

1

Preliminaries, Motivation, and Related Work

1.1 What is the Internet of Things?

The Internet of Things (IoT) encapsulates a vision of a world in which billions of objects with embedded intelligence, communication means, and sensing and actuation capabilities will connect over IP (Internet Protocol) networks. Our current Internet has undergone a fundamental transition, from hardware-driven (computers, fibers, and Ethernet cables) to market-driven (Facebook, Amazon) opportunities. This has come about due to the interconnection of seemingly disjoint intranets with strong horizontal software capabilities. The IoT calls for open environments and an integrated architecture of interoperable platforms. Smart objects and cyber-physical systems – or just “things” – are the new IoT entities: the objects of everyday life, augmented with micro-controllers, optical and/or radio transceivers, sensors, actuators, and protocol stacks suitable for communication in constrained environments where target hardware has limited resources, allowing them to gather data from the environment and act upon it, and giving them an interface to the physical world. These objects can be worn by users or deployed in the environment. They are usually highly constrained, with limited memory and available energy stores, and they are subject to stringent low-cost requirements. Data storage, processing, and analytics are fundamental requirements, necessary to enrich the raw IoT data and transform them into useful information. According to the “Edge Computing” paradigm, introducing computing resources at the edge of access networks may bring several benefits that are key for IoT scenarios: low latency, real-time capabilities and context-awareness. Edge nodes (servers or micro data-centers on the edge) may act as an interface to data

streams coming from connected devices, objects, and applications. The stored Big Data can then be processed with new mechanisms, such as machine and deep learning, transforming raw data generated by connected objects into useful information. The useful information will then be disseminated to relevant devices and interested users or stored for further processing and access.

1.2 Wireless Ad-hoc and Sensor Networks: The Ancestors without IP

Wireless sensor networks (WSNs) were an emerging application field of microelectronics and communications in the first decade of the twenty-first century. In particular, WSNs promised wide support of interactions between people and their surroundings. The potential of a WSN can be seen in the three words behind the acronym:

- “Wireless” puts the focus on the freedom that the elimination of wires gives, in terms of mobility support and ease of system deployment;
- “Sensor” reflects the capability of sensing technology to provide the means to perceive and interact — in a wide sense — with the world;
- “Networks” gives emphasis to the possibility of building systems whose functional capabilities are given by a plurality of communicating devices, possibly distributed over large areas.

Pushed on by early military research, WSNs were different from traditional networks in terms of the communication paradigm: the address-centric approach used in end-to-end transmissions between specific devices, with explicit indication of both source and destination addresses in each packet, was to be replaced with an alternative (and somewhat new) data-centric approach. This “address blindness” led to the selection of a suitable data diffusion strategy — in other words, communication protocol — for data-centric networks. The typical network deployment would consist of the sources placed around the areas to be monitored and the sinks located in easily accessible places. The sinks provided adequate storage capacity to hold the data from the sources. Sources might send information to sinks in accordance with different scheduling policies: periodic (i.e., time-driven), event specific (i.e., event-driven), a reply in response to

requests coming from sinks (i.e., query-driven), or some combination thereof.

Because research focused on the area, WSNs have typically been associated with ad-hoc networks, to the point that the two terms have almost become – although erroneously so – synonymous. In particular, ad-hoc networks are defined as general, infrastructure-less, cooperation-based, opportunistic networks, typically customized for specific scenarios and applications. These kinds of networks have to face frequent and random variations of many factors (radio channel, topology, data traffic, and so on), implying a need for dynamic management of a large number of parameters in the most efficient, effective, and reactive way. To this end, a number of key research problems have been studied, and solutions proposed, in the literature:

- self-configuration and self-organization in infrastructure-less systems;
- support for cooperative operations in systems with heterogenous members;
- multi-hop peer-to-peer communication among network nodes, with effective routing protocols;
- network self-healing behavior providing a sufficient degree of robustness and reliability;
- seamless mobility management and support of dynamic network topologies.

1.3 IoT-enabled Applications

The IoT touches every facet of our lives. IoT-enabled applications are found in a large number of scenarios, including: home and building automation, smart cities, smart grids, Industry 4.0, and smart agriculture. In each of these areas, the use of a common (IP-oriented) communication protocol stack allows the building of innovative applications. In this section, we provide a concise overview of potential applications in each of these areas.

1.3.1 Home and Building Automation

As the smart home market has seen growing investment and has continued to mature, ever more home automation applications have

appeared, each designed for a specific audience. The result has been the creation of several disconnected vertical market segments. Typical examples of increasingly mainstream applications are related to home security and energy efficiency and energy saving. Pushed by the innovations in light and room control, the IoT will foster the development of endless applications for home automation. For example, a typical example of an area of home automation that is destined to grow in the context of the IoT is in healthcare, namely IoT-enabled solutions for the physically less mobile (among others, the elderly, particularly relevant against a background of aging populations), and for the disabled or chronically ill (for instance, remote health monitoring and air-quality monitoring). In general, building automation solutions are starting to converge and are also moving, from the current applications in luxury, security and comfort, to a wider range of applications and connected solutions; this will create market opportunities. While today's smart home solutions are fragmented, the IoT is expected to lead to a new level of interoperability between commercial home and building automation solutions.

1.3.2 Smart Cities

Cities are complex ecosystems, where quality of life is an important concern. In such urban environments, people, companies and public authorities experience specific needs and demands in domains such as healthcare, media, energy and the environment, safety, and public services. A city is perceived more and more as being like a single “organism”, which needs to be efficiently monitored to provide citizens with accurate information. IoT technologies are fundamental to collecting data on the city status and disseminating them to citizens. In this context, cities and urban areas represent a critical mass when it comes to shaping the demand for advanced IoT-based services.

1.3.3 Smart Grids

A smart grid is an electrical grid that includes a variety of operational systems, including smart meters, smart appliances, renewable energy resources, and energy-efficient resources. Power line communications (PLC) relate to the use of existing electrical cables to transport data and have been investigated for a long time. Power utilities have been using this technology for many years to send or receive (limited amounts of)

data on the existing power grid. Although PLC is mostly limited by the type of propagation medium, it can use existing wiring in the distribution network. According to EU's standards and laws, electrical utility companies can use PLC for low bit-rate data transfers (with data rates lower than 50 Kbps) in the 3–148 kHz frequency band. This technology opens up new opportunities and new forms of interactions among people and things in many application areas, such as smart metering services and energy consumption reporting. This makes PLC an enabler for sensing, control, and automation in large systems spread over relatively wide areas, such as in the smart city and smart grid scenarios. On top of PLC, one can also adopt enabling technologies that can improve smart automation processes, such as the IoT. For instance, the adoption of the PLC technology in industrial scenarios (e.g., remote control in automation and manufacturing companies), paves the way to the “Industrial IoT”. Several applications have been enabled by PLC technology's ability to recover from network changes (in terms of repairs and improvements, physical removal, and transfer function) mitigating the fallout on the signal transmission.

Nevertheless, it is well known that power lines are far from ideal channels for data transmission (due to inner variations in location, time, frequency band and type of equipment connected to the line). As a result there has been increasing interest in the joint adoption of IoT and PLC paradigms to improve the robustness of communication. This has led to the suggestion of using small, resource-constrained devices (namely, IoT), with pervasive computing capabilities, and internet standard solutions (as proposed by Internet standardization organizations, such as IETF, ETSI and W3C). Such systems can be key components for implementing future smart grids.

1.3.4 Industrial IoT

The Industrial Internet of Things (IIoT) describes the IoT as used in industries such as manufacturing, logistics, oil and gas, transportation, energy/utilities, mining and metals, aviation and others. These industries represent the majority of gross domestic product among the G20 nations. The IIoT is still at an early stage, similar to where the Internet was in the late 1990s. While the evolution of the consumer Internet over the last two decades provides some important lessons, it is unclear how much of this learning is applicable to the IIoT, given its unique scope and requirements. For example, *real-time* responses are

often critical in manufacturing, energy, transportation and healthcare: real time for today's Internet usually means a few seconds, whereas real time for industrial machines involves sub-millisecond scales. Another important consideration is reliability. The current Internet embodies a "best effort" approach, which provides acceptable performance for e-commerce or human interactions. However, the failure of the power grid, the air traffic control system, or an automated factory for the same length of time would have much more serious consequences.

Much attention has been given to the efforts of large companies such as Cisco, GE, and Huawei, and government initiatives such as Industrie 4.0 in Germany. For example:

- GE announced that it realized more than \$1 billion in incremental revenues in 2014 by helping customers improve asset performance and business operations through IIoT capabilities and services.
- The German government is sponsoring "Industrie 4.0", a multi-year strategic initiative that brings together leaders from the public and private sectors as well as from academia to create a comprehensive vision and action plan for applying digital technologies to the German industrial sector.
- Other European countries have their own industrial transformation projects in which the IIoT takes center stage, such as Smart Factory (the Netherlands), Industry 4.0 (Italy), Industry of the Future (France), and others.
- China has also recently launched its "Made in China 2025" strategy to promote domestic integration of digital technologies and industrialization.

As the IIoT gains momentum, one of the biggest bottlenecks faced is the inability to share information between smart devices that may be speaking different "languages". This communication gap stems from the multiple protocols used on factory floors. So, while you can put a sensor on a machine to gather data, the ability to push that information across a network and ultimately "talk" with other systems is a bit more difficult. Standardization is therefore a key aspect of the IIoT.

The IIoT's potential payoff is enormous. Operational efficiency is one of its key attractions, and early adopters are focused on these benefits. By introducing automation and more flexible production techniques, for instance, manufacturers could boost their productivity by as much as 30%. In this context, three IIoT capabilities must be mastered:

- *sensor-driven computing*: converting sensed data into insights (using the industrial analytics described below) that operators and systems can act on;
- *industrial analytics*: turning data from sensors and other sources into actionable insights;
- *intelligent machine applications*: integrating sensing devices and intelligent components into machines.

1.3.5 Smart Farming

Modern agriculture is facing tremendous challenges as it attempts to build a sustainable future across different regions of the globe. Examples of such challenges include population increase, urbanization, an increasingly degraded environment, an increasing trend towards consumption of animal proteins, changes in food preferences as a result of aging populations and migration, and of course climate change. A modern agriculture needs to be developed, characterized by the adoption of production processes, technologies and tools derived from scientific advances, and results from research and development activities.

Precision farming or smart agriculture is an area with the greatest opportunities for digital development but with the lowest penetration, to date, of digitized solutions. The farming industry will become arguably more important than ever before in the next few decades. It could derive huge benefits from the use of environmental and terrestrial sensors, applications for monitoring the weather, automation for more precise application of fertilizers and pesticides (thus reducing waste of natural resources), and the adoption of planning strategies for maintenance.

Smart farming is already becoming common, thanks to the application of new technologies, such as drones and sensor networks (to collect data) and cloud platforms (to manage the collected data). The set of technologies used in smart farming are as complex as the activities run by farmers, growers, and other stakeholders in the sector. There is a wide spectrum of possible applications: fleet management, livestock monitoring, fish farming, forest care, indoor city farming, and many more. All of the technologies involved revolve around the concept of the IoT and aim at supporting farmers in their decision processes through decision-support systems. They involve real-time data at a level of granularity not previously possible. This

enables better decisions to be made, translating into less waste and an increase in efficiency.

Communication technologies are a key component of smart agriculture applications. In particular, wireless communication technologies are attractive, because of the significant reduction and simplification in wiring involved. Various wireless standards have been established. One can group these into two main categories, depending on the transmission range:

- *Short-range communication*: including standards for:
 - wireless LAN, used for Wi-Fi, namely IEEE 802.11
 - wireless PAN, used more widely for measurement and automation applications, such as IEEE 802.15.1 (Bluetooth) (IEEE, 2002) and IEEE 802.15.4 (ZigBee/6LoWPAN) (IEEE, 2003).

All these standards use the instrumentation, scientific and medical (ISM) radio bands, typically operating in the 2.400–2.4835 GHz band.

- *Long-range communication*: including the increasingly important sub-gigahertz IoT communication technologies, such as LoRA, in the 868–870 MHz band. These trade data transmission rates (on the order of hundreds of kbit/s) for longer transmission ranges.

Communication technologies can be also classified according to the specific application:

- environmental monitoring (weather monitoring and geo-referenced environmental monitoring)
- precision agriculture
- machine and process control (M2M communications)
- facility automation
- traceability systems.