Internet of Things| Applications & Prospects

Ala Al-Fuqaha, Ph.D.
Professor
Western Michigan University, USA
ala@ieee.org

Outline

- Introduction
- Applications & Services
- Technologies
- Architecture
- Protocols
- Experiments & Hands-on Practice
- Challenges & Research Directions
- Future Prospects
- Conclusions

Introduction

Internet Revolution

Internet of boffins	Internet of geeks	Internet of masses	Mobile Internet	Internet of things
1969 - 1995	1995 - 2000	2000 - 2007	2007 - 2011	2012 & beyond

Terminology

- **Internet:** Interconnected computer networks, based on a standard communication protocol (TCP/IP)
- **Things:** any unique object in the world
- **Internet of Things:** connected objects uniquely addressable, based on standard communication protocol

IoT ➔ Big Data ➔ Extract knowledge (offering value-added services)

- **Example of IoT**: Imagine when you enter your house, your car send signals to open garage door, turn on air condition/ heat system, lights, TV, Stove, etc. to find everything ready for you, making your life easier and save your money buy saving energy.
- Internet-Connected Bed to track your sleeping pattern and make your bed auto-adjusts itself.
- Internet-Connected onesies to track yourbaby's respiration, pressure, moisture and temperature.

What is Internet of Things?

"Internet of Things" "Internet of Everything" (Cisco) "Smarter Planet" (IBM) "Cyber Physical Systems (CPS)" (NSF)

(1) The Internet of Things (IoT), also called Internet of Everything, is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the production, operator and/or other connected devices based on the infrastructure of International Telecommunication Union's Global Standards Initiative.[1] The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure,[2] creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.

------Wikipedia

(2) Internet of Things refers to the concept that the Internet is no longer just a global network for people to communicate with one another using computers, but it is also a platform for devices to communicate electronically with the world around them."

--Center for Data and Innovation

What is Internet of Things?

(3) The term "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects.

------IoT in 2008

(4) "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts".

-------IoT in 2020

What is Internet of Things?

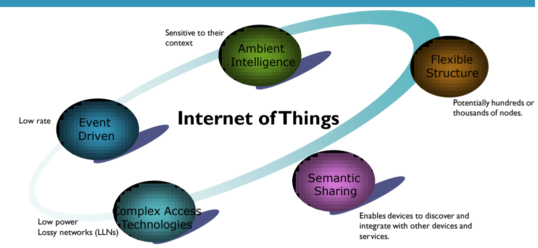
- A network of Physical Objects that can interact with each other to share information and take Action.
- The term was first proposed by Kevin Ashton in 1999.
- The concept of IoT first became popular at the Auto-ID center, MIT.
- Machine-to-Machine (M2M) Type communications are a big part of IoT but it is not everything.

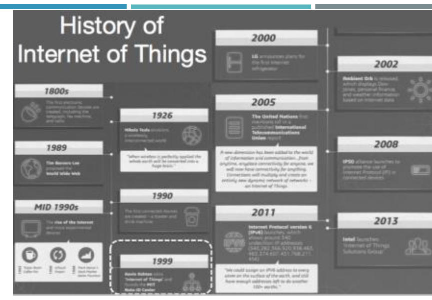
What is M2M?

- Communication between devices without human intervention.

M2M traffic is growing rapidly.

Characteristics

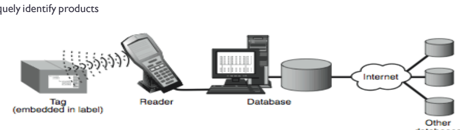




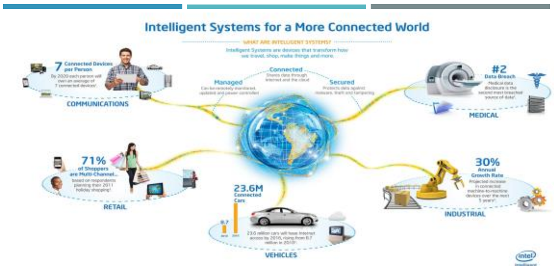
Source: Government Accountability Office (GAO)

History of IoT

- IoT was originally introduced by the Auto-ID research center at MIT (Massachusetts Institute)in 1999
- Founded by Kevin Ashton, David Brock and Sanjay Sarma to develop the Electronic Product Code or EPC to uniquely identify products



Source: Government Accountability Office (GAO)

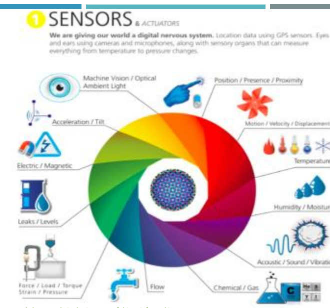


*** It is estimated that <1% of the physical object are connected to the Internet → 100 folds growth potential!**
*** $14 Trillion market value projected over the next 10 years.**
*** Cisco projects that 50 Billion devices will be Internet-Connected by 2020.**

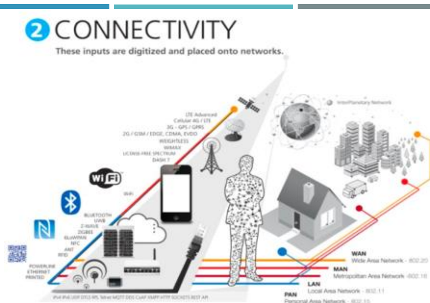
Smart Systems and IoT

Smart Systems and The Internet of Things are driven by a combination of:

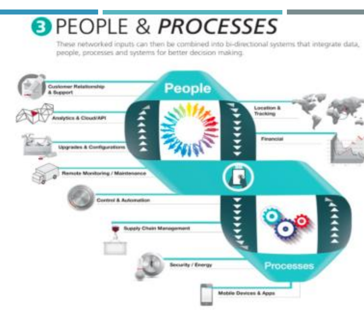
Source: Postscape - http://postscapes.com/what-exactly-is-the-internet-of-things-infographic



Source: Postscape - http://postscapes.com/what-exactly-is-the-internet-of-things-infographic

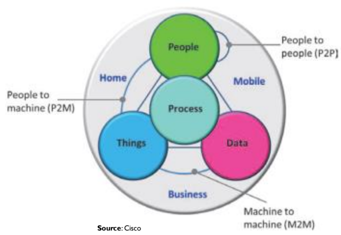


Source: Postscape - http://postscapes.com/what-exactly-is-the-internet-of-things-infographic



Source: Postscape - http://postscapes.com/what-exactly-is-the-internet-of-things-infographic

Internet of Everything

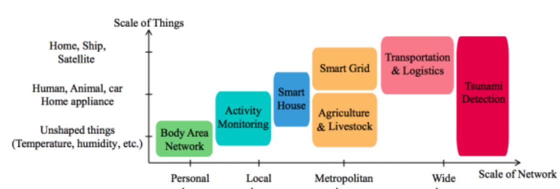


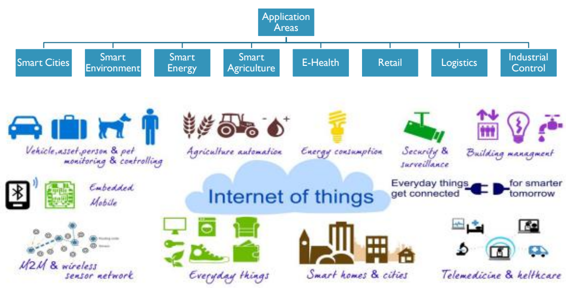
Source: Cisco

Source: Postscape - http://postscapes.com/what-exactly-is-the-internet-of-things-infographic

Applications & Services

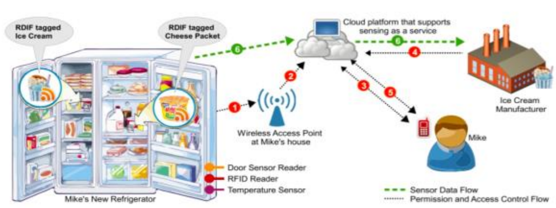
Classifications and Examples of IoT Systems





Smart Home

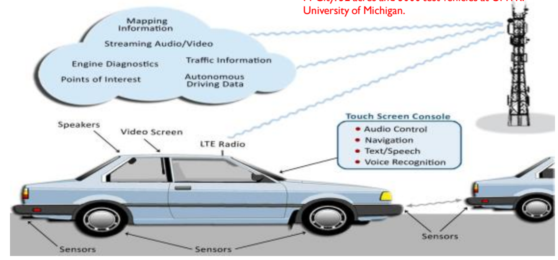
Smart Home Scenario



[Source: "Sensing as a Service Model for Smart Cities Supported by Internet of Things", Charith Perera et. al., Transactions on Emerging Telecommunications Technology, 2014]

Smart Cars (aka the Internet of Vehicles)

M-City: 32 acres and 3000 test vehicles at UMTRI University of Michigan.

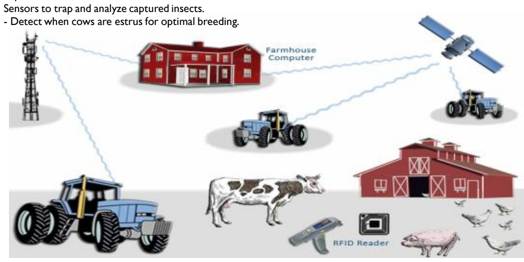


E-Healthcare

Offer remote health services for baby boomers.
Help them to live independently at their homes instead of nursing homes.

Smart Farms

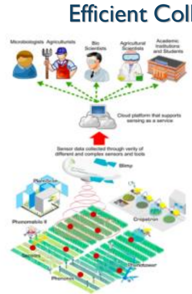
- Temperature sensors, moisture sensors, etc.
- Sensors to trap and analyze captured insects.
- - Detect when cows are estrus for optimal breeding.



Efficient Waste Management in Smart Cities

[Source: "Sensing as a Service Model for Smart Cities Supported by Internet of Things", Charith Perera et. al., Transactions on Emerging Telecommunications Technology, 2014]

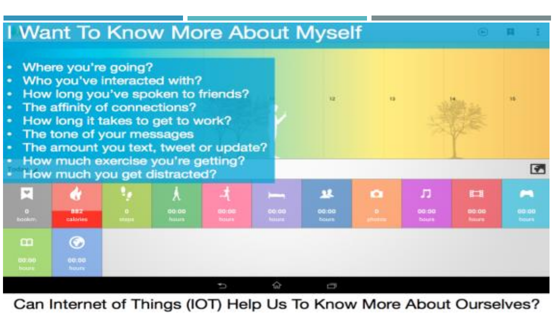
Efficient Collaborative Research




The sensing-as-a-service model allows researchers to share resources across borders and understand phenomenon which are not available in their own countries.


How Well Do I Sleep?
Sleep
Sleep Stats
Your sleep pattern asleep awake
YOUR SLEEP EFFICIENCY 92%
You went to bed at 11:00PM
Time to fall asleep 0min
Times awakened 20
You were in bed for 6hrs 40min
Actual sleep time 6hrs 6min
Time asleep over the past 30 days in hours
Times awoken over the past 30 days
8 h 50 mins asleep
Awake for 212 mins (81x)
Restless for 278 mins (91x)
Thursday, February 27
fitbit flex

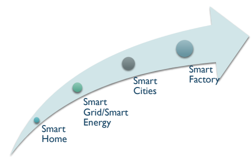

Am I Healthy?

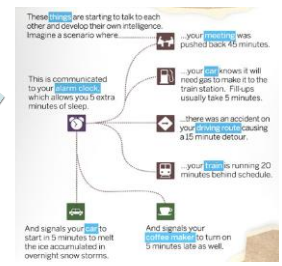

I Want To Know More About Myself
Where you're going?
Who you've interacted with?
How long you've spoken to friends?
The affinity of connections?
How long it takes to get to work?
The tone of your messages
The amount you text, tweet or update?
How much exercise you're getting?
How much you get distracted?
Can Internet of Things (IOT) Help Us To Know More About Ourselves?


Lifelogging
Take a Stroll Down a Virtual Memory Lane
"How much more IOT can do is only left to your imagination and to your budget. You can do as little or as much with IoT as you want."
MIT SCIENTIST CAPTURES 90,000 HOURS OF VIDEO OF HIS SON'S FIRST WORDS, GRAPHS IT → BIG DATA

Current Scenario

Future Scenario





Cloud Services Frameworks

- ThingWorx
  - provides a complete application design, runtime, and intelligence environment - allowing organizations to rapidly create M2M applications and intelligent connected Things
- SmartThings
  - Variety of sensors and a development platform.
- Eclipse IoT
  - An ecosystem of companies and individuals that are working together to establish an Internet of Things based on open technologies.
- SHODAN
  - IoT search engine.
- Nimbits
  - Data Logging Service and Rule Engine Platform for connecting people, sensors and software to the cloud and one another

Cloud Services Frameworks

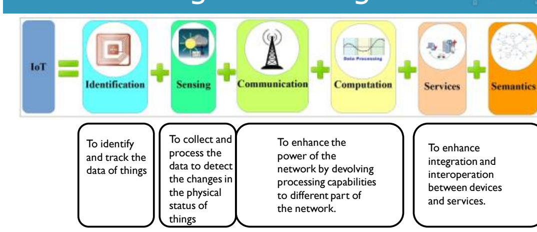
- Xively (formerly Cosm)
  - A web platform to connect sensors with users.
- Cisco
  - Networking infrastructure. For example, Cisco ISR 819 IoT gateway.
- IBM
  - IoT foundation service to develop, simulate and manage IoT applications (emphasis on MQTT)
- Add More ….

Technologies

Source: Gartner, 2013, online at http://www.gartner.com/newsroom/id/2636073

IoT Enabling Technologies

IoT Enabling Technologies

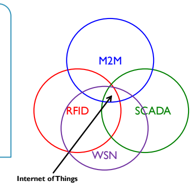


IoT Enabling Technologies

IoT Elements		Samples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, , LTE-A
Computation	Hardware	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, Smart Phones
	Software	OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc.)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)
Semantic		RDF, OWL, EXI

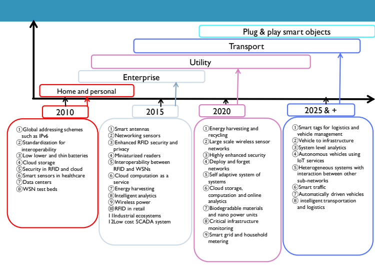
IoT Enabling Technologies

- RFID Technology
- Sensor Technology (nano-technology)
- Wireless Communication (low power, lossy networks)
- Energy Harvesting Technologies
- Cloud Computing
- Advanced Internet Protocol (IPv6)



Essential Technologies Involved in IoT

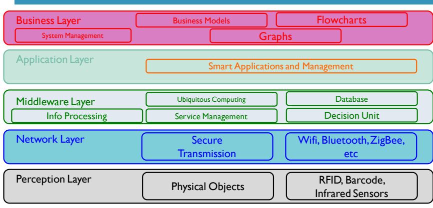
Roadmap of key technological developments with IoT



Source : Jayavardhana Gubbi

Architecture

Architecture of IoT

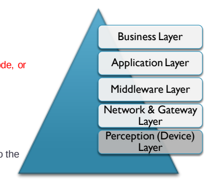


Meanwhile, there are some projects like IoT-A which try to design a common architecture based on the analysis of the needs of researchers and the industry.

Source: future internet, 2012

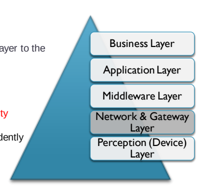
IoT layers – Perception Layer

- **Perception (Device) Layer**:
  - Lowest Abstraction Layer
  - Consist of the physical objects and sensor devices (i.e., RFID, 2D-barcode, or any sensor depending on required functionality)
  - Collection of objects information by the Sensors
  - Collects and processes the real time information
  - Collected information passed to Network layer for secure transmission to the information processing system in middleware layer



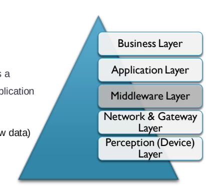
IoT layers - Network Layer

- **Network Layer (Transmission):**
  - Transfer information securely from sensor devices in Perception (device) layer to the information processing system in Middleware layer
  - Robust and high performance network infrastructure
  - Supports the communication requirements for latency, bandwidth or security
  - Allows multiple organizations to share and use the same network independently



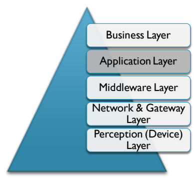
IoT layers - Middleware Layer

- **Middleware Layer:**
  - Responsible for the device management and interoperation.
  - Performs information processing and ubiquitous computation and makes a decision by sending specific sensor info to the related applications in Application layer to do specific jobs.
  - Data Analytics (Extracts relevant information from massive amount of raw data)
  - Ensures security and privacy of data.



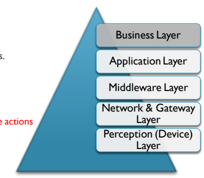
IoT layers - Application Layer

- **Application Layer:**
  - Provides a global management for the application based on the objects processed in Middleware layer
  - Different applications for various sectors (i.e., Transportation, Healthcare, Agriculture, Supply chains, Government, Retail, etc.)

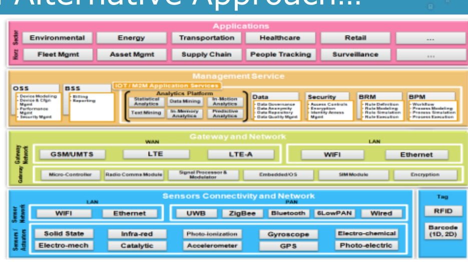


IoT layers - Business Layer

- **Business Layer:**
  - Maintain overall IoT system management including the applications and services.
  - Build business models, graphs, flowcharts, etc. based on the data received from Application layer.
  - Analyzing and monitoring of models results, which help to determine the future actions and business strategies.



An Alternative Approach…



Protocols

IoT Protocols & Standards

Application Protocol		DDS	CoAP	AMQP	MQTT	MQTT-NS	XMPP	HTTP REST
Service Discovery		mDNS				DNS-SD		
Infrastructure Protocols	Routing Protocol	RPL						
	Network Layer	6LoWPAN					IPv4/IPv6	
	Link Layer	IEEE 802.15.4						
	Physical/ Device Layer	LTE-A	EPCglobal	IEEE 802.15.4	Z-Wave			
Influential Protocols		IEEE 1888.3, IPSec					IEEE 1905.1	

X10

- X10 is a protocol for communication among electronic devices used for home automation. It primarily uses power line wiring for signaling and control.
- X10 controllers send signals over existing AC wiring to receiver modules
- X10 technology transmits binary data using the Amplitude Modulation (AM) technique.
- Data is encoded onto a 120 kHz carrier which is transmitted as bursts during the relatively quiet zero crossings of the 50 or 60 Hz AC alternating current waveform. One bit is transmitted at each zero crossing.

Z-Wave (ITU-T G.9959)

- Z-Wave as a low-power wireless communication protocol for Home Automation Networks (HAN) has been used widely in the remote control applications in smart homes as well as small-size commercial domains .
- This protocol was initially developed by ZenSys (currently Sigma Designs) and later was employed and improved by Z-Wave Alliance. Z-Wave covers about 30 meters point-to-point communication and is specified for applications that need tiny data transmission like light control, household appliance control, smart energy and HVAC, access control, wearable health care control, and fire detection. Z-Wave operates in ISM bands (around 900 MHz) and allows transmission rate of 40 kbps.
- The recent versions also support up to 200 kbps. Its MAC layer benefits from a collision avoidance mechanism. Reliable transmission is possible in this protocol by optional ACK messages.
- In its architecture, there are controller and slave nodes. Controllers manage the slaves by sending commands to them. For routing purposes, a controller keeps a table of the whole network topology. Routing in this protocol is performed by source routing method in which a controller submits the path inside a packet.

HomePlug (IEEE 1901)

- **IEEE 1901** is a standard for high speed (up to 500 Mbit/s at the physical layer) communication devices via electric power lines, often called broadband over power lines (BPL). The standard uses transmission frequencies below 100 MHz.

- HomePlug 1.0
- HomePlug AV
- HomePlug AV2
- HomePlug Green PHY (Energy efficient)

Convergence Digital Home (IEEE 1905.1)

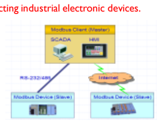
- Allows wireless and power line communication home automation protocols to interoperate.

BACnet (ISO 16484-5)

- **BACnet** is a communications protocol for **building automation** and **control networks**.
- BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control, lighting control, access control, and fire detection systems and their associated equipment.

ModBus, FieldBus, IE

- An open data communication protocol used widely for connecting industrial electronic devices.
- Open structure
- Flexible
- Widely known
- Supplied by many SCADA software
- 2 serial transmission modes:
  - ASCII
  - RTU (Binary)
- Communication interface
  - RS-232/485
  - Ethernet (TCP/IP)



Other protocols for industrial automation:
- FieldBus (**IEC 61158).**
- **Industrial Ethernet (ruggedized Ethernet)**

ISO/IEC 18000

- **ISO/IEC 18000** is an international standard that describes a series of diverse RFID technologies, each using a unique frequency range.

18000-1: General guidelines
18000-2: less than 135 KHz
18000-3: HF 13.56 MHz
18000-4: 2.45 GHz
18000-6: UHF 860-960 MHz
18000-7: 433 MHz

NFC is a branch of High-Frequency (HF) RFID, that operates at the 13.56 MHz frequency. NFC is designed to be a secure form of data exchange, and an NFC device is capable of being both an NFC reader and an NFC tag. This unique feature allows NFC devices to communicate peer-to-peer.

wireless network technology options

Network definition	*standard*	*Known as*
Wireless personal area network (WPAN)	IEEE 802.15.1	Bluetooth
Low-rate WPAN (LR-WPAN)	IEEE 802.15.4	ZigBee
Wireless local area network (WLAN)	IEEE 802.11	WiFi
Wireless metroplitan area network (WMAN)	IEEE 802.16	WiMAX
Long Term Evolution (LTE)	IMT-Advaced/3GPP	LTE Advanced

ZigBee builds upon the 802.15.4 standard to define application profiles that can be shared among different manufacturers

IEEE 802.15.4 LR-WPAN (ZigBee)

ZigBee technology is simpler (and less expensive) than Bluetooth.

The main objectives of an LR-WPAN like ZigBee are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

The raw data rate will be high enough (maximum of 250 kbit/s) to satisfy a set of simple needs such as interactive toys, but is also scalable down to the needs of sensor and automation needs (20 kbit/s or below) using wireless communications.

LR-WPAN device types

Two different device types can participate in an LR-WPAN network:

- Full-function devices (FFD) can operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device.
- Reduced-function devices (RFD) are intended for applications that are extremely simple.

An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD.

Network topologies (1)

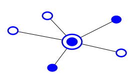
Two or more devices communicating on the same physical channel constitute a WPAN. The WPAN network must include at least one FFD that operates as the PAN coordinator.

The PAN coordinator initiates, terminates, or routes communication around the network. The PAN coordinator is the primary controller of the PAN.

The WPAN may operate in either of two topologies: the star topology or the peer-to-peer topology.

Network topologies (2)

Star topology



In a star network, after an FFD is activated for the first time, it may establish its own network and become the PAN coordinator.

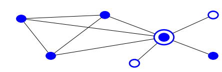
The PAN coordinator can allow other devices to join its network.

PAN coordinator (always FFD) FFD RFD

Network topologies (3)

In a peer-to-peer network, each FFD is capable of communicating with any other FFD within its radio sphere of influence. One FFD will be nominated as the PAN coordinator.

Peer-to-peer topology



A peer-to-peer network can be ad hoc, self-organizing and self-healing, and can combine devices using a mesh networking topology.

ZigBee PHY and MAC parameters

Topology	Ad hoc (central PAN coordinator)
RF band	2.4 GHz ISM frequency band
RF channels	16 channels with 5 MHz spacing
Spreading	DSSS (32 chips / 4 bits)
Chip rate	2 Mchip/s
Modulation	Offset QPSK
Access method	CSMA/CA

CSMA/CA operation

Each time a device wishes to transmit data frames or MAC commands, it shall wait for a random period. If the channel is found to be idle, following the random backoff, the device shall transmit its data. If the channel is found to be busy, following the random backoff, the device shall wait for another random period before trying to access the channel again.

Acknowledgment frames shall be sent without using a CSMA-CA mechanism.

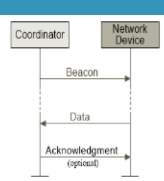
Types of ZigBee PANs

- Non-Beacon Enabled PAN
  - Un-slotted CSMA/CA
- Beacon Enabled PAN
  - Slotted CSMA/CA

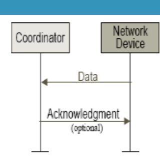
ZigBee SuperFrame Structures

- A superframe is formed by the PAN coordinator to synchronize network reception and transmission.

Communication to Coordinator

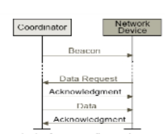


-Communication to a coordinator in a beacon-enabled network

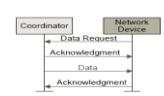


-Communication to a coordinator in a nonbeacon-enabled network

Communication from Coordinator



Communication from a coordinator a beacon-enabled network



-Communication from a coordinator in a nonbeacon-enabled network

6LoWPAN
(IPv6 in Low-Power Wireless Personal Area Networks)

- Low cost and low power devices
- Connect the physical environment to real world applications, e.g., wireless sensors networks
- Common topologies star, mesh, and combination of them
- It It allows the use of IPv6 over IEEE 802.15.4
- IPv6 datagram size can be 1280 bytes and the MTU of IEEE 802.15.4 is 127 ➔ the role of 6LoWPAN is to act as an adaptation layer between the two and compress the IPV6 headers to save energy.

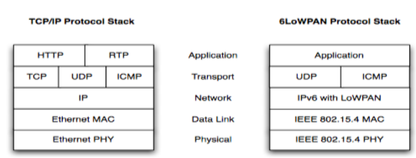
6LoWPAN characteristics

- Support 64-bit addressing
- Support low-power link layers like IEEE 802.15.4 and power-line communications PLC
- Efficient header compression
- Auto-configuration using **Neighbor Discovery** protocol
- Unicast, multicast and broadcast
- Support for IP routing like IETF RPL
- Support for link-layer mesh like 802.15.5

6LoWPAN advantages

- **Open**
- **Easy to understand**
- **Internet integrity**
- **Network maintainability**
- **Global scalability**
- **End-to-end data flows**
- **Cheaper and commercial**

6LoWPAN vs. TCP/IP Stacks



Source: 6lowpan book slides, 2009

Comparing Traditional Web and IoT Protocols

From ReST to Constrained RESTful Environments (CoRE)

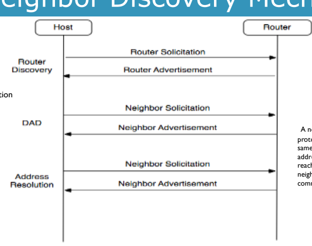
HTTP	Application layer	MQTT CoAP
TCP	Transport layer	UDP
IPv4 IPv6	Network layer	6LoWPAN Zigbee
Ethernet WiFi	Data link layer	IEEE 802.15.4
Information Resource		Thing

IPv6 Neighbor Discovery (ND) protocol

- IPv6 is the format - ND is the brains
  - "One-hop routing protocol" defined in RFC4861
- Defines the interface between neighbors
- Finding Neighbors
  - Neighbor Solicitation (NS)/ Neighbor Acknowledgement (NA)
- Finding Routers
  - Router Solicitation (RS)/ Router Advertisement(RA)
- Address resolution using NS/NA
- Detecting Duplicate Addresses using NS/NA
- Neighbor Unreachability Detection using NS/NA
- DHCPv6 may be used in conjunction with ND

IPv6 Neighbor Discovery Mechanism

Duplicate Address Detection (DAD)



A node uses Neighbor Discovery (ND) protocol to discover other nodes on the same link, to determine their link-layer addresses, to find routers, and to maintain reachability information about the paths to neighbors that the node is actively communicating with.

Routing Over Low-Power and Lossy Networks (ROLL WG)

- The Internet Engineering Task Force (IETF) standardized an IPv6-based routing solution for IP smart objects for embedded applications in 2008
- Focusing on the routing requirements on applications like urban networks including smart grid, industrial automation, home and building automation, etc.
- Introducing "Ripple" routing protocol (RPL), along with supporting specifications on routing metrics, objective functions and security

Routing in LLNs

Properties of application and link-layers considered by ROLL are:

- Traffic patterns are not only peer-to-peer unicast flows, but more often point-to multipoint or multipoint-to-point flows.
- Routers in LLNs have a very small (limited) memory
- Most LLNs must be optimized for energy consumption
- Security and manageability are important in LLNs functionality

RPL

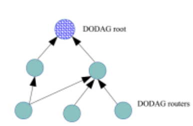
- RPL can be classified as a proactive distance-vector algorithm with advanced options for constraint-based routing, multi-topology routing and traffic engineering.
- Support for dynamic topologies and mobility
- Support multipath routing and multiple forwarding
- Typically utilized by embedded devices with limited processing, memory and power resources.

RPL

- The routing protocol uses a graph structure between nodes and LBRs (LLN Border Routers).
- The topology needs to be discovered and maintained using a minimal amount of signaling.
- After constructing the topology, the routing protocol maintains upstream (from node to LBR) and downstream (from LBR to node) paths.
- Forwarding along these paths is then performed using IPv6 forwarding.
- The coordination of constrained routing, multi-topology routing and traffic engineering is typically done by the LBR.

RPL Protocol

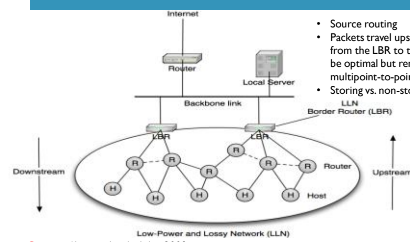
- RPL operates at the IP layer enabling routing across multiple types of link layers
- RPL is a Distance Vector IPv6 routing protocol for LLNs that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG)
- RPL uses an objective function and a set of metrics/constraints to find the 'best' path



RPL Protocol

- RPL provides multi-topology routing (MTR) by constructing and identifying multiple graphs (DODAGs) over the same physical topology.
- RPL also supports point-to-point (P2P)
- RPL is adequate for non-production phases and emergency rerouting
- For example, several DODAGs may be used with the objective
  - Find paths with best ETX [Expected Transmissions] values (metric) and avoid non-encrypted links (constraint)
  - Find the best path in terms of latency (metric) while avoiding battery-operated nodes (constraint)

RPL Protocol Architecture



- Source routing
- Packets travel upstream to the LBR and then downstream from the LBR to the destination ➔ this might not seem to be optimal but remember that RPL shines in handling multipoint-to-point traffic.
- Storing vs. non-storing nodes.

Source: 6lowpan book slides, 2009

Resource-Oriented Architecture (ROA)

- ROA is a way of turning a problem into a (REpresentational State Transfer) RESTful web service, which is a set of arrangement of URIs, HTTP, JSON and XML that works like the rest of the Web
- REST is not an architecture: it's a set of design criteria
- It can be any specific architecture that meets those criteria, but there is no one "REST architecture"
- It is not a specific set of technologies
- Using Verbs (CRUD) and RUIs to develop APIs.

What's a Resource?

- A resource is anything important enough to be referenced as a "thing" itself.
- A resource is something that can be stored on a computer and represented as a stream of bits: a document, a row in a database, or a result of running an algorithm
- A universal Resource Identifier (URI) provides the name and address of a resource. If a piece of information doesn't have a URI, it's not a resource and it's not really on the Web, except as a bit of data describing some other resource.

ROA concepts

- Resources
  - anything that's important enough to be referenced as a "thing" by itself
- Their names
  - unique identification of the resource
- Their representations
  - useful information about the current state of a resource
- The links between them (interfaces)
  - link to another representation of the same or another resource

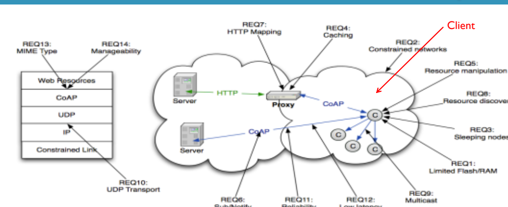
ROA properties

- Addressability
  - Every resource should have a unique address
- Statelessness
  - Since web pages are **stateless** on the server side. Once a web server gives you a copy of a web page, it forgets about you. So, ROA attempts to give web services these same properties since they are the properties that make web pages work so well for humans.
- Connectedness
  - Each resource should connect to its service
- Uniform interface
  - Interface for accessing the resource and manipulating its state

Constrained RESTful Environments (CoRE)

- An IETF Workging Group concerned with the development of resource-oriented application protocol intended to run on constrained IP networks
- Support a RESTful architectural
  - POST, GET, PUT, DELETE operations
  - Stateless – no dependency on last state
  - Expose directory structure-like URIs
  - Transfer JSON or XML representations
  - Define mappings to compact binary forms and transport over UDP

CoRE Requirements



Source: Shelby-core-tutorial-v2 slides

Constrained Application Protocol (CoAP)

- The CoRE Working Group proposed a standard called Constrained Application Protocol (CoAP) which can be easily translated to HTTP to foster integration of constrained networks with the web
- CoAP is an application layer protocol use in resource-constrained Internet devices, such as IoT nodes
- A software protocol used in very simple electronics devices that allows them to communicate interactively over the Internet
- Specially made for small low power sensors, switches, and all devices that need to be controlled remotely, through the Internet

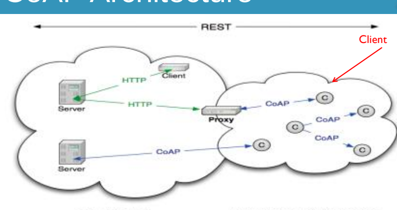
Constrained Application Protocol (CoAP)

- CoAP is designed to be used with constrained nodes and networks
- The nodes often have 8-bit microcontrollers with small amounts of ROM and RAM
- The networks often have high packet error rates and a typical throughput of 10s of kbit/s such as 6LoWPAN
- CoAP designed for machine-to-machine (M2M) applications such as smart energy and building automation

Constrained Application Protocol (CoAP)

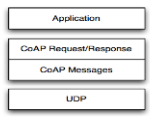
- CoAP provides a request/response interaction model between application endpoints
- supports built-in discovery of services and resources
- includes key concepts of the Web such as URIs and Internet media types
- CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support
- very low overhead and simplicity for constrained environments

The CoAP Architecture



Source: Shelby-core-tutorial-v2 slides

The Transaction Model



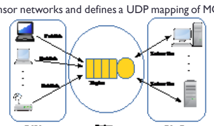
- Transport
  - CoAP currently defines:
    - UDP binding with
      Datagram Transport Layer Security
      DTLS
  - CoAP over SMS or TCP possible
- Base Messaging
  - Four types of messages: Confirmable, Non-confirmable, Acknowledgement, Reset.
  - Method codes and response codes included in some of these messages make them carry requests or responses.
- REST Semantics
  - The basic exchanges of the four types of messages are somewhat orthogonal to the request/response interactions.
  - Requests can be carried in Confirmable and Non-confirmable messages, and responses can be carried in these as well as piggy-backed in Acknowledgement messages.

CoAP implementations

- There are many open source implementations available
  1) Java CoAP Library Californium
  2) C CoAP Library Erbium
  3) libCoAP C Library (Porting libcoap to Contiki)in WP4
  4) jCoAP Java Library
  5) OpenCoAP C Library
- TinyOS and Contiki include CoAP support
- CoAP is already part of many commercial products/systems
  1) Sensinode Nano Service
  2) RTX 4100 WiFi Module
  3) Firefox has a CoAP plugin called Copper
  4) Wireshark has CoAP dissector support

MQTT

- MQTT is a messaging protocol that was introduced by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom (now Eurotech) in 1999 and was standardized in 2013 at OASIS. MQTT aims at connecting embedded devices and networks with applications and middleware.
- MQTT utilizes the publish/subscribe pattern to provide simplicity of implementation.
- MQTT is transported over TCP.
- MQTT-SN was defined specifically for sensor networks and defines a UDP mapping of MQTT and adds broker support for indexing topic names.



DDS

- Data Distribution Service (DDS) is a publish-subscribe protocol for real-time M2M communications that has been developed by Object Management Group (OMG). In contrast to other publish-subscribe application protocols like MQTT or AMQP, DDS relies on a broker-less architecture and uses multicasting to bring excellent Quality of Service (QoS) and high reliability to its applications. Its broker-less publish-subscribe architecture suits well to the real-time constraints for IoT and M2M communications. DDS supports 23 QoS policies by which a variety of communication criteria like security, urgency, priority, durability, reliability, etc. can be addressed by the developer.

- Other application protocols include: HTTP-REST, XMPP, AMQP.

Zero-Configuration Networking

- **Zero-Config Networking**
  - Easy to use
  - Based on proven technology (DHCP, DNS)
  - Widespread support by applications and devices
  - But it only works within a subnet!
- **Zero-Confing networking components**
  1) Link-local addressing (LLA)
  2) multicast DNS (mDNS)
  3) DNS Service-Discovery (DNS-SD)

Service Discovery Protocol (SDP)

- SD is a function for finding a service provider for a requested service
- SDP consists of (2)basic elements
  1) **Client:** the entity that is interested in finding and using a service
  2) **Server:** the entity that offers the service
- A service in the network can be any software or hardware entity that a user might be interested to utilize

SD Objectives

1) **Discovery** The ability to find a service provider for the request
   a) **Use a description language** services are semantically described in a certain description language like XML
   b) **Storage of service information** service information stored in different storages within two end-points
   c) **Search for services** Service requests are expressed using the description language in the network.

SD Objectives

2) **No administration**.

   The network must organize and deliver information about its content without human intervention

   a) **Maintenance against changes in service description**. Services may change their characteristics, so the SDP should be able to track them
   b) **Maintenance against topology changes**.

      Services may be unavailable or added to the network, so the SDP should be able to be updated accordingly

SD Issues

1) **Functional issues**

   a) **Service selection**. Some protocols may implement automatic service selection, based on a set of metrics that are used to define the best service offer.

   b) **Service usage**. Apart from performing SDP may also offering methods for using the services.

   c) **Security and privacy**. Because many entities interact with each other within a SDP, so security and privacy play an important role.

SD Issues

2) **Performance issues**

   a) **Network scalability**. Protocol should be able to manage large networks

      I. **Load balancing**

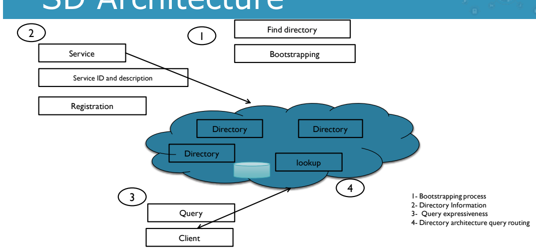
      II. **Query efficiency**

   b) **Fault tolerance**. Protocol should be able to cope with the failure of servers

   c) **Mobility support**. Protocol should be able to deal with highly dynamic environments

   d) **Integration of resource-poor devices**. Protocol should be able to run on resource constrained devices, mobile phones, home appliances or even sensors that might be able to offer or use services.

SD Architecture



Source: LILJANA, Ad Hoc Networking Towards Seamless Communications. 2006

Link-Local Addressing (LLA)

- LLA is a network address that is valid only for communications within a single network link that a host is connected to.
- not a unique address. So, routers do not forward packets using LLA.
- LLA would normally be used in cases where a protocol also supports non-link-local addresses like IPv4, IPv6

Simple idea of LLA

- When automatic IP configuration through (Dynamic Host Configuration Protocol) DHCP fails, the Operating System automatically assigns an autoconfiguration address, which allows the computer to communicate with other machines on the link, this is LLA
- In IPv4, LLA range 169.254.0.1 - 169.254.255.254
- In IPv6, LLA range begin with 1111111010 (FE80)

LLA features

- computers on a link can always communicate through IPv6 using LLA, which is not the case in IPv4 because APIPA addresses are not in the same subnet as private or public IPv4 addresses
- Thus, if the local DHCP is unavailable, the computers can still access local services through IPv6 but won't be able to reach the Internet or services in other links

Multicast DNS (mDNS)

- In 1997, Stuart Cheshire proposed adapting Apple Computer's Name Binding Protocol for IP networks. Supporting the transition from AppleTalk to IP networking
- In 2002, implementation of both mDNS and DNS-Based Service Discovery (DNS-SD) protocols announced by Apple under Rendezvous name (later renamed Bonjour), replacing the Service Location Protocol
- In 2013, the proposals were ratified as RFC 6762 and RFC 6763

Multicast DNS (mDNS)

- mDNS is a method of using programming interfaces, packet formats and operating semantics of DNS, in environments where no DNS server exists
- mDNS provides the ability to perform DNS-like operations on the local link where no Unicast DNS server exists
- mDNS designates a portion of the DNS namespace to be free for local use, without the need to pay any annual fee (.local TLD)

Multicast DNS (mDNS)

- mDNS uses APIs similar to unicast DNS but implemented over a multicast
- When a mDNS client wants to know the IP address of a computer given its name, mDNS client sends a request to a well-known multicast address
- the computer with the corresponding A record replies with its IP address
- mDNS ranges are 224.0.0.251 for IPv4 and ff02::fb for IPv6 link-local addressing.

Advantages of mDNS

1) There is no need to administration or configuration to set them up
2) Can work where no infrastructure exists
3) Can work with infrastructure failures

DNS-Based Service Discovery (DNS-SD)

- DNS-based service discovery (DNS-SD) is the other half of Apple's solution, built on top of the DNS
- Apple solution uses DNS messages, in contrast to Microsoft's competing technology and Simple Service Discovery Protocol (SSDP), which uses HTTP messages.
- Use standard DNS queries to discover a list of named instances for a specific service that a client is looking for; called as DNS-based Service Discovery, or DNS-SD

DNS-Based Service Discovery (DNS-SD)

- It is compatible with both mDNS and with unicast DNS server and client software.
- Using DNS-SD with mDNS results in zero-configuration operation. Just connecting a DNS-SD/mDNS device and its services are advertised on the local link with no further user interaction
- When using DNS-SD with unicast DNS, the unicast DNS-SD service does not have to be provided by the same DNS server hardware that is currently providing an organization's conventional host name lookup service

mDNS/DNS-SD Example

- Bonjour TXTrecord (Apple)
  - Device publishes SRV and TXT records for service
    - mDNS/DNS-SD send gratuitous announcement after Probing
    - mDNS/DNS-SD responds to queries per Protocol
    - Device removes SRV and TXT records for service when done
    - mDNS/DNS-SD send gratuitous announcement as goodbye message (TTL of 0)

mDNS/DNS-SD Example (Cont.)

- Establishes mDNS/DNS-SD query for services
- Device discovered when mDNS/DNS-SD
  - receives gratuitous announce for established query
  - receives response to query request
- Device removed when mDNS/DNS-SD
  - receives goodbye message
  - time to live expires without receiving update (timeout)

IoT Gateways & Supported Protocols

	Gateways	Application Protocols					Management		Connectivity			
		RESTful HTTP	COAP	MQTT	XMPP	DDS	OMA-DM	BBF TR-069	Cellular	Zigbee	Bluetooth	WiFi
Practice	Ponte	✓	✓	✓								
	oneM2M	✓	✓	✓			✓	✓	✓	✓	✓	✓
	SmartM2M	✓	✓				✓		✓	✓	✓	✓
	Intel IoT Platform			✓			✓	✓	✓	✓	✓	✓
	LWM2M								✓	✓		✓
Research	IoT Communication Gateway [9]								✓	✓		
	IoT Gateway Centric Model [10]	✓								✓		✓
	HTTP-CoAP Cross Protocol Proxy [11]	✓	✓									
	Semantic Gateway [12]		✓	✓	✓							
	Proposed Enhance MQTT	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓

UbiWare and LinkSmart are examples of middleware that enables the creation and interoperation of heterogeneous IoT services.

TR-069

A technical specification published by the Broadband Forum and defines an application layer protocol for remote management of end-user devices (designed for broadband modems and wired infrastructure).

It is based on SOAP = HTTP + XML ➔ ☹ Not good for IoT.

OMA-DM

OMA Device Management is a device management protocol specified by the Open Mobile Alliance (OMA) Device Management (DM) Working Group and the Data Synchronization (DS) Working Group. Uses HTTP + XML ☹

It support the following features:

- **Provisioning** – Configuration of the device (including first time use), enabling and disabling features
- **Device Configuration** – Allow changes to settings and parameters of the device
- **Software Upgrades** – Provide for new software and/or bug fixes to be loaded on the device, including applications and system software
- **Fault Management** – Report errors from the device, query about status of device

OMA-LWM2M

Like OMA-DM but targets resource constrained devices. It makes use of a light and compact protocol as well as an efficient resource data model. It provides a choice for the M2M Service Provider to deploy a M2M system to provide service to the M2M User. It is frequently used with CoAP.

Open source implementation is available: Eclipse Wakaama and Eclipse Californium.

Use-Case Discussions

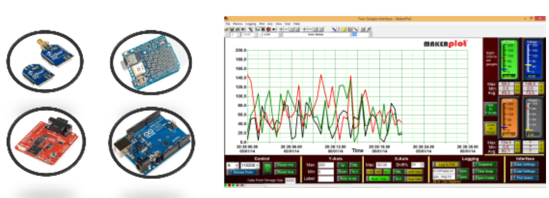
Experiments & Hands-on Practice

Check REST, MQTT, CoAP Examples

- sudo easy_install pip
- sudo easy_install web.py
- sudo pip install httplib2
- sudo pip install paho_mqtt
- git clone git://github.com/Tanganelli/CoAPthon
- python setup.py sdist
- sudo pip install dist/CoAPthon-4.0.0.tar.gz –r requirements.txt
- Check: https://github.com/Tanganelli/CoAPthon
- See attached REST, MQTT, CoAP Examples.

The Arduino Sleuth

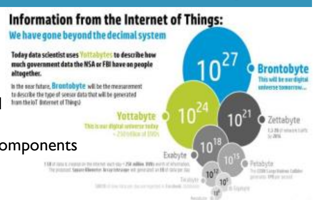
Telemetry System for Electric Vehicle



IoT Challenges & Research

Major Challenges

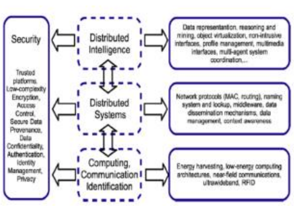
- Society
  - People
  - Security & Privacy
- Technological
  - Advanced Internet Protocol
  - Power efficiency
  - Massive Scaling/Countless components
  - Big Data Explosion
  - Silo IoT Solutions
  - Openness
  - Humans in the Loop



Research Areas

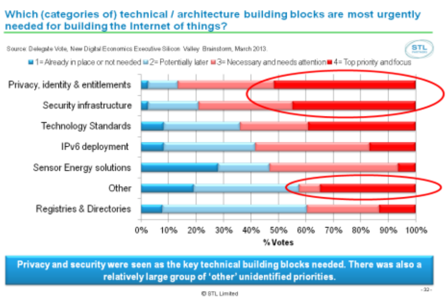
A. *Massive Scaling*
B. *Architecture and Dependencies*
C. *Creating Knowledge and Big Data*
D. *Robustness*
E. *Openness*
F. *Security*
G. *Privacy*
H. *Humans in the Loop*

Taxonomy to Research Areas to IoT

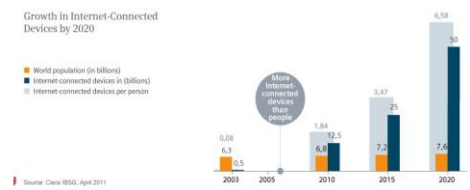


Research Communities

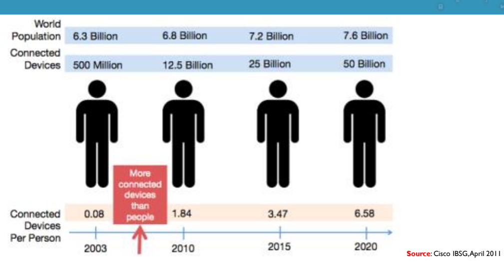
- Internet of Things (IoT)
- Mobile Computing (MC)
- Pervasive Computing (PC)
- Wireless Sensor Networks (WSN)
- Cyber Physical Systems (CPS).



Internet connected things



More Connected Devices Than People



Security and privacy requirements of IoT

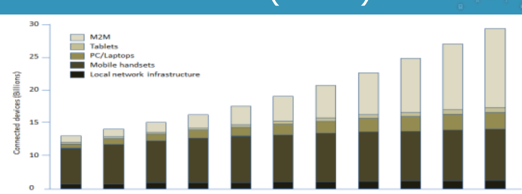
- Resilience to attacks: The system has to avoid single points of failure and should adjust itself to node failures.
- Data authentication: As a principle, retrieved address and object information must be authenticated.
- Access control: Information providers must be able to implement access control on the data provided.
- Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

Future Prospects

IoT and markets

- In terms of marketing, IoT represents a tremendous opportunity for various types of companies
- Based the IoT technologies and services (IoT application and service providers, IoT platform providers and integrators)
- Number of connected devices was grown to 9 billion in 2011 and expected to 50 billion in 2020.

IoT and markets (cont.)



Expected growth in the number of connected devices

Source: GSMA (2011), Connected Life - GSMA Position Paper

IoT and markets (cont.)

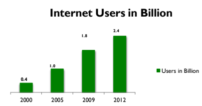
- The most drastic growth is assumed to take place in M2M connections, from 2 billion at the end of 2011 to 12 billion by the end of 2020 (GSMA 2011).
- Cellular technologies are expected to get a 19% share (2.3 billion) of connections by 2020 (GSMA 2011).
- The M2M market is expected to be the largest submarket within the IoT market and M2M is expected to make a total EUR 714 billion in 2020 (Machina Research 2010).

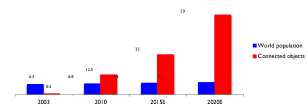
IoT and markets (cont.)

- M2M submarket, GSMA (2011) expects the main vertical segments to be the following:
  - Automotive (revenue opportunity USD 202 billion)
  - Healthcare (revenue opportunity USD 97 billion)
  - Consumer electronics (revenue opportunity USD 445 billion)
  - Utilities (revenue opportunity USD 36 billion).

IoT and markets (cont.)

The number of internet users is restricted by the growth of human population





Source: http://www.internetworldstats.com (for 2012)

IoT and markets (cont.)

- In 2008
- there were more things on the internet than human beings on earth
- In 2020
- 50 billion Things will be connected to the internet according to CISCO
- Some companies are already taking advantage of this revolution

Source: http://www.cisco.com

IoT and markets (cont.)

Compound Annual Growth Rate

Number of items, billion	2010	2011	2012	2013	2014	2015	2016	2017	2020	CAGR (%)
RFID tags										
Passive tags	0.06	0.08	0.10	0.13	0.17	0.22	0.28	0.37	0.80	29.57
Active tags	2.30	3.43	5.11	7.61	11.33	16.89	25.16	37.49	124.00	48.99
Tags, total	2.40	3.56	5.29	7.86	11.67	17.32	25.72	38.19	125.00	48.48
Connected devices										
Connected M2M devices	1.64	2.00	2.44	2.98	3.63	4.43	5.41	6.60	12.00	22.03
Connected devices, total	8.04	8.99	10.05	11.23	12.55	14.02	15.67	17.52	24.45	11.76
Total tags and connected devices	10.44	12.55	15.34	19.08	24.21	31.34	41.39	55.70	149.45	31.68

Number of "things" available, in billions

Source: Oleksiy Mazhelis (2013), internet of things market, value networks, and business models

IoT and markets (cont.)

Number of items, billion	2010	2011	2012	2013	2014	2015	2016	2017	2020	CAGR (%)
Type of communications										
Modules	0.19	0.27	0.39	0.56	0.80	1.16	1.67	2.41	7.22	44.20
WPAN	0.06	0.10	0.17	0.29	0.48	0.80	1.35	2.26	10.70	67.80
WWAN (GSM, CDMA, Satellite, etc.)	0.05	0.07	0.09	0.12	0.15	0.19	0.25	0.32	0.69	29.00
wireline	0.03	0.04	0.05	0.06	0.07	0.09	0.11	0.14	0.25	22.80
Vertical segment										
Consumer electronics	0.16	0.24	0.31	0.50	0.59	0.78	1.14	1.58	4.20	38.56
Healthcare	0.04	0.05	0.07	0.10	0.13	0.18	0.24	0.32	0.77	34.48
Automotive/Transportation	0.09	0.12	0.16	0.21	0.27	0.35	0.47	0.61	1.40	31.58
Utilities	0.07	0.10	0.14	0.18	0.25	0.33	0.45	0.61	1.50	35.11

Number of connected devices shipped or sold, by type of communication and by vertical segments, in billions

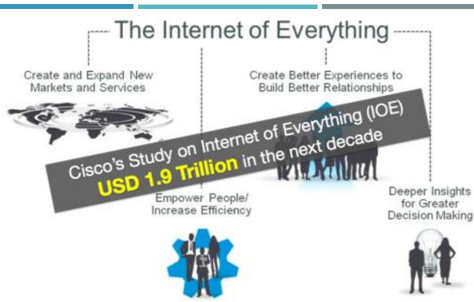
Source: Oleksiy Mazhelis (2013), internet of things market, value networks, and business models

IoT and markets (cont.)

Revenues, USD billion	2010	2011	2012	2013	2014	2015	2016	2017	2020	CAGR (%)
RFID tags										
Tags	2.1	2.5	2.9	3.3	3.9	4.6	5.3	6.2	9.9	16.8
Other (e.g. integration service)	3.5	4.0	4.5	5.1	5.7	6.5	7.3	8.3	12.0	13.1
RFID tags, total	5.6	6.4	7.4	8.4	9.7	11.1	12.7	14.5	21.9	14.6
Connected devices										
Connected devices by level										
Devices	5.2	6.2	7.4	8.9	10.7	12.8	15.4	18.5	32.0	20.0
Network Services	24.5	32.1	42.0	54.9	71.8	93.9	122.8	160.7	359.6	30.8
Horizontal System Application	18.1	23.1	29.6	37.9	48.5	62.1	79.5	101.7	213.3	28.0
Vertical Value Added Applications	68.0	89.6	117.9	155.1	204.1	268.6	353.5	465.2	1060.2	31.6
Connected devices by vertical segment										
Consumer electronics	315.0	332.0	349.9	368.7	388.6	409.5	431.5	454.7	532.2	5.4
Healthcare	1.4	2.0	3.1	4.5	6.9	10.2	15.4	23.0	91.8	50.4
Automotive/ Transportation	13.3	17.5	23.1	30.4	40.0	52.7	69.4	91.4	208.9	31.7
Utilities	6.7	7.9	9.5	11.3	13.4	16.0	19.1	22.8	38.6	19.2
Connected M2M devices, total	121.0	148.7	182.7	224.5	275.9	339.0	416.6	512.0	950.0	22.9
Connected life, total	560.0	629.4	707.3	794.9	893.4	1004.0	1128.3	1268.1	1800.0	12.4

Revenues from tags and connected devices (by level and vertical segment)

Source: Oleksiy Mazhelis (2013), internet of things market, value networks, and business models



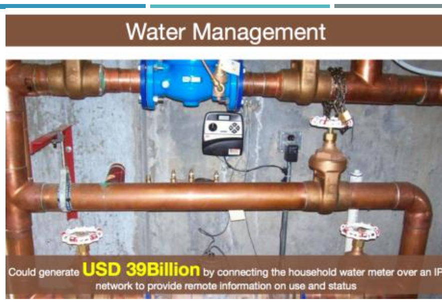
Source: http://www.telecomreseller.com/2014/01/11/cisco-study-says-ioe-can-create-savings/

Smart Building

Source: http://www.teleomreseller.com/2014/01/11/cisco-study-says-ioe-can-create-savings/

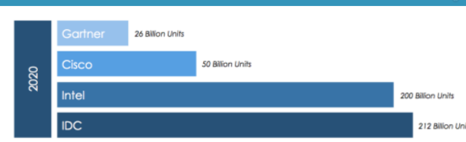
Source: http://www.telecomreseller.com/2014/01/11/cisco-study-says-ioe-can-create-savings/

Source: http://www.telecomreseller.com/2014/01/11/cisco-study-says-ioe-can-create-savings/



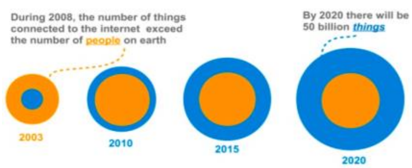
Source: http://www.telecomreseller.com/2014/01/11/cisco-study-says-ioe-can-create-savings/

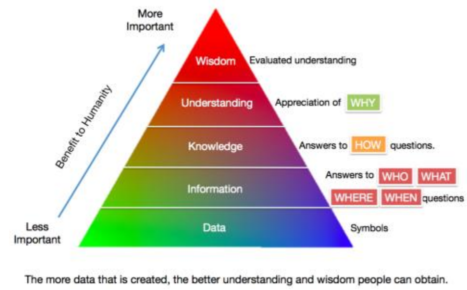
By 2020, How many Devices will exist?



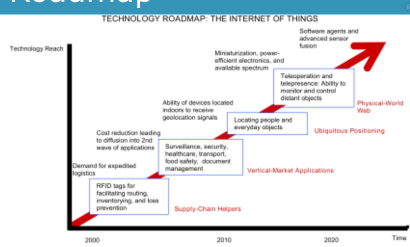
Source:
[1] http://www.gartner.com/newsroom/id/2684616
[2] http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[3] http://share.cisco.com/internet-of-things.html
[4]
http://www.zdnet.com/article/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things/

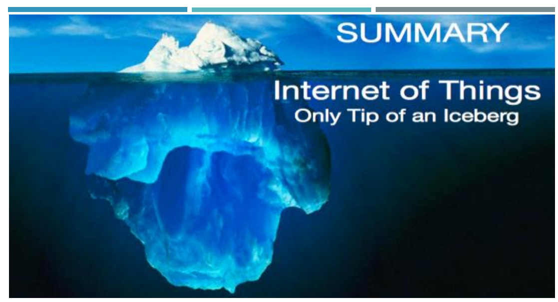
Growth of "Things" Connected to the Internet





IoT Roadmap



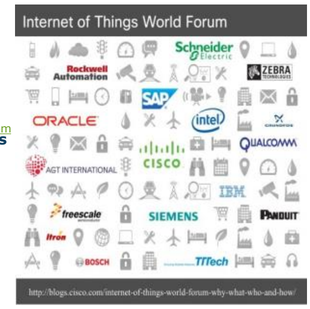


Some Interesting updates

- The term "Internet of Things" was added in oxford dictionary in August, 2013.
  - the term has been defined as : **"A proposed development of the internet in which everyday objects have network connectivity, allowing them to send and receive data."**
- National Intelligence Council (NIC) U.S. listed IoT in the six technologies with potential impacts on U.S. interests out to 2025.
- "**Shodan**", World's first search engine that finds connected 'Things'. For more : www.shodanhq.com
- IoT 2015, 5th international conference on internet of things, going to be held on October, 2015 in Seoul, S. Korea
- The Networking and Information Technology Research and Development (NITRD) program ➔ 15 government agencies ➔ $100s of Millions
- IEEE Internet of Things Journal.

Some Important Links

- IoT World Forum
  http://www.iotwf.com/
- IEEE World Forum on IoT
  http://sites.ieee.org/wf-iot/
- Cisco World Forum
  http://blogs.cisco.com/ioe/
- http://internetofthings.electronicsforu.com



Google's ongoing IoT Projects

- **Google Glass** : Wearable computer
- **Waze** : An intelligent GPS navigation and traffic management tool
- **Nest** : Smart Thermostat and Smoke alarm
- **Open Automotive Alliance(OAA)** : An android operating system for automobiles