Internet of Things

Naeem Khademi

Cyber-Physical Systems, 26.11.2010

UNIVERSITY OF OSLO

Internet of Things

- The Internet of things, also known as the Internet of objects, refers to the networked interconnection of everyday objects
- Described as a *self-configuring* wireless network of sensors whose purpose would be to interconnect all things
- The next generation of Internet applications using IPv6 would be able to communicate with devices attached to virtually all human-made objects because of the extremely large address space of IPv6
- A developer can link real world items to the online world using *RFID tags* and *QR Codes*

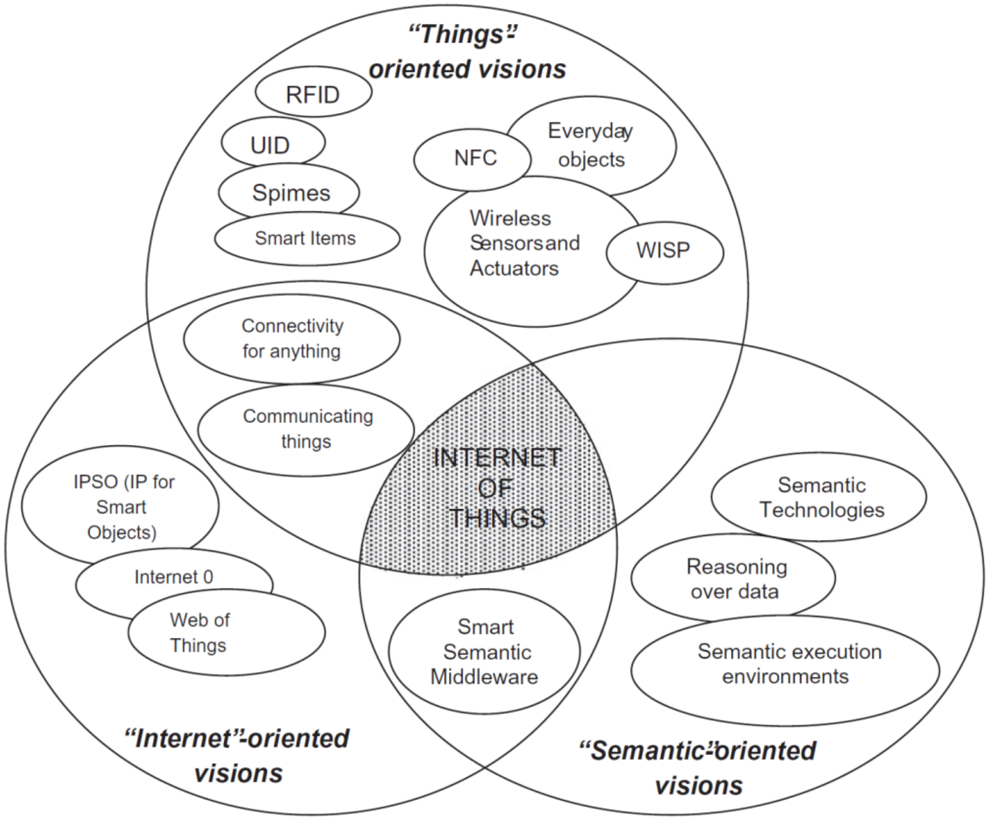
Internet of Things

- **Private users point of view:** domotics (home automation), assisted living, e-health, enhanced learning, etc
- **Business users point of view:** automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods
- **Problematic issues:** full interoperability of interconnected devices, higher degree of smartness, adaptation and autonomous behavior, guaranteeing trust, privacy and security, networking aspects such as computation and energy capacity, resource efficiency and scalability

IoT Visions

- Object oriented (Things oriented)
- Network oriented (Internet oriented)
- Semantic oriented
  - The object unique addressing and the representation and storing of the exchanged information become the most challenging issues

IoT Visions


"Things" oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

IoT Visions (Things oriented)

- RFID Auto-ID Labs, EPCglobal standards to improve object visibility (e.g. traceability, status and location)

- Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) together with RFID as ‘‘the atomic components that will link the real world with the digital world”

- **Spime:** An object that can be tracked through space and time throughout its lifetime and that will be sustainable, enhanceable, and uniquely identifiable (*Smart items* as real-world implementations of *Spimes*)

IoT Visions (Things oriented, some IoT definitions)

- **ITU :** ''from anytime, anyplace connectivity for anyone, we will now have connectivity for anything"

- **European Commission:** ''Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts"

- **Consortium CASAGRAS:** ''a world where things can automatically communicate to computers and each other providing services to the benefit of the human kind" (things oriented + Internet oriented)

IoT Visions (Internet oriented, IPSO)

- **IPSO (IP for Smart Objects) Alliance:** A forum to promote the Internet Protocol as the network technology for connecting Smart Objects around the world.

- **IPSO vision:** The IP stack is a light protocol that already connects a huge amount of communicating devices and runs on tiny and battery operated embedded devices. This guarantees that IP has all the qualities to make IoT a reality.

- Deployment of IoT through a wise IP adaptation and by incorporating IEEE 802.15.4 into the IP architecture

IoT Visions (Internet oriented, Internet Ø)

- **Internet Ø:** Reducing the complexity of the IP stack to achieve a protocol designed to route ‘‘IP over anything”

- Move from the *Internet of Devices* to the *Internet of Things*

IoT Visions (Semantic oriented)

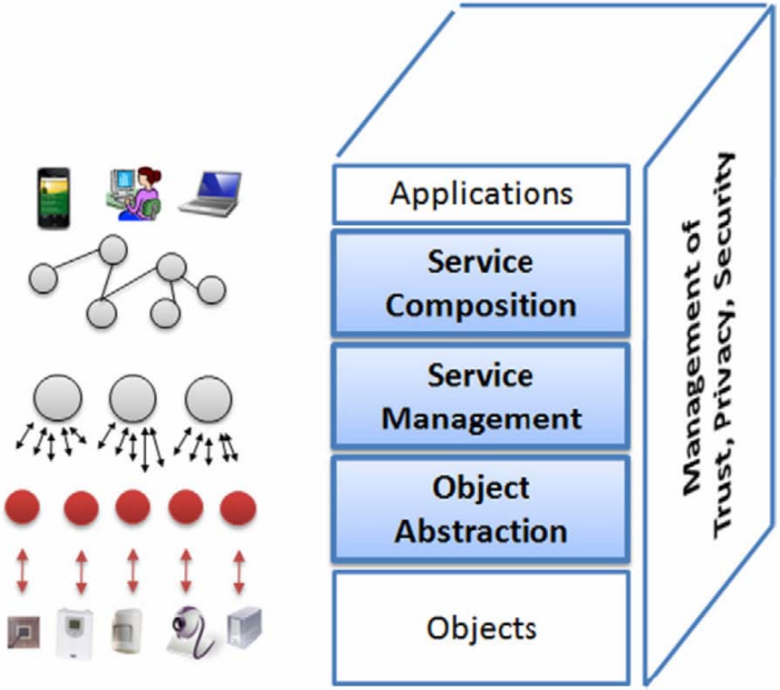
- Appropriate *modeling* solutions for things description
- *Reasoning* over data generated by IoT
- Semantic execution environments
- Scalable storing and communication infrastructure

IoT Visions (Even one more: Web oriented)

- **Web of things:** Web standards are re-used to connect and integrate into the Web everyday-life objects that contain an embedded device or computer

Enabling Technologies

- Identification, sensing and communication technologies
  - RFID (LF or UHF bands)
  - Wireless Sensor Networks
    (802.15.4, multi-hop, report to *sinks*)
- Middleware
  - Applications
  - Service Composition
  - Service Management
  - Object Abstraction
  - Trust, privacy and security management



Enabling Technologies (802.15.4 Sensor Nodes)

- A low power and low bit-rate PHY/MAC for WPANs

- **Problem:** integration of sensor nodes in Internet!

  - Availability of IP addresses
  - The largest PHY packet in IEEE 802.15.4 has 127 bytes; the resulting MAX frame size at the MAC layer is 102 octets, which may further decrease based on the link layer security algorithm utilized. Such sizes are too small when compared to typical IP packet sizes.
  - Sensor nodes spend a large part of their time in a *sleep mode* to save energy and cannot communicate during these periods. This is absolutely anomalous for IP networks.

Enabling Technologies (RFID Sensor Networks)

- **Sensing RFID systems:** RFID sensor networks consisting of small, RFID-based sensing and computing devices, and RFID readers, which are the sinks of the data generated by the sensing RFID tags and provide the power for the network operation.

Enabling Technologies

Comparison between RFID systems, wireless sensor networks, and RFID sensor networks

	Processing	Sensing	Communication	Range (m)	Power	Lifetime	Size	Standard
RFID	No	No	Asymmetric	10	Harvested	Indefinite	Very small	ISO18000
WSN	Yes	Yes	Peer-to-peer	100	Battery	<3 years	Small	IEEE 802.15.4
RSN	Yes	Yes	Asymmetric	3	Harvested	Indefinite	Small	None

Enabling Technologies (Middleware)

- The *middleware* is a software layer or a set of sub-layers interposed between the technological and the application levels

- Applications are on the top of the architecture, exporting all the system's functionalities to the final user

- Service composition on top of a SOA-based middleware provides the functionalities for the composition of single services offered by networked objects to build specific applications. On this layer there is no notion of *devices* and the only visible assets are *services*.

Enabling Technologies (Middleware)

- Service management provides the main functions that are expected to be available for each object and that allow for their management
  - Object dynamic discovery, status monitoring and service configuration
  - Some middleware proposals include functionalities related to the QoS management and lock management, as well as some semantic functions
- Object abstraction is capable of harmonizing the access to the different devices with a common language and procedure
  - *Interface sub-layer* (A web-interface to manage all messaging operations)
  - *Communication sub-layer* (Translates the messages to device-specific commands, e.g. TinyTCP)

Applications

- Transportation and logistics domain
- Healthcare domain
- Smart environment (home, office, plant) domain
- Personal and social domain

Applications

- **Transportation and logistics**
  - Logistics
  - Assisted driving
  - Mobile ticketing
  - Environment monitoring
  - Augmented maps
- **Heathcare**
  - Tracking
  - Identification, authentication
  - Data collection
  - Sensing
- **Smart environments**
  - Comfortable homes/offices
  - Industrial plants
  - Smart museum and gym
- **Personal and social**
  - Social networking
  - Historical queries
  - Losses
  - Thefts
- **Futuristic**
  - Robot taxi
  - City information model
  - Enhanced game room

Open Issues

- Standardization activity
- Addressing and networking issues
- Security and privacy

Open Issues (Standardization Activity)

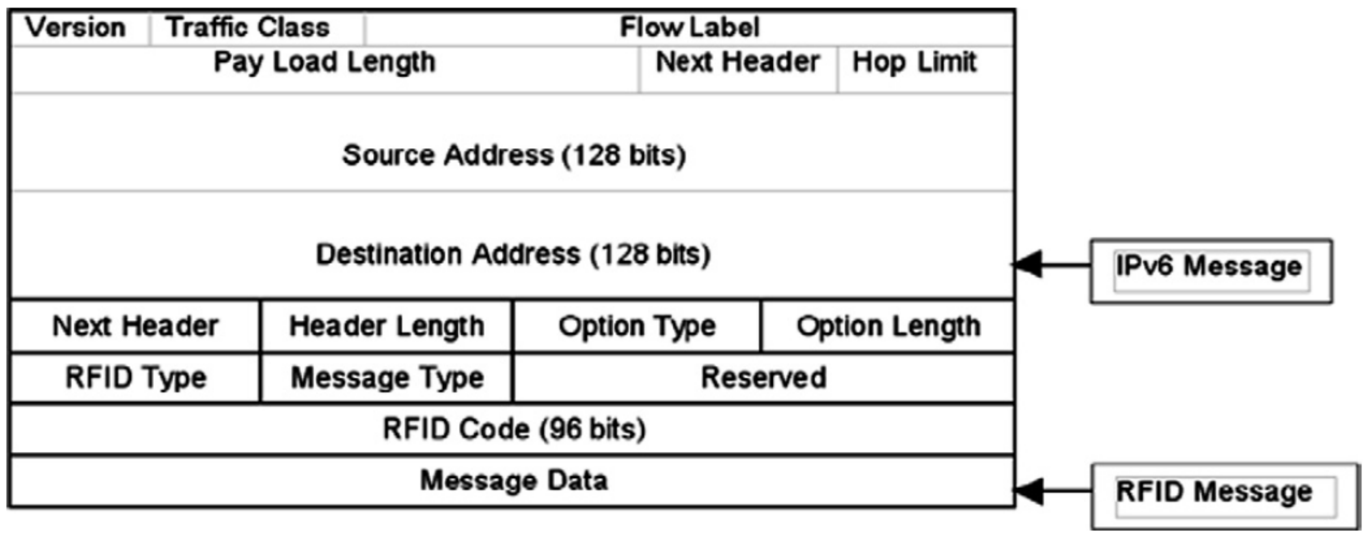
Standard	Objective	Status	Comm. range (m)	Data rate (kbps)	Unitary cost ($)
Standardization activities discussed in this section					
EPCglobal	Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products	Advanced	~ 1	$\sim 10^2$	~ 0.01
GRIFS	European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the *Internet of Things*	Ongoing	~ 1	$\sim 10^2$	~ 0.01
M2M	Definition of cost-effective solutions for machine-to-machine (M2M) communications, which should allow the related market to take off	Ongoing	N.S.	N.S.	N.S.
6LoWPAN	Integration of low-power IEEE 802.15.4 devices into IPv6 networks	Ongoing	10–100	$\sim 10^2$	~ 1
ROLL	Definition of routing protocols for heterogeneous low-power and lossy networks	Ongoing	N.S.	N.S.	N.S.
Other relevant standardization activities					
NFC	Definition of a set of protocols for low range and bidirectional communications	Advanced	$\sim 10^{-2}$	Up to 424	~ 0.1
Wireless Hart	Definition of protocols for self-organizing, self-healing and mesh architectures over IEEE 802.15.4 devices	Advanced	10–100	$\sim 10^2$	~ 1
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced	10–100	$\sim 10^2$	~ 1

Open Issues (Addressing and Networking)

- RFID tags use 64-96 bits identifiers
- IPv6 address is 128 bits
- Integration of RFID tags into IPv6
  - 64 bit RFID tag → Interface identifier of IPv6 address
  - Address of gateway between RFID tag and Internet → Network prefix

This approach can't be used for 96 bits RFID tags!

Open Issues (Addressing and Networking)



Encapsulation of RFID message into an IPv6 packet for 96 bits RFID tags

Open Issues (Addressing and Networking)

- ONS (Object Name Service) instead of DNS
- OCMS (Object Code Mapping Service): P2P approach is suggested to improve scalability

Open Issues (Addressing and Networking)

- New conception of Transport Layer for IoT (Problems)
  - Unnecessary Connection setup in TCP (three-way handshaking)
  - Performance problems of TCP Congestion control for a very small sessions
  - Data buffering in TCP both at the source and destination

Open Issues (Privacy and Security)

- IoT is extremely vulnerable to attacks
  - Components spend most of the time unattended (physical attack)
  - Most of the communications are wireless (eavesdropping)
  - IoT components are simple and low-energy (can't implement complex security schemes)
- Major problems: authentication and data integrity

Open Issues (Privacy and Security)

- Authentication
  - Proxy attack (*man-in-the-middle* attack)
- Data integrity
  - Read-Write memory protection in tags against end nodes
  - Hash Message Authentication Code (H-MAC) against intermediate nodes

References

1. Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A survey, Computer Networks, Volume 54, Issue 15, 28 October 2010, Pages 2787-2805, ISSN 1389-1286
2. http://en.wikipedia.org/wiki/Internet_of_Things

Thank You

Questions?