From Ubiquitous Computing to Internet of Everything: Challenges and Opportunities

Paul Patras
## Hype or genuine evolution?

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1988</td>
<td>Mark Weiss (Xerox PARC) – Ubiquitous Computing</td>
</tr>
<tr>
<td></td>
<td>“…hundreds of wireless computing devices per person per office,… This is different from PDA’s, dynabooks, or information at your fingertips. It is invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere.… its highest ideal is to make a computer so imbedded, so fitting, so natural, that we use it without even thinking about it.”</td>
</tr>
<tr>
<td></td>
<td>“In retrospect it looks like the rapid growth of the World Wide Web may have been just the trigger charge that is now setting off the real explosion, as things start to use the Net.”</td>
</tr>
<tr>
<td>2005</td>
<td>Kevin Ashton (Auto-ID @ MIT) – Internet of Things</td>
</tr>
<tr>
<td></td>
<td>“We need an internet for things, a standardized way for computers to understand the real world”</td>
</tr>
<tr>
<td>2009</td>
<td>ITU Internet Report: The Internet of Things</td>
</tr>
<tr>
<td></td>
<td>“always on communications, in which new ubiquitous technologies (such as radio-frequency identification and sensors) promise a world of networked and interconnected devices (e.g. fridge, television, vehicle, garage door, etc.) that provide relevant content and information wherever the location of the user – heralding the dawn of a new era, one in which the internet (of data and people) acquires a new dimension to become an Internet of Things.”</td>
</tr>
<tr>
<td>2013</td>
<td>EC, IoT — An action plan for Europe</td>
</tr>
<tr>
<td></td>
<td>“network of interconnected objects, from books to cars, from people, processes, data, and things to make every interaction valuable than ever before – turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and so many, so many countries.”</td>
</tr>
<tr>
<td></td>
<td>Cisco – coins Internet of Everything (IoE) brings together people, processes, data, and things to make each new connection more relevant and valuable than ever before – turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and so many, so many countries.”</td>
</tr>
</tbody>
</table>

"""
Numerous opportunities

- Healthcare and assisted living
- Transportation
- Environment monitoring and agriculture
- Smart buildings
- Many more
Interconnecting many devices that exchange (big) data is challenging

How to model and predict the behaviour of complex systems?

How to ensure reliable connectivity and optimally share communications infrastructure?

How to aggregate large data sets and exploit only context specific information in real-time?

How to preserve user privacy while achieving some utility from data processing?

How to ensure Internet-connected ‘things’ are secure and easy to use?
Different perspectives needed

UK researchers wrote Ubicomp manifesto in 2006* – some challenges facing ubiquitous system design still hold

**Theoretical perspective:** rigorous models that capture system behaviour at different levels of abstraction.

**Engineering perspective:** architectural and network challenges posed by large scale, heterogeneous, and dynamic nature.

**Experience perspective:** understand what principles underpin human-machine interaction and how a ubiquitous computing society might be shaped from a socio-technical perspective.

---

Application specific challenges

Computationally/energy constrained vs unconstrained devices

Communication type (decentralised vs scheduled and range (long vs short)

User interface (display, keys, touch, voice, gestures)
Example: Wristband fitness trackers (activity, sleep, heart rate monitoring)
Operation model

Stage 1: Fitness Band
Stage 2: Smartphone
Stage 3: Server

Adapted from securelist.com
Surveillance at 10,000m

13 devices detected within <1 minute
Security still an afterthought

- Intercepting sensitive personal information is possible
- Injection of fake activity reports to gain rewards
- Compromising victim’s personal statistics

Smart Homes

A range of appliances controllable via a mobile app

Source: eurocomms.com
Obvious benefits...

• Lower carbon footprint

• Personalisation (access control)

• Increased comfort and safety (?)
...come with risks

• Communication again wireless and subject to abuse

• Control via software (app) – risk of malware and privileges abuse

• Hijacking and weaponisation
Example: Taking down a surveillance camera

- Wireless camera
- Home wireless router
- Impersonate home router
- Rogue access point

Steps:
- De-authentication
- Re-authentication + Video stream interception
Example: Faking IoT device and exploiting generous app permission
Example: Faking IoT device and exploiting generous app permission

- Possible to ask phone app to send photos taken by user, list of contacts, and other sensitive information
What we can do

Help design systems with scalability in mind.

Work to achieve strong encryption with limited computing capabilities.

Standardise security by design.

Define sustainable development of new devices.

Train developers/engineers that understand embedded systems, programming, and security.