802.15.4

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for Low-Rate Wireless Personal Area Networks (LR-WPANs). It is maintained by the IEEE 802.15 working group and is defined it in 2003. It is the basis for the ZigBee, ISA100.11a, WirelessHART, MiWi and Thread specifications, each of which further extends the standard by developing the *upper layers* which are not defined in IEEE 802.15.4. Alternatively, it can be used with 6LoWPAN and standard Internet protocols to build a wireless embedded Internet.

ZigBee

The ZigBee is a wireless communication standard (supports star, tree and mesh topology) to create low-power LANs / HANs. ZigBee focusses on consumer and industrial equipment, requiring short-range low-rate wireless data transfer. It uses the ISM frequency (868 MHz or 2.4 GHz) and due to low power the communication range varies from 20 meters (indoor) to 100 meters (outdoor). It has a data range of 250 kbps.

ZigBee usage examples are: Home Automation, electrical meters, traffic management systems.

Thread

Thread is a wireless IPv6-based communication standard / protocol for "smart" household devices to communicate on a network.

Thread uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol with mesh communication, as does ZigBee and other systems. Thread is IP-addressable, with cloud access and AES encryption.

It uses the ISM frequency (2.4 GHz), has a data rate of 250 kbps and a communication range of up to 30 meters.

WirelessHART

WirelessHART is a wireless technology for sensors based on the HART (Highway Addressable Remote Transducer). The underlying wireless technology is based on the work of TSMP (Time Synchronized Mesh Protocol) technology.

WirelessHART uses the 2.4 GHz ISM frequency and has a data range of 250 kbps. The communication range varies from 50 meters (indoor) to 250 meters (outdoor).

MiWi

MiWi and MiWi P2P are proprietary wireless protocols designed by Microchip Technology that use small, low-power digital radios.

It is designed for low data transmission rates and short distance, cost constrained networks, such as industrial monitoring and control, home and building automation, remote control, low-power wireless sensors, lighting control and automated meter reading.

It uses the ISM frequency (2.4 GHz) and communication range varies from 50 meters (indoor) to 300 meters (outdoor). It has a data range of 250 kbps.

P802.11ah (low power WiFi)

The 802.11ah is a wireless networking protocol that is an amendment of the "known" WiFi standard (IEEE 802.11).

It utilizes the sub-1GHz ISM bands (868 MHz) to provide extended range compared to the conventional Wi-Fi networks operating in the 2.4 GHz and 5 GHz bands. It benefits from lower energy consumption, allowing the creation of large groups of sensors that cooperate to share the signal.

It supports a data range of 150 kbps (for range up to 1 km) up to (in Europe) 7.8 Mbps (for shorter range; thus << 1 km).

The P802.11AH is a preliminary standard and is scheduled to be finalized early 2016.

CoCo

The CoCo (Controlled Comfort) protocol is a basic wireless communication protocol based on the X10 protocol (not compatible). It has one-way communication and limited number of devices that can be connected. It is popular due to the low prices of CoCo switches (e.g. used to remotely control light).

It uses the 433 MHz ISM frequency. The communication range varies from 30 meters (indoor) to 70 meters (outdoor).

Below 2 short range communication technologies are mentioned in this overview as they are very popular in the DIY community and for solution providers (easy to use, low price (< 5 euros), big community).

Nordic nRF24L01+

The nRF24L01 is a low-power wireless transceiver chip from Nordic Semiconductor. It is using the 2.4 GHz ISM frequency and has a date rate of up to 250 kbps.

ESP8266

The ESP8266 is a microcontroller from Chinese manufacturer Espressif that includes Wi-Fi capability to connect to WiFi networks. IoT communication via MQTT.

Medium / long range

Radio technologies that have a range of 1 km or more are summarized in this section.

Cellular

Existing cellular infrastructures (xG) have the technical potential of becoming a solid fundament for a global IoT network (WAN/GAN). However the existing cellular technologies are not designed for low-power and moderate data rates. Industry initiatives led to a number of adapted cellular technologies in order to become IoT capable.

EC-GSM

The Extended Coverage (EC) GSM is an enhancement of the GSM technology which improves the device indoor reachability (up to 20 dB gain), reduces complexity/power and has a lower data rate (<100 kbps). For the network infrastructure software upgrades are required and most likely no hardware changes. The cellular devices (called CIoT) on the other hand must be EC-GSM compliant to benefit from the extended coverage (network range up to 15 km).

EC-GSM specifications (see 3GPP TR 45.820) are scheduled to be completed in 2016. Note that the EC-GSM applies to networks based on GERAN and (re-)uses the same licensed frequency.

LTE-M

The LTE-M is LTE technology optimized for M2M devices. It has lower data rates, lower complexity/power and is best deployed in the sub-1GHz frequency.

In the current 3GPP R12 version of LTE-M the data rate is up to 1 Mbps while in the upcoming R13 the data rate is reduced to 200 kbps. Ranges are estimated to be up to 11 km.

NB-LTE-M

The Narrow Band (NB) LTE-M optimizes LTE-M even further by using smaller bandwidth (200 kHz instead of 1.4 MHz). This is realized in 3GPP R13; NB-LTE-M enhances the capacity and the range (up to 15 km).

CDMA450

The CDMA450 technology is based on CDM2000 and operates in the lower frequency spectrum (450 MHz). Obviously the lower frequency allows wide area coverage with little number of cells. However from an IoT perspective there are not many CDMA450 device manufacturers. In the Netherlands a utility company rolled out a CDMA450 network in order to receive data from smart meters (electricity, gas).

CDMA450 ranges are estimated to be approx. 25 km (up to max. of 50 km).

LTE-U

The LTE technology used in an Unlicensed frequency spectrum is called LTE-U. In case the access to the unlicensed network is provided after "approval" from a 'licensed' network it is referred to as Licensed Assisted Access (LAA).

The LTE-U is scheduled to use the 2.4 or 5 GHz frequency bands. LTE-U is (similar to WiFi) not an IoT tailored technology and it is mentioned here as it operates in the same unlicensed frequencies and add interferes to IoT related technologies.
LTE-U is being tested and final 'go' (approval) should come from the 3GPP.

Clean-slate

Clean-slate technology (FDMA) is initiated by Neul / Huawei and uses the existing cellular infrastructure. It operates in the licensed sub-1GHz bands.

It supports a data rate of up 50 kbps and the communication range is up to 15 km. Clean-Slate attempts to standardize under 3GPP GERAN for licensed spectrum operation.

Besides using existing cellular network technologies (with enhancements) as described above also new initiatives have led to new long range network technologies.

LoRa

LoRa stands for Long Range and was initiated by Semtech. Today it is led by the LoRa Alliance. The technology is using spread spectrum modulation on unlicensed sub-1GHz bands.

LoRa offers data rates from 0.3 kbps to 50 kbps and the communication range varies from 5 km (urban areas) to 15 km (suburban / rural areas).

Today there are a limited number of LoRA device manufacturers. LoRa usage areas are: Home Automation, electrical meters, traffic management systems.

SIGFOX

Sigfox is a French company that builds wireless networks to connect low-energy IoT devices which need to be continuously on and require low data-rates. The technology is using ultra narrow-band modulation on unlicensed sub-1GHz ISM bands (868 MHz in Europe and 915 MHz in the US).

It supports a data rate of up 100 bits per second and the communication range varies from 10 km (urban areas) to 50 km (rural areas).
Sigfox submitted its technology specifications to ETSI in order to turn the proprietary technology into an ETSI standard.

Weightless

Weightless is a wireless connectivity technology for low power, wide area networks for IoT.

The Weightless-W (Whitespace) standard defines a technology designed to operate in TVWS (TV White Space) spectrum (2013 standard). The Weightless-N (Narrowband) standard defines a technology designed to operate in the unlicensed ISM band (2015 standard). In Europe weightless-N operates on 868 MHz and sometimes referred to as NWave. The Weightless-P standard (expected in 2016) offers carrier grade solutions in the unlicensed ISM spectrum.

Per standard different data rates are supported (W up to 10 Mbps, N up to 100 bps (no downlink) and P up to 100 kbps). The weightless-N/W communication range in urban areas is up to 5 km, the weightless-P up to 2 km.

Weightless are open standards led by a consortium of Accenture, ARM, Cable & Wireless, CSR and Neul (Weightless SIG).

Ingenu (previously On-Ramp)

Ingenu is using wireless RPMA (Random Phase Multiple Access) technology. It is a low-power wide-area channel access method used in machine-to-machine (M2M) communication.

Ingenu uses the ISM frequency (2.4 GHz) and has a communication range of approx. 4 km.

Dash7 Alliance Protocol 1.0

The DASH7 Alliance (D7A) is a group of companies and universities with the goal to create a complete interoperable RF technology to exchange data for wireless sensor networks and devices at a block scale (300 m – 1 km). An open source reference implementation is freely available (e.g. to enable IoT via Raspberry, Arduino etc.).

DASH7 uses sub-1GHz ISM frequencies. Primarily the 433 MHz range and today mostly it is using 868 MHz to reduce antenna size and increase throughput. It supports a date rate of up to 167 kbps and has a communication range of up to 5 km.

Area Networks

In the IoT context there are many type of Area Networks defined. Below a summary of the most common area networks is given:

BAN (Body Area Network) – Network of sensors placed on the human body.

PAN (Personal Area Network) - Network organized around an individual person. PANs generally cover a range of less than 10 meters.

LAN (Local Area Network) – Network of devices in a local geographical area. LANs generally cover a range of less than 100 meters (like school, small office or home).

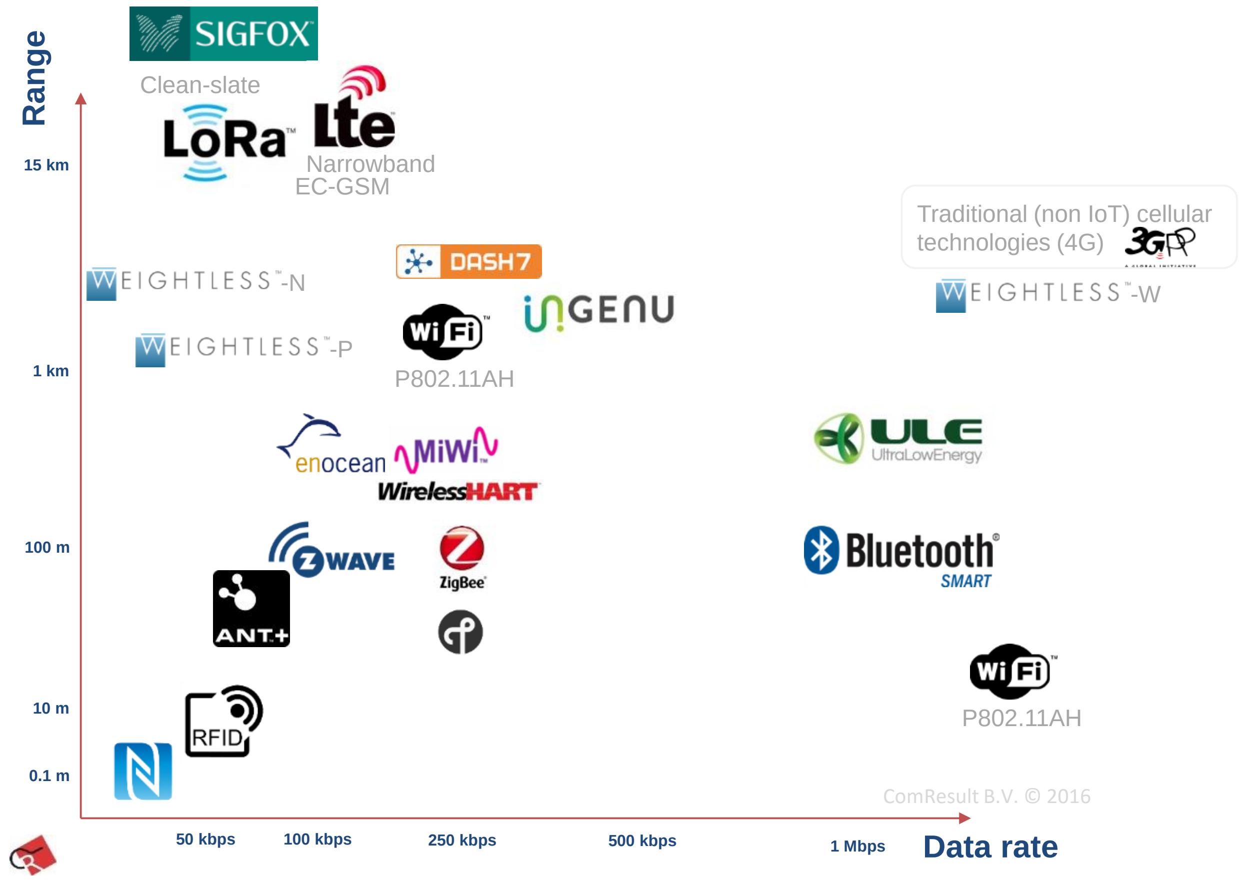
HAN (Home Area Network) – Network of devices in a domestic home. HAN is a LAN type.

CAN (Campus Area Network) – Number of LANs connected together at governmental and educational buildings such as colleges and universities. CANs generally cover a range of a couple of kilometers.

MAN (Metropolitan Area Network) – Network that cover a wide metropolitan area - such as city centre. MANs are largers than CANs and generally cover a range of 5-10 kilometers or more.

WAN (Wide Area Network) – Network that connects regional, national and international networks together (like the internet). Largest area network defined although some people refer to GAN (Global Area Network) as the biggest network.

In the overview below the relation between the range and the data rate for the main wireless technologies are depicted.



The radio connectivity standards, as described on previous pages, often include the protocol as well. This is however not always the case and in the next section the IoT relevant protocols are described which are not bounded to a specific radio technology.

Protocols

Like the radio connectivity also on the protocol side a significant number of standards are available in the market. In this section an overview of the Device-2-Device (D2D) and the Device-2-Server (D2S or S2D) are shown (non-exhaustive). The Server-2-Server (S2S) protocols are not in scope of this paper.

Vendor specific

For most of the commercial devices on the market there are vendor specific protocols required. These protocols are not described in this paper.

There are many vendor specific protocols and below some well-known are listed: Belkin WeMo, Philips HUE, Insteon Hub / PLM, Sonos, Somfy URTSI, Logitech Harmony, DigitalSTROM, Fritzbox etc. etc.

MQTT

MQTT (Message Queue Telemetry Transport) is a protocol for collecting device data and communicating it to servers (D2S). It targets large networks of small devices that need to be monitored or controlled from the cloud.

MQTT runs on top of TCP.

XMPP

XMPP (Extensible Messaging and Presence Protocol) is a protocol for connecting devices to people, a special case of the D2S pattern, since people are connected to the servers.

XMPP runs on top of TCP.

DDS

DDS (Data Distribution Service) targets devices that directly use device data. It is a bus protocol for integrating intelligent machines (D2D).

CoAP

Constrained Application Protocol (CoAP) is a software protocol used in very simple electronics devices that allows them to communicate over the Internet.

CoAP runs on top of TCP.

Weave

Weave is an open protocol which is designed for IoT. The protocol is from Nest (a Google owned company). Weave creates its own WiFi network such that the devices are not depending on an internet connection to work.

Weave runs on top of TCP and is an open protocol.

JMS

Java Message Service API is a Java Message Oriented Middleware (MOM) API for sending messages between two or more clients,

JMS runs on top of TCP.

REST

REpresentational State Transfer is a style of software architecture for distributed systems such as the World Wide Web

KNX

KNX is a standardized OSI-based network communications protocol for intelligent buildings.

The standard also included several physical communication media (both wired (Ethernet, twisted pair and powerline) and wireless (868 MHz or infrared)).

X10

X10 is the first open communication protocol for Home Automation which was developed in 1975. For communication it uses the power line wiring or the ISM frequency (433 MHz).

X10 technology remains worldwide available but since the bankruptcy of the original X10 factory in 2011 it led to a situation where there are no more developments and no new products.
On top of that X10 is moved to the background due to new more sophisticated technologies as described here.

Considering the dynamic stage of IoT and the energy the Industry puts into IoT development, it is expected that new protocols will be added to the above list.

What's next?

In the last year the 'Internet of Things' went over the peak of inflated expectations in the Gartner Hype Cycle and now moving in direction of 'trough of disillusionment'. This hype contributed that there are (too) many existing and new protocols for network connectivity in the market today. This number continues to grow this year and it is expected that in the coming years the network connectivity market is slowly diverting towards a limited number of technologies and expected to start stabilizing after 2017.

A 'network connectivity' market which is stable will trigger investments. This feeds product and app developments, used for the IoT solutions. This growth stage goes hand in hand with product scalability and price drops and is expected to last until approx. 2022. Around that time IoT will be a commodity and the market is entering the maturity phase.
In the upcoming years many IoT related networks are rolled out in Europe with different protocols. In parallel the number of IoT solutions will slowly grow – unfortunately with a wide range of different (incompatible) protocols. This incompatibility drives the amount of stand-alone (vertical) solutions.

As the amount of forecasted IoT devices is tremendous the importance of the network connectivity for the industry is high. The industry players in this battle have the ultimate goal to reach such a dominant position in the market that they become the 'de facto' industry standard. For now it means that the IoT market remains chaotic and nobody can predict how it is going to develop and what standards wins. At this stage we can make intelligent guesses what we believe is going to happen but for sure we will need to revise our vision in the future.

As a closing statement I would like to mention the risk that many technologies are utilizing ISM frequencies. One of the risks is that interference is likely to become an issue in the near future. A kind of analogy can be made with the WiFi situation today, with the big difference that the 'things' will for sure outnumber the WiFi hotspots.

A whitepaper describing the end-to-end IoT value chain is scheduled for the coming months. In case you are interested you can follow me on twitter or send me an email to subscribe to my white papers.

About the author …

Jeroen van Bussel has almost 20 years of experience in the Telecom / IT arena. He is owner / co-founder of consultancy firm ComResult BV. He worked internationally for several telecom operators and suppliers in different roles (Project Manager, Solution Architect / Lead, Consultant, Technical Sales).

Jeroen today works as independent consultant / advisor and is interested in latest upcoming innovative technologies and market developments. In case you have questions, suggestions or remarks feel free to get in touch – below the contact details:

jeroen.vanbussel@comresult.com.
www.comresult.com