The Internet of Things: A survey

Luigi Atzori, Antonio Iera & Giacomo Morabito

Computer Networks 2010

Presenter - Bob Kinicki

Internet of Things

Fall 2015

Outline

- Introduction
- Visions
- Enabling Technologies
- Middleware
- Applications {will be skipped here}
- Open Issues
- Conclusions

Introduction

- 2010 view starts with the concept of a pervasive set of objects that can interact with each other and cooperate with their neighbors to reach common goals. Authors coming from the RFID space.
- IoT is expected to have high impact both positively and negatively (disruptive technologies and potential threats).
- Central issues are full interoperability of interconnected devices and more smartness while guaranteeing trust, privacy and security.

- Authors trying to describe different visions.

Three Visions

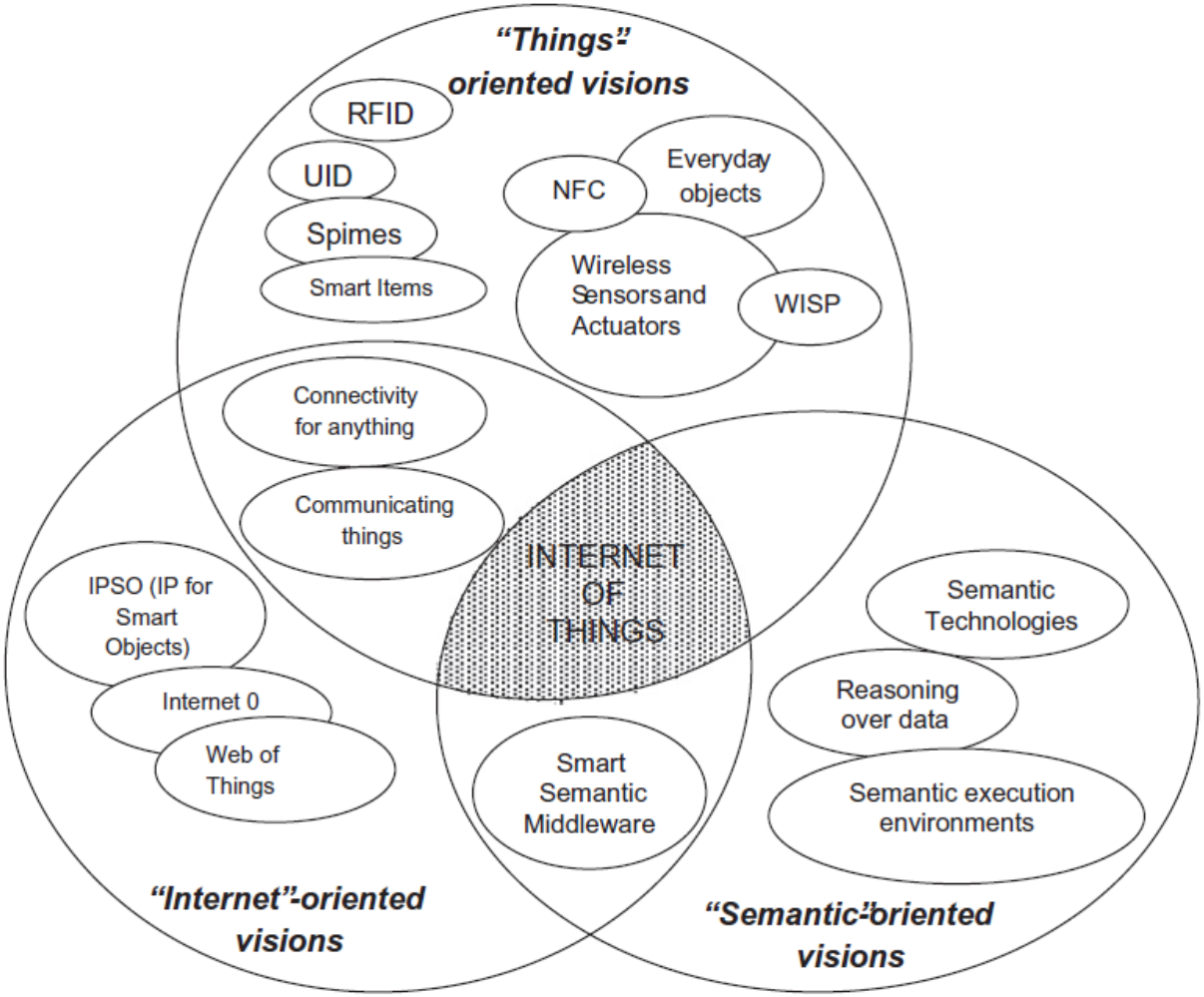

Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

One Definition

"Internet of Things semantically means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols."

Challenges include object unique addressing and the representation and storing of exchanged information.

RFID Viewpoint

- EPC (Electronic Product Code)
  - Standards to improve object visibility (traceability and awareness of an object)
- Mere object identification is NOT wide enough vision of IoT.
- RFID, NFC and WSAN (Wireless Sensor and Actuator Networks) seen as "atomic elements" of IoT.

Things Vision

- Smart items can relate to concept of a spime.
- Spime:: an object that can be tracked through space and time throughout its lifetime and will be sustainable, enhanceable and uniquely identified.

Internet Vision

- IPSO (IP for Smart Objects) Alliance promotes Internet-oriented vision and claims wise IP adaptation with IEEE802.15.4 and 6LowPAN will enable IoT automatically.
- IPSO and Internet O advocate simplification of IP to make it adaptable to any object.

Semantic Vision

- Issues involved with handling IoT object information is very challenging and modeling, reasoning and semantic execution environments and architectures will be needed to address the scalability of storing and communicating about IoT objects.

Enabling Technologies

- Interested in the role each technology will play in the IoT.
- Identification, sensing and communication
  - Wireless
    - RFID (passive, semi-passive and active)
    - WSNs
      - 802.15.4 in most commercial WSNs already
    - Integration of these two
    - RSNs (RFID Sensing Networks)

Middleware

- Layers between the technology and the application.
- Some propose SOA (Service Oriented Architecture) approach for middleware
  - e.g., designed workflows of coordinated services which are associated with object actions.
  - Goal is complete, integrated approach.

Figure 2 SOA-based Architecture

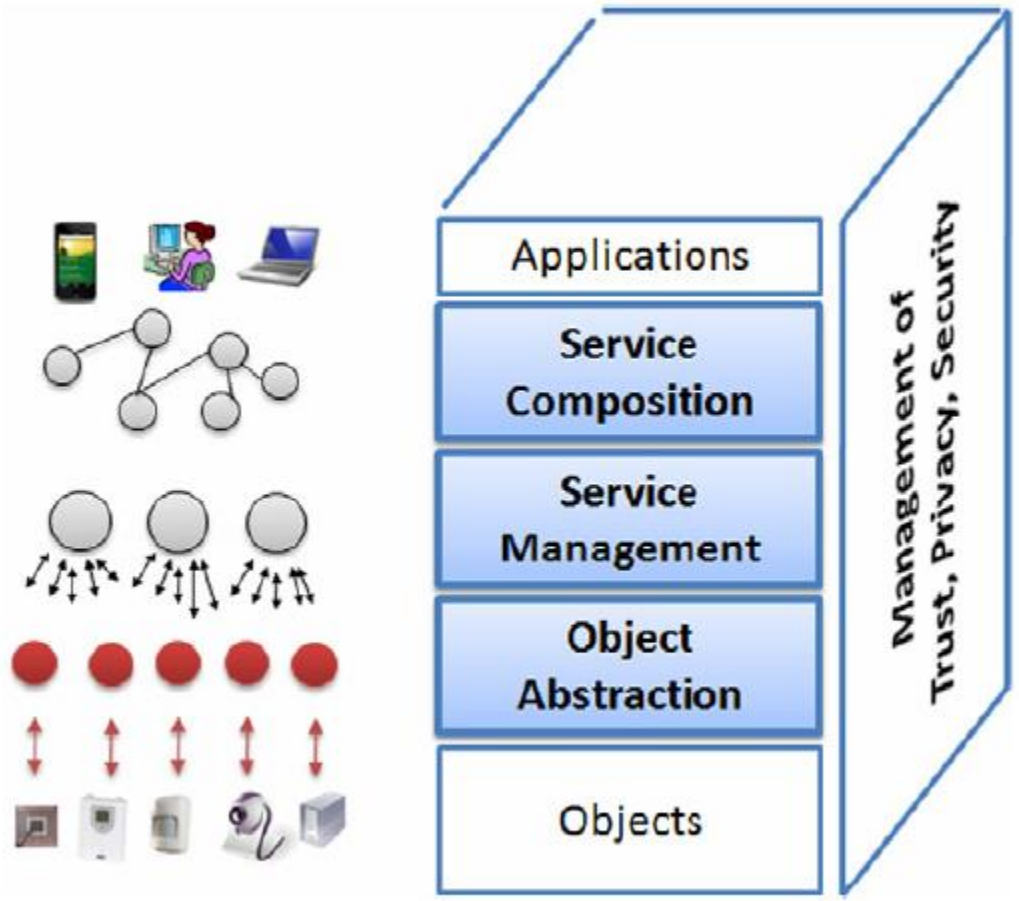

Fig. 2. SOA-based architecture for the IoT middleware.

Service Composition

- Provides functionality for the composition of services offered by objects to build applications.
- Workflow languages here such as Web Service Definition Language (WSDL).

Service Management

- Basic set of services encompass:
  - Object dynamic discovery
  - Status monitoring
  - Service configuration
- Functionalities related to QoS and lock management.

Object Abstraction

- Need an abstraction layer to handle heterogeneous set of objects to harmonize the access with common language and procedures.
- Speak of a wrapping layer to handle:
  - Web interface
  - Second interface converts service methods into device-specific commands for communicating with objects.

Object Abstraction

- Some propose embedded stack in devices to provide wrapping function.
- However, more often direction is for a proxy which uses socket style communication with device.

Trust, Privacy and Security

- Personal objects communicating potentially enables a surveillance system.
- Hence middleware must manage trust, privacy and security.

Final Comment – Not all proposed middleware follow the model shown in Figure 2.

Open Research Issues

Table 2
Open research issues.

Open issue	Brief description of the cause	Details in
Standards	There are several standardization efforts but they are not integrated in a comprehensive framework	Section 5.1
Mobility support	There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems	Section 5.2
Naming	Object Name Servers (ONS) are needed to map a reference to a description of a specific object and the related identifier, and *vice versa*	Section 5.2
Transport protocol	Existing transport protocols fail in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in *objects*	Section 5.2
Traffic characterization and QoS support	The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes	Section 5.2
Authentication	Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is a serious problem	Section 5.3
Data integrity	This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection	Section 5.3
Privacy	A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques	Section 5.3
Digital forgetting	All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years	Section 5.3

Standardization

Table 3
Characteristics of the most relevant standardization activities.

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	~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	~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	~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	~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	~10^2	~1
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced	10–100	~10^2	~1

Addressing and Networking

- RFID tags using 64-96 bits (standardized by EPCglobal) complicates IPv6 128 bit addressing.
- Integration and mapping strategies for these two addressing schemes have been proposed.
- Support of mobile in IoT is important.
  - Suggest Mobile IP approach with home agent.

Addressing and Networking

- Need ONS (Object Name Service) to supersede DNS.
  - need to associate description of specified object to a given RFID tag identifier.
- Additional need for the inverse OCMS (Object Code Mapping Service).

Addressing and Networking

- TCP not effective for IoT {maybe CoAP with REST}.
- Traffic characteristics in WSNs.
- Rsearch in QoS support for IoT is needed.
  - Some done already in QoS for M2M.

Security

- Authentication is a major problem as current authentication procedures are not feasible in the IoT.
- There are no curent solutions in the IoT space for proxy attacks and man-in-the-middle attacks.
- Data integrity gets more complicated when you have unattended nodes like RFID tags.

Security

- Cryptography solutions expend energy and bandwidth resources at both source and destination and therefore cannot be readily applied to IoT.
- Some light symmetric key schemes have been proposed.

Privacy

- Concerns about privacy protection have been a significant barrier against diffusion of the technologies involved in IoT.
- Unlike the Internet where privacy problems mostly arise from active users, IoT privacy problem scenarios can threaten even for people not using any IoT service.

Privacy

- In tracking systems, position movement of individual users needs to handled in terms of aggregate users. Namely, this motion information should not be linkable to identities.
- People need to be informed about the scope of the tracking information.
- Tracking info collected should be processed and then deleted (e.g., heating and lighting controls).

Privacy

- W3C group has defined the Platform for Privacy Preferences (P3P) which provides descriptive language for preferences and policies.
- Very challenging task in sensor networks e.g., surveillance cameras.
- RFID tags are problematic.
- Proposed privacy broker proxies do not scale.
- Need for "digital forgetting".

Conclusions

- IoT has potential to add a new dimension to the concept of moving the interactions between people at a virtual level on the Internet.
- This potential comes from enabling communication among smart objects.
- Paper surveys most important aspects of IoT emphasizing current activities and challenges.