Building the Internet of Things with IPv6 and MIPv6

The Evolving World of M2M Communications

Daniel Minoli

WILEY

BUILDING THE INTERNET OF THINGS WITH IPv6 AND MIPv6

BUILDING THE INTERNET OF THINGS WITH IPv6 AND MIPv6

The Evolving World of M2M Communications

DANIEL MINOLI

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Minoli, Daniel, 1952–
Building the internet of things (IoT) with IPv6 and MIPv6 / Daniel Minoli.
pages cm
ISBN 978-1-118-47347-4 (hardback)
1. Embedded Internet devices. 2. Internet of things. 3. TCP/IP (Computer network protocol) 4. Mobile computing. I. Title.
TK7895.E43M56 2013
004.6′2–dc23

2012049072

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For Anna

CONTENTS

PREFACE

The proliferation of an enlarged gamut of devices able to be directly connected to the Internet is leading to a new ubiquitous-computing paradigm: the Internet of Things (IoT). The IoT is a new type of Internet application that endeavors to make the thing's information (whatever that may be) available on a global scale. It has two attributes: (i) being an Internet application, and (ii) dealing with thing's information. The IoT is predicated on the expansion of the scope, network reach, and possibly even architecture of Internet through the inclusion of physical, instrumented objects. IoT aims at providing smarter services to the environment or the end-user as more *in situ*, transferable data becomes available. Thus, the IoT is seen as a new-generation information network that realizes machine-to-machine communication. The IoT eliminates time and space isolation between geographical space and virtual space, forming what proponents label as "smart geographical space," and creating new human–environment relationships. The latter implies that the IoT can advance the goal of integration of human beings and their surroundings. Applications range from energy efficiency to logistics, and many more.

At the "low end" of the spectrum, the thing's information is typically coded by the Unique Identification (UID) and/or Electronic Product Code (EPC); the information is (typically) stored in a Radio Frequency Identification (RFID) electronic tag; and, the information is uploaded by noncontact reading using an RFID reader. More generally, smart cards (SCs) will also play an important role in IoT; SCs typically incorporate a microprocessor and storage. At the mid-range of the spectrum one finds devices with embedded intelligence (microprocessors) and embedded active wireless capabilities to perform a variety of data gathering and possibly control functions. On-body biomedical sensors (supporting body area networks), home appliance and power management, and industrial control are some examples of these applications. At the

other end of the spectrum, more sophisticated sensors can be employed in the IoT: some of these sensor approaches use distributed wireless sensor networks (WSNs) systems that can collect, process, and forward a wide variety of environmental data such as temperature, atmospheric and environmental chemical content, or even low or high resolution ambient video images from geographic dispersed locations; these objects may span a city, region, or large distribution grid.

The IoT is receiving a large amount of interest on the part of researchers, with thousands of papers published on this topic in the recent past. While specific applications have existed for several years, perhaps supported on private enterprise networks, Internet-based systems along with system supporting a broader application scope are now beginning to be deployed. *The capabilities offered by IP Version 6 (IPv6) are critical to the wide-spread deployment of the technology.*

This text aims at exploring these evolving trends and offering practical suggestions of how these technologies can be implemented in the service provider networks to support cost-effective applications, and how new revenue-generating services could be brought to the market. All the latest physical layer, MAC layer, and upper layer IoT and Machine to Machine (M2M) protocols are discussed.

Planners are asking questions such as: What is the Internet of Things? How does M2M apply? How can it help my specific operation? What is the cost of deploying such a system? Will standardization help? What are the security implications? This text addresses the following IoT aspects: evolving wireless standards, especially low energy and medical applications; IPv6 technologies; Mobile IPv6 (MIPv6) technologies; applications; key underlying technologies for IoT applications; implementation approaches; implementation challenges; and mid-range and long-range opportunities.

More specifically, the text reviews the latest technologies, the emerging commercial applications (especially health care), and the recently evolving standards, including all layers of the protocol stack applicable to IoT/M2M. The text focuses on extensively IPv6, MIPv6, and 6LowPAN/RPL and argues that the IoT/M2M may be the killer app for IPv6. It covers the latest standards supporting the IoT and the M2M applications, including home area networking (HAN), AMI, IEEE 802.15.4, 6LowPAN/RPL, Smart Energy 2.0, ETSI M2M, ZigBee IP (ZIP); ZigBee Personal Home and Hospital Care (PHHC) Profile; IP in Smart Objects (IPSO); BLE; IEEE 802.15.6 wireless body area networks (WBAN); IEEE 802.15 WPAN Task Group 4j (TG4j) medical body area networks; ETSI TR 101 557; near field communication (NFC); dedicated short-range communications (DSRC)/WAVE and related protocols; the Internet Engineering Task Force (IETF) IPv6 Routing Protocol for Low power and lossy networks (RPL)/Routing Over Low power and Lossy networks (ROLL); IETF Constrained Application Protocol (CoAP); IETF Constrained RESTful environments (CoRE); 3rd Generation Partnership Project (3GPP) Machine-Type Communications (MTC); long term evolution (LTE) cellular systems; and IEEE 1901.

This text covers the latest standards supporting IoT/M2M from the perspective of Body Area Network/E-health/Assistive Technologies; it also covers over-the-air surveillance, object tracking, smart grid, smart cards, and home automation.

This is believed to be the first book on MIPv6 with applications to the IoT, especially in a mobile context. This work will be of interest to technology investors; planners with carriers and service providers; CTOs; logistics professionals; engineers at equipment developers; technology integrators; Internet and Internet Service Providers (ISP); and telcos, and wireless providers, both domestically and in the rest of the world.

ABOUT THE AUTHOR

Among other activities, Mr. Minoli has done extensive work in Internet engineering, design, and implementation over the years. The results presented in this book are based on the foundation work done while at *Telcordia, NYU, Stevens Institute of Technology, Rutgers University, AT&T*, and other engineering firms, starting in the early 1990s and continuing to the present. Some of his Internet- and wireless-related work that plays a role in the deployment of the Internet of Things has been documented in books he has authored, including:

- *Internet and Intranet Engineering* (McGraw-Hill, 1997)
- *Internet Architectures* (co-authored) (Wiley, 1999)
- *Hotspot Networks: Wi-Fi for Public Access Locations* (McGraw-Hill, 2002)
- *Wireless Sensor Networks* (co-authored) (Wiley 2007)
- *Handbook of IPv4 to IPv6 Transition Methodologies For Institutional & Corporate Networks* (co-authored) (Auerbach, 2008)
- *Satellite Systems Engineering in an IPv6 Environment* (Francis and Taylor 2009)
- *Mobile Video with Mobile IPv6* (Wiley 2012)

Mr. Minoli has many years of technical hands-on and managerial experience in planning, designing, deploying, and operating IP/IPv6, telecom, wireless, satellite, and video networks, and Data Center systems and subsystems for global Best-In-Class carriers and financial companies. He has worked on advanced network deployments at financial firms such as *AIG, Prudential Securities, Capital One Financial*, and service provider firms such as *Network Analysis Corporation, Bell Telephone Laboratories,*

ITT DTS/Worldcom, Bell Communications Research (now Telcordia), AT&T, Leading Edge Networks Inc., SES, and other institutions. In the recent past, Mr. Minoli has been responsible for (i) the development and deployment of IPTV systems, (ii) the development and deployment of terrestrial and mobile IP-based networking services; (iii) deployments of large aperture antenna at teleports in the United States and abroad; (iv) deployment of satellite monitoring services worldwide using IP/MPLS services; and (v) IPv6 services. He also played a founding role in the launching of two companies through the high tech incubator Leading Edge Networks Inc., which he ran in the early 2000s: *Global Wireless Services*, a provider of secure broadband hotspot mobile Internet and hotspot VoIP services; and, *InfoPort Communications Group*, an optical and Gigabit Ethernet metropolitan carrier supporting Data Center/SAN/channel extension and cloud network access services. For several years, he has been Session, Tutorial, and more recently overall Technical Program Chair for the IEEE ENTNET (Enterprise Networking) conference; ENTNET focuses on enterprise networking and security requirements for large financial firms and other corporate institutions.

Mr. Minoli has also written columns for *ComputerWorld, NetworkWorld*, and *Network Computing* (1985–2006). He has taught at *New York University* (Information Technology Institute), *Rutgers University*, and *Stevens Institute of Technology* (1984–2006). Also, he was a Technology Analyst At-Large, for Gartner/DataPro (1985–2001); based on extensive hand-on work at financial firms and carriers, he tracked technologies and wrote CTO/CIO-level technical scans in the area of telephony and data systems, including topics on security, disaster recovery, network management, LANs, WANs (ATM and MPLS), wireless (LAN and public hotspot), VoIP, network design/economics, carrier networks (such as metro Ethernet and CWDM/DWDM), and e-commerce. Over the years, he has advised Venture Capitals for investments of $150M in a dozen high tech companies.

Mr. Minoli has also acted as Expert Witness in a (won) $11B lawsuit regarding a VoIP-based wireless Air-to-Ground radio communication system for airplane in-cabin services, as well as for a large lawsuit related to digital scanning and transmission of bank documents/instruments (such as checks). He has also been engaged as a technical expert in a number of patent infringement proceedings in the digital imaging and VoIP space supporting law firms such as *Schiff Hardin LLP, Fulbright & Jaworski LLP, Dimock Stratton LLP/Smart & Biggar LLP,* and *Baker & McKenzie LLP*, among others.

CHAPTER 1

WHAT IS THE INTERNET OF THINGS?

1.1 OVERVIEW AND MOTIVATIONS

The proliferation of an ever-growing set of devices able to be directly connected to the Internet is leading to a new ubiquitous-computing paradigm. Indeed, the Internet—its deployment and its use—has experienced significant growth in the past four decades, evolving from a network of a few hundred hosts (in its ARPAnet form) to a platform capable of linking billions of entities globally. Initially, the Internet connected institutional hosts and accredited terminals via specially developed gateways (routers). More recently, the Internet has connected servers of all kinds to users of all kinds seeking access to information and applications of all kinds. Now, with social media, it intuitively and effectively connects all sorts of people to people, and to virtual communities. The growth of the Internet shows no signs of slowing down, and it is steadily becoming the infrastructure fabric of choice for a new paradigm for all-inclusive pervasive computing and communications. The next evolution is to connect all "things" and objects that have (or will soon have) embedded wireless (or wireline) connectivity to control systems that support data collection, data analysis, decision-making, and (remote) actuation. "Things" include, but are not limited to, machinery, home appliances, vehicles, individual persons, pets, cattle, animals, habitats, habitat occupants, as well as enterprises. Interactions are achieved utilizing a plethora of possibly different networks; computerized devices of various functions, form factors,

Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, First Edition. Daniel Minoli.

sizes, and capabilities such as iPads, smartphones, monitoring nodes, sensors, and tags; and a gamut of host application servers.

This new paradigm seeks to enhance the traditional Internet into a smart *Internet of Things* (IoT) created around intelligent interconnections of diverse objects in the physical world. In the IoT, commonly deployed devices and objects contain an embedded device or microprocessor that can be accessed by some communication mechanism, typically utilizing wireless links. The IoT aims at closing the gap between objects in the material world, the "things," and their logical representation in information systems. It is perceived by proponents as the "next-generation network (NGN) of the Internet." Thus, the IoT is a new type of Internet *application* that endeavors to make the thing's information (whatever that may be) available on a global scale using the Internet as the underlying connecting fabric (although other interconnection data networks, besides the Internet, can also be used such as private local area networks and/or wide area networks). The IoT has two attributes: (i) being an Internet application and (ii) dealing with the thing's information. The term *Internet of Things* was coined and first used by Kevin Ashton over a decade ago[1] (1). The "things" are also variously known as "objects," "devices," "end nodes," "remotes," or "remote sensors," to list just a few commonly used terms.

The IoT generally utilizes low cost information gathering and dissemination devices—such as sensors and tags—that facilitate fast-paced interactions in any place and at any time, among the objects themselves, as well as among objects and people. Actuators are also part of the IoT. Hence, the IoT can be described as a new-generation information network that enables seamless and continuous machine-to-machine (M2M)[2] and/or human-to-machine (H2M) communication. One of the initial goals of the IoT is to enable connectivity for the various "things"; a next goal is to be able to have the "thing" provide back appropriate, application-specific telemetry; an intermediary next step is to provide a web-based interface to the "thing" (especially when human access is needed); the final step is to permit actuation by the "thing" (i.e., to cause a function or functions to take place). Certain "things" are stationary, such as an appliance in a home; other "things" may be in motion, such as a car or a carton (or even an item within the carton) in a supply chain environment (either end-to-end, or while in an intermediary warehouse).

At the "low end" of the spectrum, the thing's information is typically coded by the unique identification (UID) and/or electronic product code (EPC); the information is (typically) stored in a radio frequency identification (RFID) electronic tag; and, the information is uploaded by noncontact reading using an RFID reader. In fact, UID and RFID have been mandated by the Department of Defense (DoD) for all their suppliers to modernize their global supply chain; RFID and EPC were also mandated

[1] Synonym key words are: "Ubiquitous computing (Ubi-comp), pervasive computing, ambient intelligence, sentient computing, and internet of objects." Multiple terminology terms should not confuse the reader, because, as a side note, often industry players redefine terms just to give the concept some cachet. For example, what some in the late 1960s called "time-sharing," others in the 1980s called it "utility computing." Then in the 1990s, people called it "grid computing." And now in the 2000s–2010s all the rage is "cloud." Same concepts, just new names.

[2] Some (e.g., 3GPP) also use the term machine-type communications (MTC) to describe M2M systems.

by Wal-Mart to all their suppliers as of January 1, 2006, and many other commercial establishments have followed suit since then. More generally, smart cards (SCs) will also play an important role in IoT; SCs typically incorporate a microprocessor and storage.

At the "mid range" of the spectrum, one finds devices with embedded intelligence (microprocessors) and embedded active wireless capabilities to perform a variety of data gathering and possibly control functions. On-body biomedical sensors, home appliance and power management, and industrial control are some examples of these applications.

At the other end of the spectrum, more sophisticated sensors can also be employed in the IoT: some of these sensor approaches use distributed wireless sensor network (WSN) systems that (i) can collect a wide variety of environmental data such as temperature, atmospheric and environmental chemical content, or even low- or high resolution ambient video images from geographically dispersed locations; (ii) can optionally pre-process some or all of the data; and (iii) can forward all these information to a centralized (or distributed/virtualized) site for advanced processing. These objects may span a city, region, or large distribution grid.

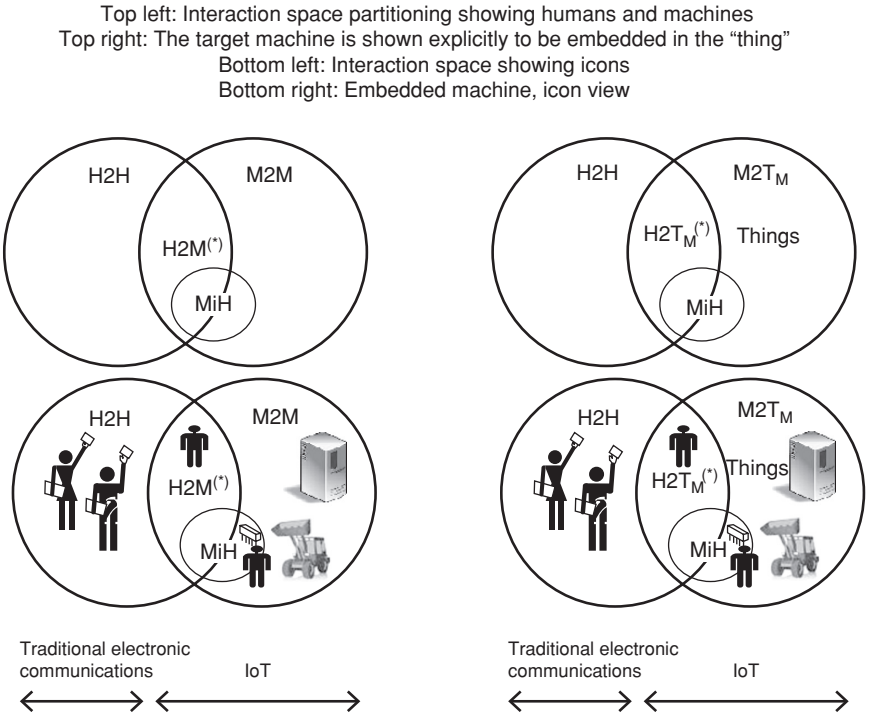
Other "things" may be associated with personal area networks (PANs), vehicular networks (VNs), or delay tolerant networks (DTNs).

The IoT is seen by many as a comprehensive extension of the Internet and/or Internet services that can establish and support pervasive connections between objects (things) (and their underlying intrinsic information) and data collection and management centers located in the network's "core" (possibly even in a distributed "cloud") (2,3). The IoT operates in conjunction with real-time processing and ubiquitous computing. The IoT is also perceived as a global network that connects physical objects with virtual objects through the combination of data capture techniques and communication networks. As such, the IoT is predicated on the expansion of the scope, network reach, and possibly even the architecture of the Internet through the inclusion of physical instrumented objects, such expansion fused with the ability to provide smarter services to the environment or to the end user, as more *in situ* transferable data become available. Some see the IoT in the context of ambient intelligence; namely, a vision where environment becomes smart, friendly, context aware, and responsive to many types of human needs. In such a world, computing and networking technology coexist with people in a ubiquitous, friendly, and pervasive way: numerous miniature and interconnected smart devices create a new intelligence and interact with each other seamlessly (4).

The IoT effectively eliminates time and space isolation between geographical space and virtual space, forming what proponents label as "smart geographical space" and creating new human-to-environment (and/or H2M) relationships. The latter implies that the IoT can advance the goal of integration of human beings with their surroundings. A smart environment can be defined as consisting of networks of federated sensors and actuators and can be designed to encompass homes, offices, buildings, and civil infrastructure; from this granular foundation, large-scale end-to-end services supporting smart cities, smart transportation, and smart grids (SGs), among others, can be contemplated. Recently, the IEEE Computer Society stated that

"... The Internet of Things (IoT) promises to be the most disruptive technology since the advent of the World Wide Web. Projections indicate that up to 100 billion uniquely identifiable objects will be connected to the Internet by 2020, but human understanding of the underlying technologies has not kept pace. This creates a fundamental challenge to researchers, with enormous technical, socioeconomic, political, and even spiritual, consequences. IoT is just one of the most significant emerging trends in technology ..." (5).

Figure 1.1 depicts the high level logical partitioning of the interaction space, showing where the IoT applies for the purpose of this text; the figure illustrates human-to-human (H2H) communication, M2M communication, H2M communications, and machine in (or on) humans (MiH) communications (MiH devices may include human embedded chips, medical monitoring probes, global positioning system (GPS) bracelets, and so on). The focus of the IoT is on M2M, H2M, and MiH applications; this range of applicability is the theme captured in this text.



H2H: Human to Human
H2M: Human to Machine = $H2T_M$: Human to Thing with Microprocessor/Machine
M2M: Machine to Machine = $M2T_M$: Machine to Thing with Microprocessor/Machine
MiH: Machine in Humans
(e.g., medical sensors)
(also includes chips in animals/pets)

(*) People have been communicating with computers for over half-a-century, but in this context "machine" means a microprocessor embedded in some objects (other than a traditional computer)

FIGURE 1.1 H2H, H2M, and M2M environment.

Recently, the IoT has been seen as an emerging "paradigm of building smart communities" through the networking of various devices enabled by M2M technologies (but not excluding H2M), for which standards are now emerging (e.g., from European Telecommunications Standards Institute [ETSI]). *M2M services* aim at automating decision and communication processes and support consistent, cost-effective interaction for ubiquitous applications (e.g., fleet management, smart metering, home automation, and e-health). *M2M communications* per se is the communication between two or more entities that do not necessarily need direct human intervention: it is the communication between remotely deployed devices with specific roles and requiring little or no human intervention. M2M communication modules are usually integrated directly into target devices, such as automated meter readers (AMRs), vending machines, alarm systems, surveillance cameras, and automotive equipment, to list a few. These devices span an array of domains including (among others) industrial, trucking/transportation, financial, retail point of sales (POS), energy/utilities, smart appliances, and healthcare. The emerging standards allow both wireless and wired systems to communicate with other devices of similar capabilities; M2M devices, however, are typically connected to an application server via a mobile data communication network.

IoT applications range widely from energy efficiency to logistics, from appliance control to "smart" electric grids. Indeed, there is increasing interest in connecting and controlling in real time all sorts of devices for personal healthcare (patient monitoring and fitness monitoring), building automation (also known as building automation and control (BA&C)—for example, security devices/cameras; heating, ventilation, and air-conditioning (HVAC); AMRs), residential/commercial control (e.g., security HVAC, lighting control, access control, lawn and garden irrigation), consumer electronics (e.g., TV, DVRs); PC and peripherals (e.g., mouse, keyboard, joystick, wearable computers), industrial control (e.g., asset management, process control, environmental, energy management), and supermarket/supply chain management (this being just a partial list). Figures 1.2–1.5 provide some pictorial views of actual IoT applications; these figures only depict illustrative cases and are not exhaustive or normative. As it can be inferred, however, in an IoT environment there are a multitude of applications and players that need to be managed across multiple platforms (6). Some see IoT in the context of the "Web 3.0" (a name/concept advanced by John Markoff of *The New York Times* in 2006), although this term has not yet gained industry-wide, consistent support (7). The proposed essence of the term implies "an intelligent Web," such as supporting natural language search, artificial intelligence/machine learning, and machine-facilitated understanding of information, with the goal of providing a more intuitive user experience. IoT might fit such paradigm, but does not depend on it.

The initial vision of the IoT in the mid-2000s was of a world where physical objects are tagged and uniquely identified by RFID transponders; however, the concept has recently grown in multiple dimensions, encompassing dispersed sensors that are able to provide real-world intelligence and goal-oriented collaboration of distributed smart objects via local interconnections (such as through wireless LANs, WSNs, and so on), or global interconnections (such as through the Internet). The

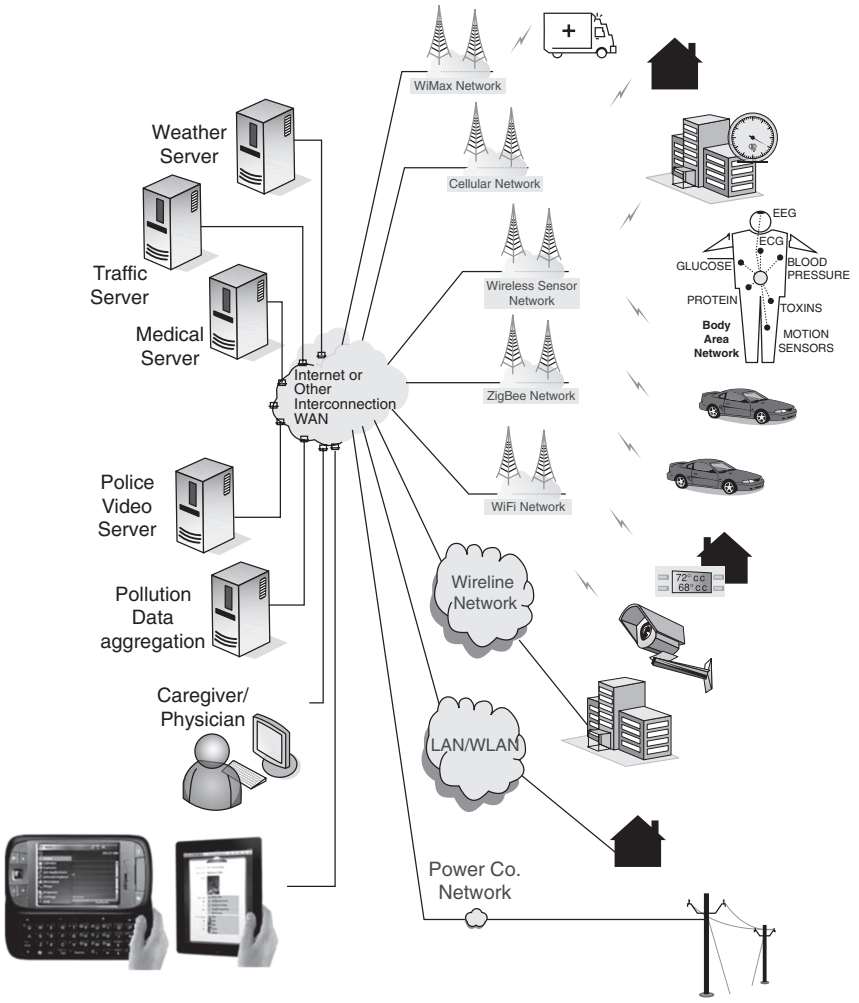


FIGURE 1.2 Illustrative example of the IoT.

seamless integration of communication capabilities between RFID tags, sensors, and actuators is seen as an important area of development. WSNs are likely the "outer tier" communication apparatus of the IoT. Thus, the IoT is not just an extension of today's Internet: it represents an aggregate of intelligent end-to-end systems that enable smart solutions, and, as such, it covers a diverse range of technologies, including sensing, communications, networking, computing, information processing, and intelligent control technologies, some of which are covered in this text.

As stated above, we take the IoT to encompass the M2M, H2M, and MiH space. It has been estimated that in 2011, there were 7 billion people on earth and 60 billion machines worldwide. Market research firm Frost & Sullivan recently forecasted that

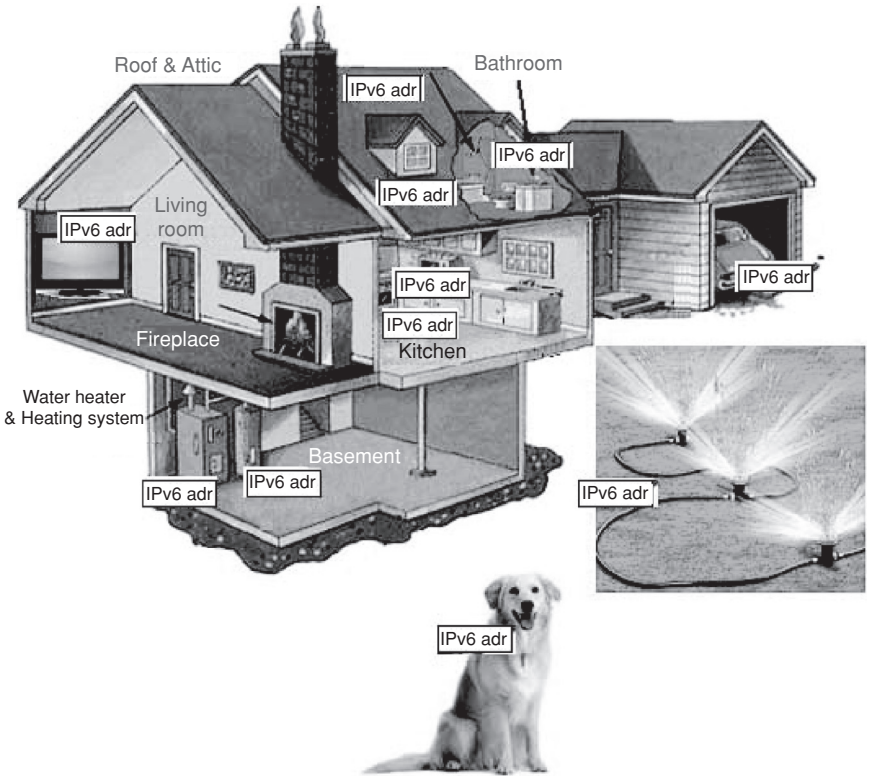


FIGURE 1.3 Another illustrative example of the IoT.

mobile computing devices, such as connected laptops, netbooks, tablets, and MiFi nodes, will increase to 50 million units by 2017 in the United States, while total cellular M2M connections are expected to increase from around 24 million in 2010 to more than 75 million over the same period; worldwide, the expectation is that the number of M2M device connections will grow from around 60 million in 2010 to over 2 billion in 2020 (8). Other market research puts the worldwide M2M revenues at over $38 billion in 2012 (9). Yet other market research companies project 15 billion connected devices moving 35 trillion gigabytes of data at a cost of $3 trillion annually by 2015 (10). These market data point to major development and deployment of the IoT technology in the next few years. Note that personal communication devices (smartphones, pads, and so on) can be viewed as machines or just simply as end nodes; when personal communication devices are used for H2M devices where the human employs the smartphone to communicate with a machine (such as a thermostat or a home appliance), then we consider the personal communication devices part of the IoT (otherwise we do not).

The definition of "IoT" has still some variability and can encompass different aspects depending on the researcher and/or the field in question. The European

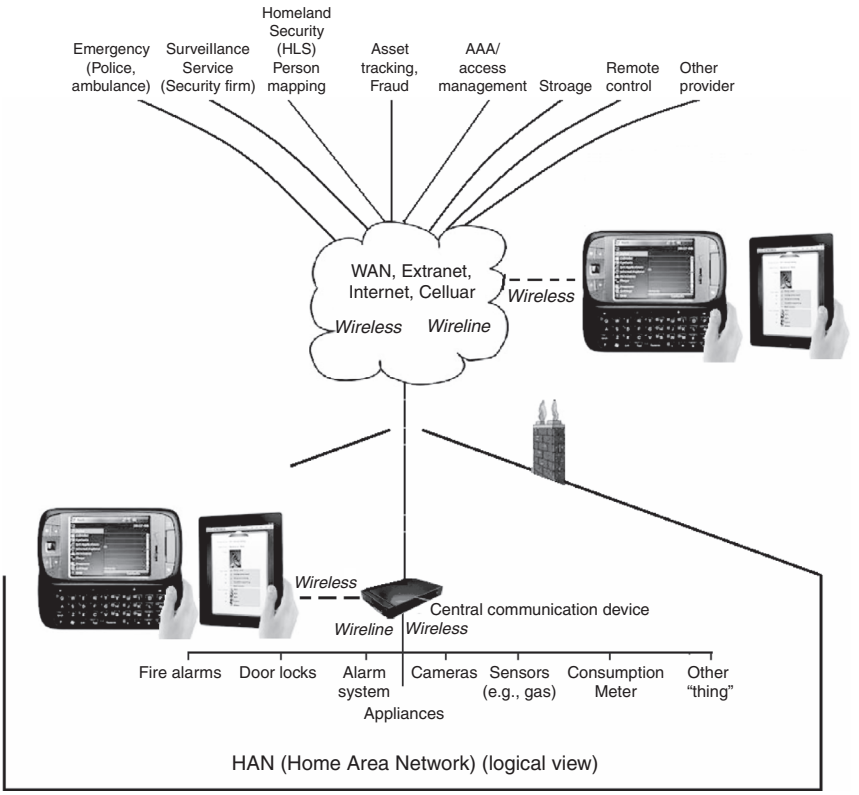


FIGURE 1.4 Yet another illustrative example of the IoT showing service providers.

Commission recently made these observations, which we can employ in our discussion of the IoT (11):

> "... Considering the functionality and identity as central it is reasonable to define the IoT as *"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts."* A different definition, that puts the focus on the seamless integration, could be formulated as "Interconnected objects having an active role in what might be called the Future Internet." The semantic origin of the expression is composed by two words and concepts: "Internet" and "Thing," where "Internet" can be defined as *"The world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP),"* while "Thing" is *"an object not precisely identifiable."* Therefore, semantically, "Internet of Things" means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols ..."

Some see IoT as an environment where "things talk" and/or "things talk back" (7); effectively this simply means that devices have communication capabilities. The set of

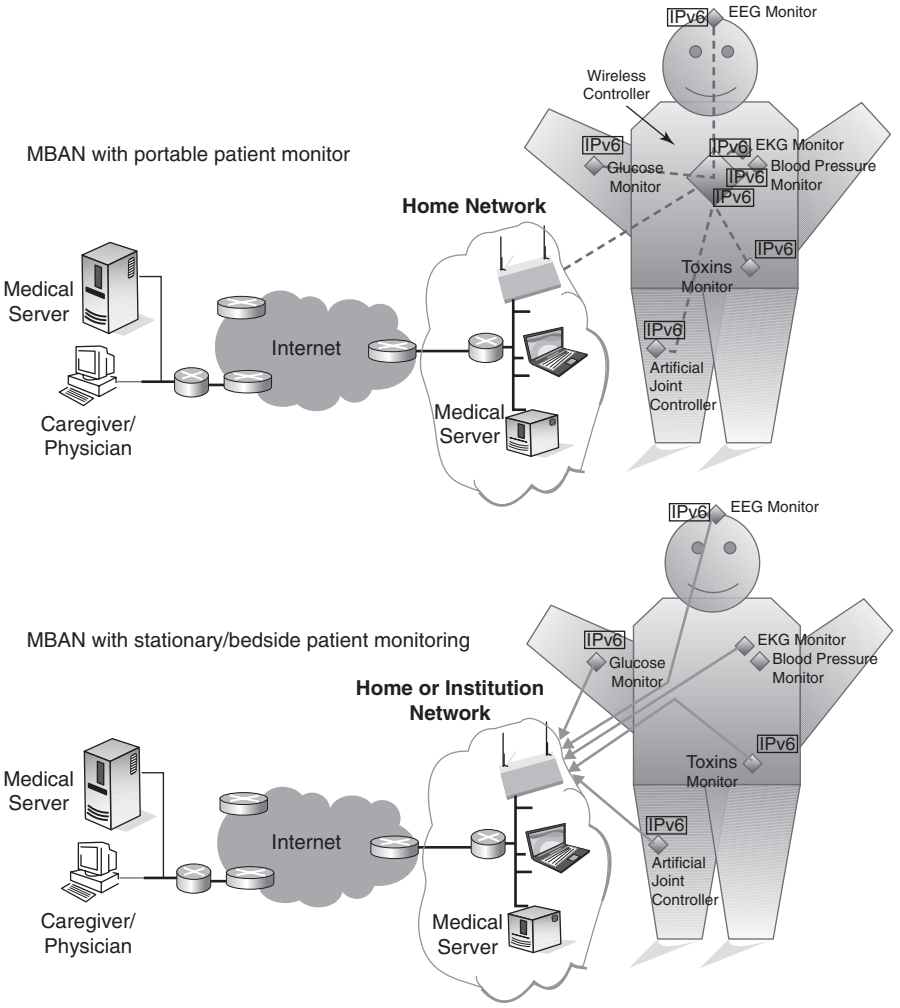


FIGURE 1.5 Yet another illustrative example of the IoT (body area network (BAN) application).

data and environmental awareness that objects should have depends on the application in question. Researchers are suggesting that objects should have the capability to be aware of such data as, but not limited to, its creation, transformation, ownership change, and physical-world parameters. Also, in some applications, objects should be able to interact actively with the environment, operating as actuators.

At a macro level, an IoT comprises a remote set of assets (a sensing domain), a network domain, and an applications domain. We define the data processing thing, also known as data integration point or person (DIPP), as the point (entity, person) where the administrative decisioning and/or the data accumulation takes place. We

define the "remote things," also known as data end points (DEPs), as the devices where events are sensed, data are collected, and/or an actuation takes place. Table 1.1 provides a working taxonomy of "things" in the IoT universe, as perceived in this text. There are interactions of interest between a DIPP being a human (H) and a "remote thing" being a machine/device (e.g., a thermostat) (such as a person changing the setting of the thermostat while away from home) or between two machines (M) (such as a server handling the usage reading from a residential electric meter). A person/human may use a PC or laptop, but increasingly a person may be using an iPad/tablet or a smartphone. The DIPP could be accessing the IoT system from a stationary location (e.g., a PC or server), from a wireless local environment (e.g., a fixed home hotspot), or from a completely mobile venue (e.g., using a smartphone). The "remote thing" could be stationary (e.g., a thermostat), on a wireless LAN or sensor network (but be relatively stationary), or be completely mobile (e.g., on a mobile ad hoc Network (MANET)—a self-configuring infrastructureless network of mobile devices connected by wireless links—or on a 3G/4G cellular network).

IoT is not seen by advocates as a future thing, but a set of capabilities that are already available at this time. Proponents and developers are endeavoring to reuse what is already available by way of the Internet suite of protocols, although there may be a need for some more research and/or standards, especially for large-scale, low power, broadly dispersed (where sensors are broadly dispersed in the environment) applications. An overriding goal is not to redesign the Internet (12); many researches position the IoT and work in support of the IoT simply as the (normal) "Evolution of the Internet" (what might be called by analogy with cellular networks, the long-term evolution of the Internet (LTEI)). A key observation is that if each of the large multitude of things in the IoT is to be addressed directly and individually, then a large address space is needed.

Cost as well as energy requirements of embedded devices require the use of efficient protocols and efficient communication architectures for the IoT. Standardization of IoT elements also becomes critical: the benefits of standardization include reduced complexity of IoT deployments, reduced deployment time for new services, lower capital requirements (CAPEX), and lower operating expense (OPEX). The IoT requires robust "last-yard," "last-mile," and "core" network technologies to make it a commercial reality.

Various technologies have indeed emerged in the past two decades that can be utilized for implementations, including PANs, such as IEEE 802.15.4; wireless local area networks (WLANs); WSNs; 3G/4G cellular networks; metro-Ethernet networks; multiprotocol label switching (MPLS); and virtual private network (VPN) systems. Wireless access and/or wireless ad hoc mesh systems reduce the "last-mile" cost of IoT applications, such as for distributed monitoring and control applications. However, we believe that the fundamental technical advancement that will foster the deployment of the IoT is IP Version 6 (IPv6). *In fact, IoT may well become the "killer-app" for IPv6.* IoT is deployable using IP Version 4 (IPv4) as has been the case in the recent past, but only IPv6 provides the proper scalability and functionality to make it economical, ubiquitous, and pervasive. There are many advantages in using IP for IoT, but we have to ascertain that the infrastructure and the supporting