CHAPTER 2

INTERNET OF THINGS DEFINITIONS AND FRAMEWORKS

This chapter elaborates on the concept, definition, and a usable framework of the Internet of Things (IoT).

2.1 IoT DEFINITIONS

We noted in Chapter 1 that the IoT is an evolving type of Internet *application* that endeavors to make a thing's information (whatever that may be) securely available on a global scale if/when such information is needed by an aggregation point or points. Since the definition of the IoT is still evolving, the material that follows provides illustrative concept definitions rather than a tightly worded definition; nonetheless, a provisional "working definition" is in fact provided in order to baseline our discussion.

2.1.1 General Observations

Some applicable observations related to the definition of the IoT include the following:

> "Internet of Things is a twenty-first century phenomenon in which physical consumer products (meta products) connect to the web and start communicating with each other by means of sensors and actuators . . ." (1).

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

"Today's Internet is experienced by users as a set of applications, such as email, instant messaging, and social networks. While these applications do not require users to be present at the time of service execution, in many cases they are. There are also substantial differences in performance between the various end devices, but in general end devices participating in the Internet are considered to have high performance. As we move forward with the interconnection of all kinds of devices via the Internet, these characteristics will change. The term "Internet of Things" denotes a trend where a large number of devices benefit from communication services that use Internet protocols. Many of these devices are not directly operated by humans, but exist as components in buildings, vehicles, and the environment. There will be a lot of variation in the computing power, available memory, and communications bandwidth between different types of devices. Many of these devices provide new services or provide more value for previously unconnected devices. Some devices have been connected in various legacy ways in the past but are now migrating to the use of the Internet Protocol, sharing the same communications medium between all applications and enabling rich communications services . . . " (2).

"The M2M . . . term is used to refer to machine-to-machine communication, i.e., automated data exchange between machines. ("Machine" may also refer to virtual machines such as software applications.) Viewed from the perspective of its functions and potential uses, M2M is causing an entire "Internet of Things", or internet of intelligent objects, to emerge . . . On closer inspection, however, M2M has merely become a new buzzword for demanding applications involving telemetry (automatic remote transmission of any measured data) and SCADA (Supervisory, Control and Data Acquisition). In contrast to telemetry and SCADA-based projects, the majority of M2M applications are broadly based on established standards, particularly where communication protocols and transmission methods currently in use are concerned. Telemetry applications involve completely proprietary solutions that, in some cases, have even been developed with a specific customer or application in mind. M2M concepts, meanwhile, use open protocols such as TCP/IP, which are also found on Internet and local company networks. The data formats in each case are similar in appearance . . . " (3).

"IoT spans a great range of applications. People bring varied assumptions about what devices are 'things'. Most IoT devices have constraints but the nature of constraints varies. IoT needs to be divided into manageable topic areas . . . " (4).

"Information Communications Technology (ITC) evolution has led to wireless personal devices such as smart phones, personal computers and PDAs. These devices have in common that they are designed to operate over IP networks. Hence, the number of devices that are connected to the Internet is growing exponentially. This has led to define a new concept of Internet, the commonly called Future Internet and Internet of Things (IoT). The objective of IoT is the integration and unification of all communication systems located surrounds us. Thereby, the systems can get control and total access of the other systems for leading to provide ubiquitous communication and computing with the purpose of defining a new generation of services . . . " (5).

"The vision of the internet of things is to attach tiny devices to every single object to make it identifiable by its own unique IP address. These devices can then autonomously communicate with one another. The success of the internet of things relies on overcoming

the following technical challenges: (1) The current manner of using IP addresses must change to a system that provides an IP address to every possible object that may need one in the future. (2) The power behind the embedded chips on such devices will need to be smaller and more efficient. And, (3) The software applications must be developed that can communicate with and manage the stream of data from hundreds of interconnected non-computing devices that comprise a 'smart' system which can adapt and respond to changes . . . " (6).

" . . . Order(s) of magnitude bigger than the Internet, no computers or humans at end-point, inherently mobile, disconnected, unattended . . . IoT is going to be an advanced network including normal physical objects together with computers and other advanced electronic appliances. Instead of forming ad hoc network, normal objects will be a part of whole network so that they can collaborate, understand real time environmental data and react accordingly in need . . . The basic idea is that IoT will connect objects around us (electronic, electrical, non electrical) to provide seamless communication and contextual services provided by them. Development of RFID (radio-frequency identification) tags, sensors, actuators, mobile phones make it possible to materialize IoT which interact and co-operate each other to make the service better and accessible anytime, from anywhere . . . The 'Internet of Things (IoT)' refers to the networked interconnection of everyday objects. An 'IoT' means 'a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols' . . . In the IoT, 'things' are very various such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc. These things are classified as three scopes: people, machine (for example, sensor, actuator, etc) and information (for example clothes, food, medicine, books and so on). These 'things' should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities . . . if the 'thing' is identified, we call it the 'object' . . . " (7, 8).

" . . . Commonly we focus on the deployment of a new generation of networked objects with communication, sensory and action capabilities for numerous applications with a vision 'from simple connected objects as sensor networks to more complex and smarter communicated objects as in the envisioned IoT' . . . In the IETF/IRTF perspective, one of our visions is to provide global interoperability via IP for making heterogeneous/constraint objects very smart . . . " (8, 9).

" . . . M2M describes devices that are connected to the Internet, using a variety of fixed and wireless networks and communicate with each other and the wider world. They are active communication devices. The term embedded wireless has been coined, for a variety of applications where wireless cellular communication is used to connect any device that is not a phone. This term is widely used by the GSM Association (GSMA) . . . " (10).

Originally the term "Internet of Things" was invented by the MIT Auto-ID Center in 2001 and referred to an architecture that comprises four elements, as follows (11):

- Passive radio frequency identification (RFIDs), such as Class-1 Generation-2 UHF RFIDs, introduced by the electronic product code (EPC) Global Consortium and operating in the 860–960 MHz range[1]
- Readers plugged to a local (computing) system, which read the EPC
- A local system offering IP connectivity that collects information pointed by the EPC, thanks to a protocol called object naming service (ONS)
- EPCIS (EPC Information Services) servers that process incoming ONS requests and returns physical markup language (PML) files, for example, XML documents carrying meaningful information linked to RFIDs

However, as noted in the discussion so far, the term is now much more encompassing. A short, incomplete bibliography of articles describing the IoT includes the references at the end of this chapter in general and the following in particular: (7–9, 12–19).

2.1.2 ITU-T Views

The ITU-T is in the process of identifying a common way to define/describe the IoT. So far, the ITU-T has not found "*a good definition to cover all aspects of IoT as the IoT has quite big scope not only the technological viewpoints but also other views . . . We recognized whatever we define, everyone cannot be happy*" (20).

One can view the Internet as an *infrastructure* providing a number of technological capabilities or as a *concept* to provide an array of data exchange and linkage services. The infrastructure perspective describes the Internet as a global system of interconnected computer networks (of many conceivable technologies) that use the TCP/IP Internet Protocol Suite to communicate; the networks comprise millions of private, public, business, academic, and governmental servers, computers, and nodes. The concept perspective sees the Internet as a worldwide logical interconnection of computers and networks that support the exchange of information among users, including but not limited to interlinked hypertext documents of the World Wide Web (WWW). Similarly, at the current time different experts can define the IoT differently, the conceptual way or the infrastructural way as follows (20):

View A: IoT is just a concept (conceptual aspects of definition): the IoT does not refer to a network infrastructure; the IoT is not a technical term but a concept (or a phenomenon).

View B: IoT is an infrastructure: The IoT refers to an infrastructure.

As shown in Figure 2.1, if defined as an infrastructure, IoT should be identified for all aspects of infrastructure such as service and functional requirements, architectures,

[1](also known as the "Gen 2" standard) this standard defines the physical and logical requirements for a passive-backscatter, interrogator-talks-first (ITF), RFID system operating in the 860–960 MHz frequency range; the system comprises interrogators (also known as readers), and tags (also known as labels).

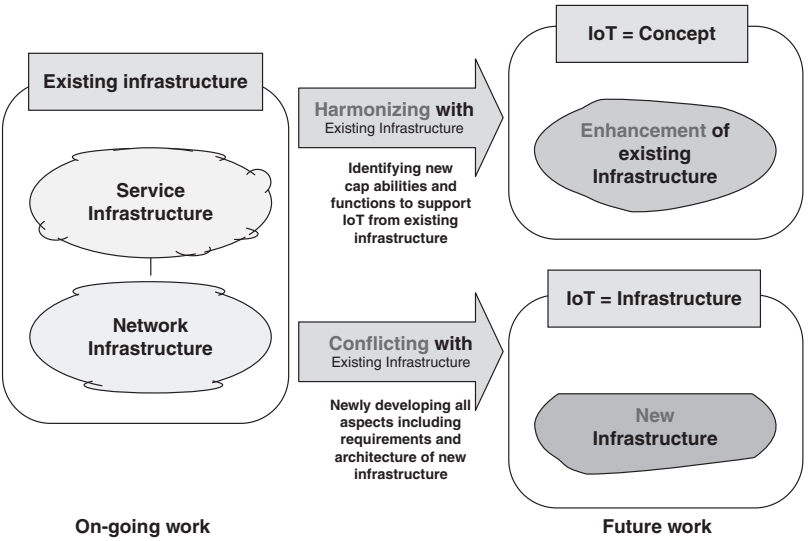

FIGURE 2.1 Direction for standardization according to IoT definition.

and so on. If defined as a concept, all relevant capabilities and specific functions to support (or realize) that concept of IoT will need to be identified for each technical area.

When ITU-T SG13 had developed Y.2002 ("*Overview of ubiquitous networking and of its support in NGN*"), the study group (SG) noted that ubiquitous networking is not a new network; the IoT is a conceptual design goal, which one has to consider for developing standards. Based on this conceptual goal (a simple definition), each SG can define detailed concepts with its own view. From SG13's perspective, next-generation network (NGN), smart ubiquitous network (SUN), and the future network (FN) should support key characteristics for realizing IoT. The main role of SG13 is to focus on the enhancement of networking technologies based on the NGN, the SUN, and the FN, rather than creating a new network.

The ITU-T is suggesting to define the IoT as a short definition with more general concept rather than as a technical definition; this should be done, in their view, in order for the IoT to be easily incorporated into various areas from technology, as well as accepted to all other interested SGs. After that, one can concentrate on defining the scope for IoT (e.g., service, network, control, security, quality, billing/charging aspects, and others) and finding related technological issues for further standardization work. ITU-T "*strongly insists on a short definition as concept instead of a technical definition (long or detailed description of technology)*" (20). Tables 2.1 and 2.2 from TD27 (IoT-GSI) show a representative set of working definitions.

Some see machine-to-machine (M2M) deployments into four domains: sensors and controllers; "the edge," where data from these devices are gathered; the cloud, where the data are stored and managed; and the client, where that data are ultimately evaluated (21).

TABLE 2.1 Examples of Definitions for Case A (IoT is Just a Concept)

Candidate Definition	Reference
A technological revolution that represents the future of computing and communications, and its development depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology	Source: ITU Internet Reports 2005: The Internet of Things, Executive Summary
The networked interconnection of objects—from the sophisticated to the mundane—through identifiers such as sensors, RFID tags, and IP addresses	Margery Conner, Technical Editor of EDN Magazine, "Sensors empower the 'Internet of Things' ", May 2010
The Internet of things *links the objects of the real world with the virtual world*, thus enabling anytime, anyplace connectivity for anything and not only for anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time	Cluster of European Research Projects on the Internet of Things, "Vision and Challenges for Realizing the Internet of Things", March 2010
The IoT refers to as *ubiquitous networking or pervasive computing environments*, is *a vision* where all manufactured things can be network enabled, that is connected to each other via wireless or wired communication networks	European Network and Information Security Agency (ENISA)
The IoT is *a world where physical objects are seamlessly integrated into the information network*, and where the physical objects can become active participants in business processes. Services are available to interact with these "smart objects" over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues. RFID, sensor networks, and so on are just enabling technologies	SAS
IoT is a [*high-level service concept* based on] existing and evolving global ICT (Information and Communication Technology) infrastructures that provide information services by interconnecting things	

2.1.3 Working Definition

Generalizing from the published literature and the observations made thus far in this text, we characterize the IoT with a "working definition" as follows:

Definition: *A broadly-deployed aggregate computing/communication application and/or application-consumption system, that is deployed over a local (L-IoT),*

TABLE 2.2 Examples of Definitions for Case B (Infrastructural Aspects of Definition)

Candidate Definition	Reference
A *global network infrastructure*, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object identification, sensor and connection capability as the basis for the development of independent federated services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity, and interoperability	Coordination and Support Action (CSA) for Global RFID-related Activities and Standardization (CASAGRAS)
A global information and communication infrastructure enabling automated chains of actions (not requiring explicit human intervention) facilitating information assembly and knowledge production and contributing to enrichment of human life by interconnecting physical and logical objects based on standard and interoperable communication protocols and through the exploitation of data capture and communication capabilities supported by existing and evolving information and communication technologies NOTE: Physical objects may include sensors, devices, machines, and so on. Logical objects may include contents and so on	Originally produced by the discussion among China-Japan-Korea. ITU Q3/13 has made some modifications
A global ICT infrastructure linking physical objects and virtual objects (as the informational counterparts of physical objects) through the exploitation of sensor and actuator data capture, processing and transmission capabilities. As such, the IoT is an overlay above the "generic" Internet, offering federated physical-object-related services (including, if relevant, identification, monitoring, and control of these objects) to all kinds of applications.	Proposed by France Telecom on the IoT definition mailing list.
IoT is (*a global ICT infrastructure*) which provides information services by interconnecting things NOTE: Infrastructure should not be interpreted only as a network	
A more prescriptive definition follows:	
The Internet of Things consists *of networks of sensors attached to objects and communication devices*, providing data that can be analyzed and used to initiate automated actions. The data also generate vital intelligence for planning, management, policy, and decision-making	Proposed by Cisco

metropolitan (M-IoT), regional (R-IoT), national (N-IoT), or global (G-IoT) geography, consisting of (i) dispersed instrumented objects ("things") with embedded one- or two-way communications and some (or, at times, no) computing capabilities, (ii) where objects are reachable over a variety of wireless or wired local area and/or wide area networks, and, (iii) whose inbound data and/or outbound commands are pipelined to or issued by a(n application) system with a (high) degree of (human or computer-based) intelligence.

In this definition, things are generally objects, tags, sensors, or actuators in the environment, but not typically business/personal PCs, laptops, smartphones, or tablets. We posit that this definition looks at the IoT as both a concept and an infrastructure, from a hybrid perspective. Unless there is a specific need to clarify the nature of the geographic scope, we use the generic term IoT to cover all instances of the technology.

Note that a variety of definitions could be formulated; the above formulation is not offered to be exclusive of other definitions offered by other researchers, but simply to be a useful reference baseline for the present discussion.

Two other related "working definitions" are as follows:

Definition: *Sensors are active devices that measure some variable of the natural or man-made environment (e.g., a building, an assembly line, an industrial assemblage supporting a process).*

The technology for sensing and control includes electric and magnetic field sensors; radiowave frequency sensors; optical-, electro-optic-, and infrared sensors; radars; lasers; location/navigation sensors; seismic and pressure-wave sensors; environmental parameter sensors (e.g., wind, humidity, heat, and so on); and, biochemical Homeland Security-oriented sensors.

Sensor networks usually consider remote devices as belonging to two classes, based on device capabilities: Full-function devices (FFDs) and reduced function devices (RFDs). Sensors and actuators are part of a larger universe of objects. Objects in the IoT context can also be classified from a functionality perspective.

Definition: *An actuator is a mechanized device of various sizes (from ultra-small to very large) that accomplishes a specified physical action, for example, controlling a mechanism or system, opening or closing a valve, starting some kind or rotary or linear motion, or initiating physical locomotion. An actuator is the mechanism by which an entity acts upon an environment.*

The actuator embodies a source of energy, such as an electric current (battery, solar, motion), and a source of physical interaction such as a hydraulic fluid pressure or a pneumatic pressure; the device converts that energy into some kind of action or motion upon receipt of an external command or stimulus.

An object is a model of an entity. An object is distinct from any other object and is characterized by its behavior. An object is informally said to perform functions and offer services (an object that performs a function available to other entities and/or objects is said to offer a service). For modeling purposes, these functions

and services are specified in terms of the behavior of the object and of its interfaces (18, 22). An object can, as needed, perform more than one function and a function can be performed by the cooperation of several objects. Objects are also called "smart/connected objects" by some. In the definition of the ITU (18), objects include terminal devices (e.g., used by a person to access the network such as mobile phones, personal computers, and so on), remote monitoring devices (e.g., cameras, sensors, and so on), information devices (e.g., content delivery server), products, contents, and resources. We stated in Chapter 1, however, that for the purpose of our discussion, 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 (e.g., a thermostat or a home appliance), then we consider the personal communication devices as part of the IoT; otherwise, we do not. Smart/connected objects are heterogeneous with different sizes, mobility capabilities, power sources, connectivity mechanisms, and protocols. A physical object interacts with several entities, performs various functionalities, and generates data that might be used by other entities. Usually, the resources of these objects are limited. Furthermore, there are various types of networking interfaces that have different coverage and data rates. These environments have the characteristics of low power and lossy networks such as Bluetooth, IEEE 802.15.4 (6LoWPAN, ZigBee), near field communication (NFC), and so on (8). Things (objects) can be classified as shown in Figure 2.2. Objects have the following characteristics, among others, (8):

- have the ability to sense and/or actuate
- are generally small (but not always)
- have limited computing capabilities (but not always)
- are energy/power limited
- are connected to the physical world
- sometimes have intermittent connectivity
- are mobile (but not always)
- of interest to people
- managed by devices, not people (but not always)

While the IoT can in principle be seen as a more encompassing concept than what is captured under the ETSI M2M standards and definitions, nonetheless the M2M definitions can serve the purpose adding some structure to the discussion. We noted in Figure 1.1 a high level logical partitioning of the entity-to-entity interaction space that included human to human (H2H) communication, M2M communication, human to machine (H2M) communications, and machine in (or on) human (MiH) communications. (MiH devices may include medical monitoring probes, global positioning system (GPS) bracelets, and so on.) For the present discussion, the focus of the IoT is on M2M, H2M, and MiH applications; this range of applicability is the theme captured in this text, also as depicted in Figure 2.3. Figure 2.4 illustrates classes of generic IoT arrangements that are included in our discussion.

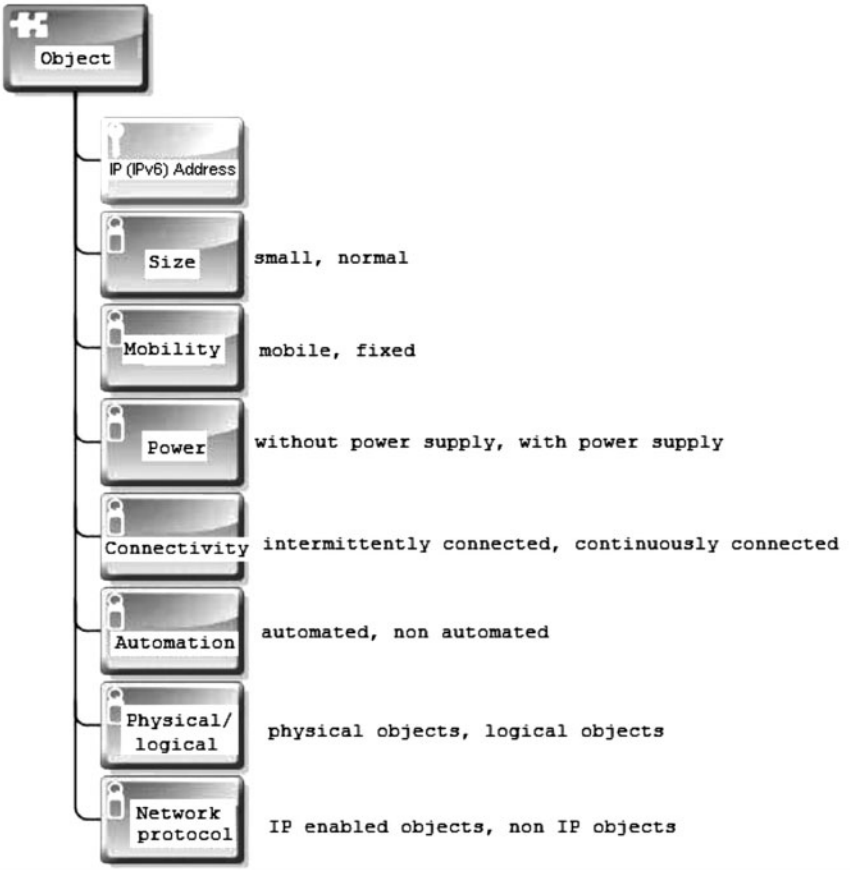

FIGURE 2.2 Object classification.

Intuitively, an M2M/H2M environment comprises three basic elements: (i) the data integration point (DIP)[2]; (ii) the communication network; and; (iii) the data end point (DEP) (again, a machine M). See Figure 2.5, where the process (X) and application (Y) form the actual functional end points. Typically, a DEP refers to a microcomputer system, one end of which is connected to a process or to a higher level subsystem via special interfaces; the other end is connected to a communication network. However, the DEP can also be a machine M in a human H, as is the case in the MiH environment. Many applications have a large base of dispersed DEPs (3). A DIP can be an Internet server, a software application running on a firm-resident host, or an application implemented as a cloud service. As previously mentioned,

[2]In Chapter 1, we also called the DIP a "data integration point or person (DIPP)" because the DIP corresponds with a point (P, that is a machine M) or with a person (P).

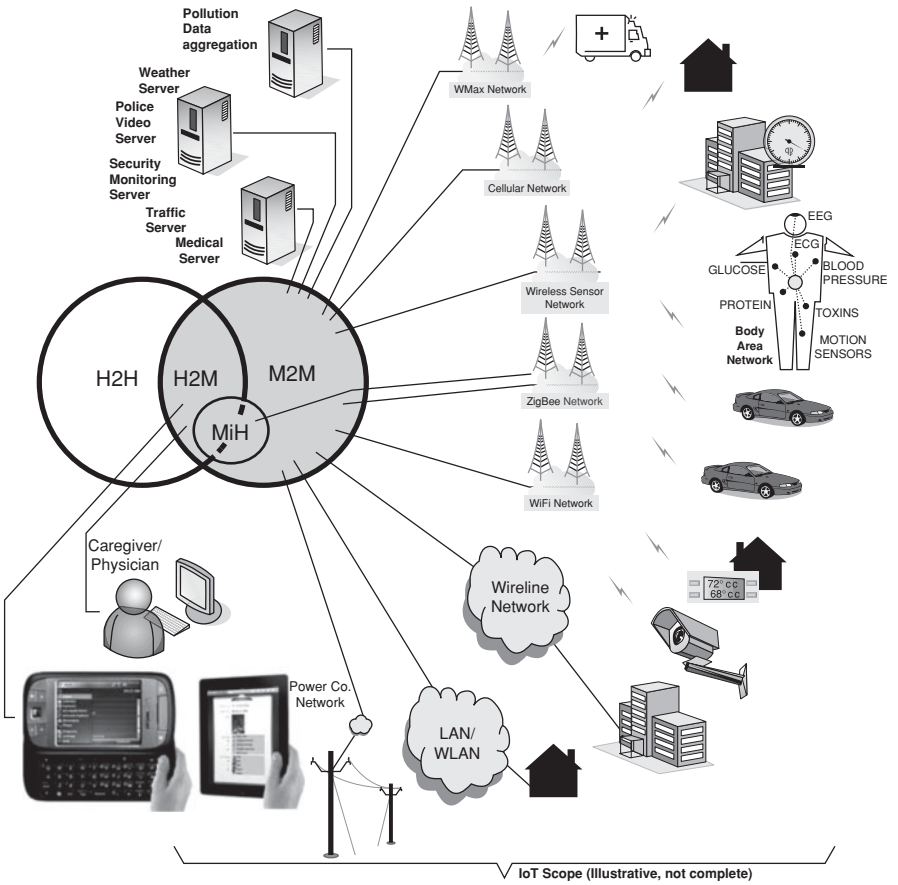

FIGURE 2.3 Scope of IoT by way of illustration.

basic applications include, but are not limited to, smart meters, e-health, track-and-trace, monitoring, transaction, control, home automation, city automation, connected consumers, and automotive.

As noted in Chapter 1, at a macro level, an IoT comprises a remote set of sensing assets (sensing domain, also known as M2M domain in an M2M environment), a network domain, and an applications domain. Figures 2.6 and 2.7 provide illustrative pictorial view of the domains.

2.2 IoT FRAMEWORKS

A high level M2M system architecture (HLSA) (see Figure 2.8) is defined in the ETSI TS 102 690 V1.1.1 (2011–10) specification that is useful to the present discussion. We describe the HLSA next, summarized from Reference 23. The HLSA comprises the device and gateway domain, the network domain, and the applications domain.

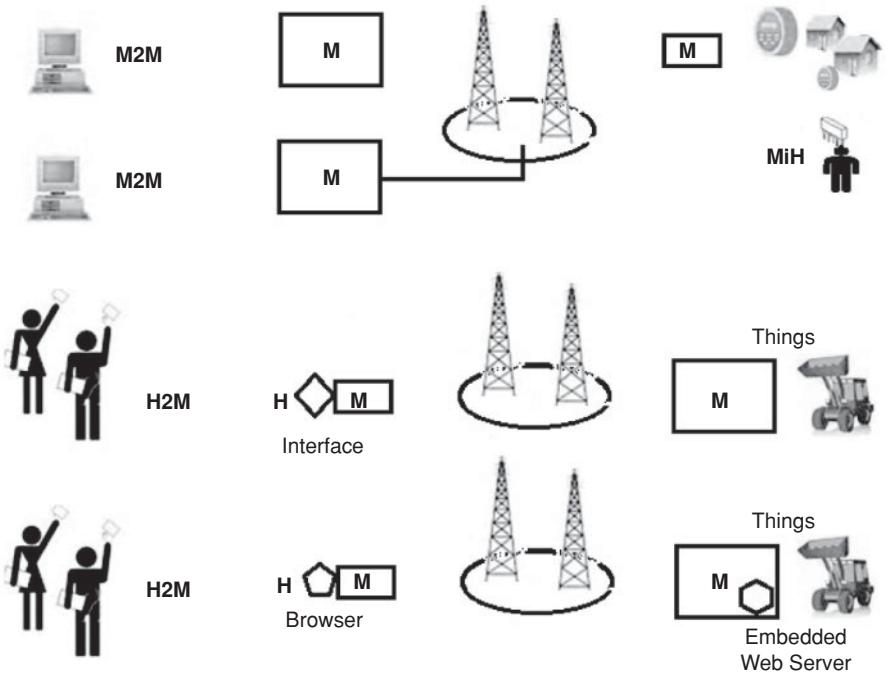

FIGURE 2.4 Classes of generic IoT arrangements.

The **device and gateway domain** is composed of the following elements:

1. **M2M device:** A device that runs M2M application(s) using M2M service capabilities. M2M devices connect to network domain in the following manners:
   – **Case 1 "Direct Connectivity":** M2M devices connect to the network domain via the access network. The M2M device performs the procedures such as

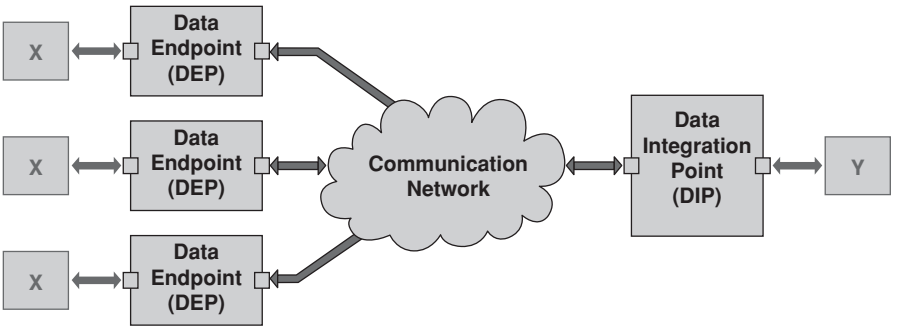

FIGURE 2.5 Basic elements of an M2M application.

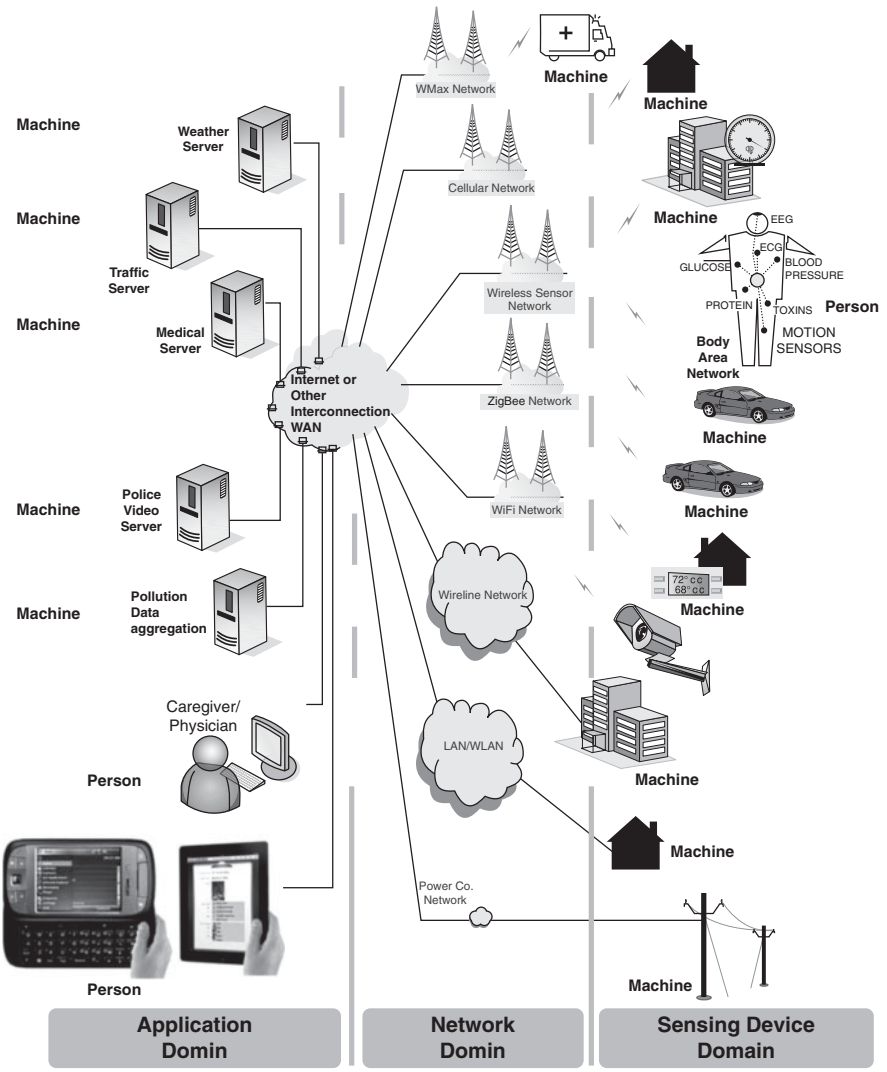

FIGURE 2.6 M2M domains.

registration, authentication, authorization, management, and provisioning with the network domain. The M2M device may provide service to other devices (e.g., legacy devices) connected to it that are hidden from the network domain.

– **Case 2 "Gateway as a Network Proxy":** The M2M device connects to the network domain via an M2M gateway. M2M devices connect to the M2M gateway using the M2M area network. The M2M gateway acts as a proxy for the network domain toward the M2M devices that are connected to it.

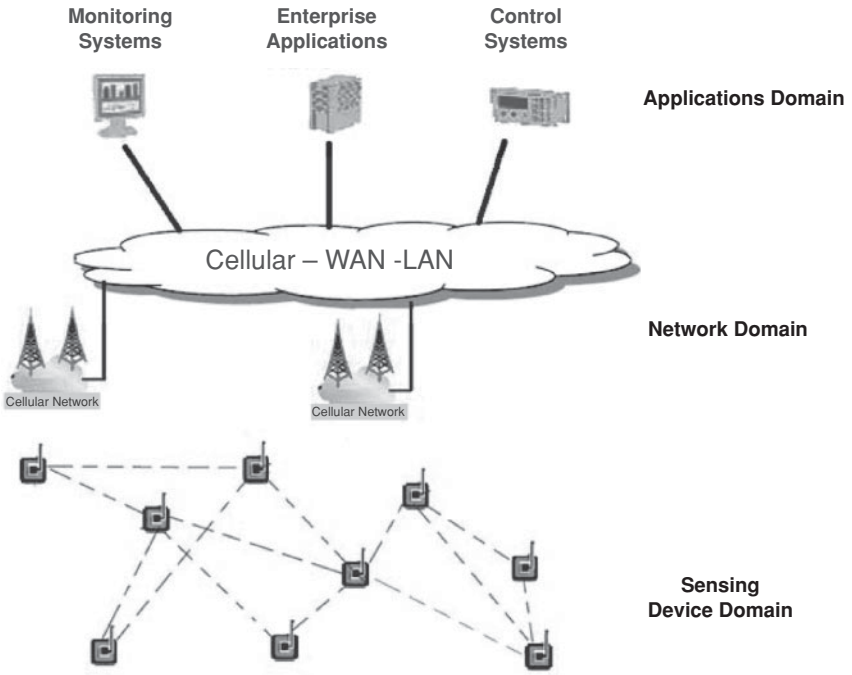

FIGURE 2.7 Other example of M2M domains.

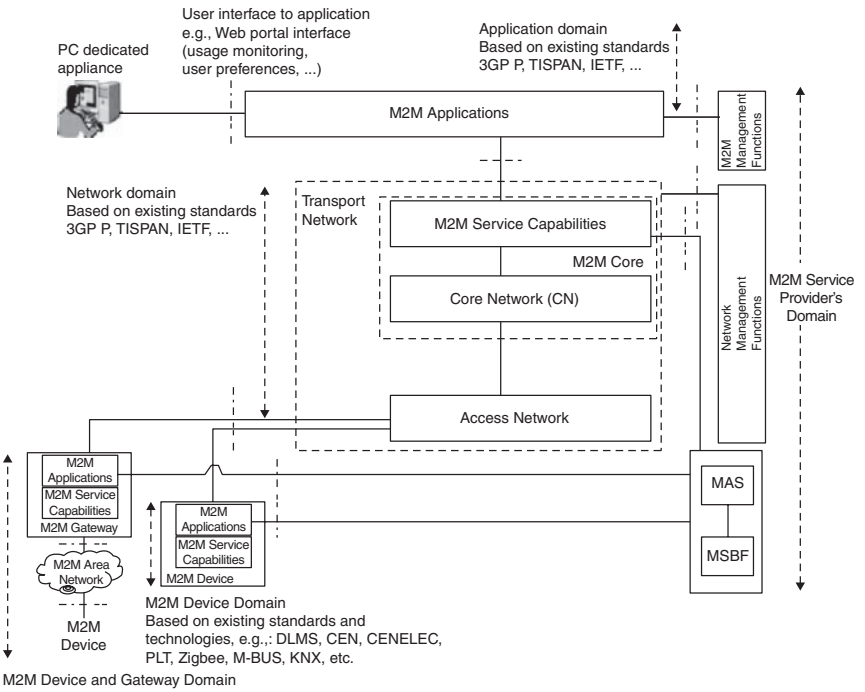

FIGURE 2.8 M2M HLSA.

Examples of procedures that are proxied include authentication, authorization, management, and provisioning.
(M2M devices may be connected to the network domain via multiple M2M gateways.)

2. **M2M area network:** It provides connectivity between M2M devices and M2M gateways. Examples of M2M area networks include personal area network (PAN) technologies such as IEEE 802.15.1, Zigbee, Bluetooth, IETF ROLL, ISA100.11a, among others, or local networks such as power line communication (PLC), M-BUS, Wireless M-BUS, and KNX.[3]
3. **M2M gateway:** A gateway that runs M2M application(s) using M2M service capabilities. The gateway acts as a proxy between M2M devices and the network domain. The M2M gateway may provide service to other devices (e.g., legacy devices) connected to it that are hidden from the network domain. As an example, an M2M gateway may run an application that collects and treats various information (e.g., from sensors and contextual parameters).

The **network domain** is composed of the following elements:

1. **Access network:** A network that allows the M2M device and gateway domain to communicate with the core network. Access networks include (but are not limited to) digital subscriber line (xDSL), hybrid fiber coax (HFC), satellite, GSM/EDGE radio access network (GERAN), UMTS terrestrial radio access network (UTRAN), evolved UMTS terrestrial radio access network (eUTRAN), W-LAN, and worldwide interoperability for microwave access (WiMAX).
2. **Core network:** A network that provides the following capabilities (different core networks offer different features sets):
   – IP connectivity at a minimum, and possibly other connectivity means
   – Service and network control functions
   – Interconnection (with other networks)
   – Roaming

[3]KNX (administered by the KNX Association) is an OSI-based network communications protocol for intelligent buildings defined in standards CEN EN 50090 and ISO/IEC 14543. KNX is the follow-on standard built on the European Home Systems (EHS) Protocol, BatiBUS, and the European Installation Bus (EIB or Instabus). Effectively, KNX uses the communication stack of EIB but augmented with the physical layers and configuration modes BatiBUS and EHS; thus, KNX includes the following PHYs:

- Twisted pair wiring (inherited from the BatiBUS and EIB Instabus standards). This approach uses differential signaling with a signaling speed of 9.6 Kbps. Media access control is controlled with the CSMA/CA method
- Powerline networking (inherited from EIB and EHS)
- Radio (KNX-RF)
- Infrared
- Ethernet (also known as EIBnet/IP or KNXnet/IP)

- Core networks (CoNs) include (but are not limited to) 3GPP CoNs, ETSI TISPAN CoN, and 3GPP2 CoN

3. **M2M service capabilities:**
   - Provide M2M functions that are to be shared by different applications
   - Expose functions through a set of open interfaces
   - Use CoN functionalities
   - Simplify and optimize application development and deployment through hiding of network specificities

The "M2M service capabilities" along with the "core network" is known collectively as the "M2M core."

The **applications domain** is composed of the following elements:

1. **M2M applications:** Applications that run the service logic and use M2M service capabilities accessible via an open interface.

There are also management functions within an overall M2M service provider domain, as follows:

1. **Network management functions:** Consists of all the functions required to manage the access and core networks; these functions include provisioning, supervision, fault management.
2. **M2M management functions:** Consists of all the functions required to manage M2M service capabilities in the network domain. The management of the M2M devices and gateways uses a specific M2M service capability.
   - The set of M2M management functions include a function for M2M service bootstrap. This function is called M2M service bootstrap function (MSBF) and is realized within an appropriate server. The role of MSBF is to facilitate the bootstrapping of permanent M2M service layer security credentials in the M2M device (or M2M gateway) and the M2M service capabilities in the network domain.
   - Permanent security credentials that are bootstrapped using MSBF are stored in a safe location, which is called M2M authentication server (MAS). Such a server can be an AAA server. MSBF can be included within MAS, or may communicate the bootstrapped security credentials to MAS, through an appropriate interface (e.g., the DIAMETER protocol defined in IETF RFC 3588) for the case where MAS is an AAA server.

The H2M portion of the IoT could theoretically make use of these same mechanisms and capabilities, but the information flow would likely need to be front-ended by an access layer (which can also be seen as an application in the sense described above) that allows the human user to interact with the machine using an intuitive interface. One such mechanism can be an HTML/HTTP-based browser

that interacts with a suitable software peer in the machine (naturally this requires some higher level capabilities to be supported by the DEP/machine in order to be able to run an embedded web server software module). (When used in embedded devices or applications, web servers must assume they are secondary to the essential functions the device or application must perform; as such, the web server must minimize its resource demands and should be deterministic in the load it places on a system.[4])

2.3 BASIC NODAL CAPABILITIES

Consistent with the HLSA, a remote device generally needs to have a basic protocol stack that supports as a minimum local connectivity and networking connectivity (we include the transport layer in our terminology here, whether this is TCP, UDP, or some other protocol); in addition, some higher layer application support protocols are generally needed, with varying degrees of computational/functional sophistication. See Figure 2.9. IoT devices may have capability differences, such as but not limited to the following (25): maximum transmission unit (MTU) differences, simplified versus full-blown web protocol stack (COAP/UDP versus HTTP/TCP), single stack versus dual stack, sleep schedule, security protocols, processing and communication bandwidth. The networking technologies listed above, including 3GPP, 3GPP2, ETSI TISPAN, eUTRAN, GERAN, HFC, IETF ROLL, ISA100.11a, KNX, M-BUS, PLC, Satellite, SCADA (Supervisory Control And Data Acquisition), UTRAN, WiMAX, Wireless M-BUS, W-LAN, and xDSL, are discussed in more detail in the chapters that follow.

Distributed control/M2M typically entails continuously changing variables to control the behavior of an application. Typical requirements include the following capabilities (26):

- Retransmission
  - Network recovers from packet loss or informs application
  - Recovery is immediate: on the order of RTTs, not seconds

[4]As an illustrative example of an embedded web server, Oracle's GoAhead WebServer is a simple, portable, and compact web server for embedded devices and applications; it runs on dozens of operating environments and can be easily ported and adapted. The GoAhead WebServer is a simple, compact web server that has been widely ported to many embedded operating systems. Appweb is faster and more powerful—but requires more memory. If a device requires a simple, low end web server and has little memory available, the GoAhead WebServer is ideal; if the device needs higher performance and extended security, then Appweb is the right choice. As one of the most widely deployed embedded web servers, Appweb is being used in networking equipment, telephony, mobile devices, consumer and office equipment as well as hosting for enterprise web applications and frameworks. It is embedded in hundreds of millions of devices. The server runs equally well stand-alone or in a web farm behind a reverse proxy such as Apache (24).

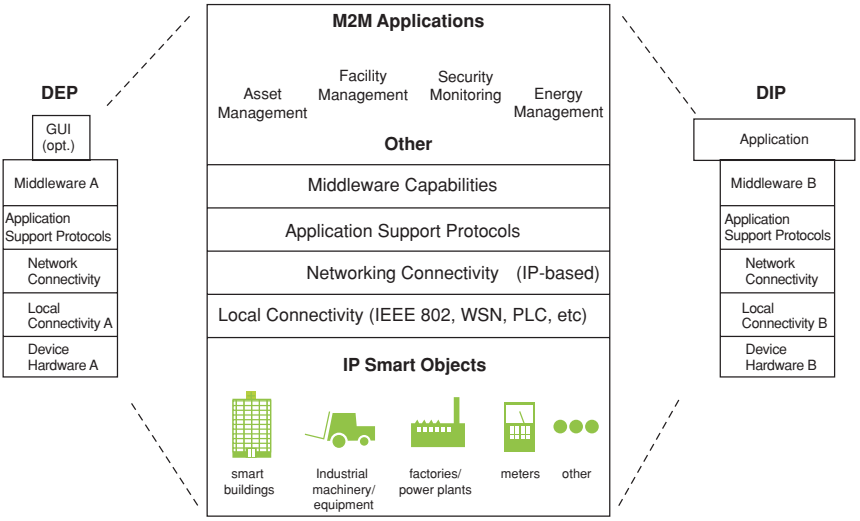

FIGURE 2.9 Protocol stack, general view.

- Network independent of MAC/PHY
- Scale
  - Thousands of nodes
  - Multiple link speeds
- Multicast
  - Throughout network
  - Reliable (positive Ack)
- Duplicate suppression
- Emergency messages
  - Routed and/or queued around other traffic
  - Other traffic slushed as delivered
- Routine traffic delivered in sequence
- Separate timers by peer/message
- Polling of nodes
  - Sequential
  - Independent of responses
- Paradigm supports peer-to-peer
  - Not everything is client/server
- Capabilities
  - Discover nodes
  - Discover node capabilities
  - Deliver multisegment records (files)

- Exchange of multisegment records
- Network and application versioning
- Simple publish/subscribe parsers
- Security
  - Strong encryption
  - Mutual authentication
  - Protection against record/playback attacks
  - Suite B ciphers

Related to the last item, Suite B security is a National Security Agency (NSA) directive that requires that key establishment and authentication algorithms be based on elliptic curve cryptography, and that the encryption algorithm be AES. Suite B defines two security levels, of 128 and 192 bits (see Glossary for additional information).

REFERENCES

1. Hazenberg W, Huisman M. *Meta Products: Building the Internet of Things*. Amsterdam, NL: BIS Publishers; 2011.
2. Internet Architecture Board. Interconnecting Smart Objects with the Internet Workshop 2011, 25th March 2011, Prague.
3. Walter K-D. Implementing M2M applications via GPRS, EDGE and UMTS. Online Article, August 2007, http://m2m.com. M2M Alliance e.V., Aachen, Germany.
4. Nordman B. Building Networks. Interconnecting Smart Objects with the Internet Workshop 2011, 25th March 2011, Prague.
5. Ladid L. Keynote Speech, International Workshop on Extending Seamlessly to the Internet of Things (esloT-2012), in conjunction with IMIS-2012 International Conference; 2012 Jul 4–6; 2012, Palermo, Italy.
6. Financial Times Lexicon, London, U.K. Available at http://lexicon.ft.com.
7. Botterman M. Internet of Things: an early reality of the Future Internet. Workshop Report, European Commission Information Society and Media, May 2009.
8. Lee GM, Park J, Kong N, Crespi N. The Internet of Things – Concept and Problem Statement, July 2011. Internet Research Task Force, July 11, 2011, draft-lee-iot-problem-statement-02.txt.
9. Staff. Smart networked objects and Internet of Things. White paper, January 2011, Association Instituts Carnot, 120 avenue du Général Leclerc, 75014 Paris, France.
10. OECD. Machine-to-Machine Communications: Connecting Billions of Devices. *OECD Digital Economy Papers*, No. 192, 2012, *OECD Publishing*. doi:10.1787/5k9gsh2gp043-en
11. Urien P, Lee GM, Pujolle G. HIP support for RFIDs. HIP Research Group, Internet Draft, draft-irtf-hiprg-rfid-03, July 2011.
12. Atzori L, Iera A, Morabito G. The internet of things: a survey. Computer Networks, October 2010;54 (15):2787–2805.

13. Guinard D, Trifa V, Karnouskos S, Spiess P, Savio D. Interacting with the SOA-based Internet of things: discovery, query, selection, and on-demand provisioning of web services. IEEE Services Computing, IEEE Transactions, July–September 2010;3 (3).
14. ITU-T Internet Reports. Internet of Things. November 2005.
15. Malatras A, Asgari A, Bauge T. Web enabled wireless sensor networks for facilities management. IEEE Systems Journal, 2008;2 (4).
16. Sarma A, Girao Joao. Identities in the Future Internet of Things. Wireless Pers Comm., 2009.
17. Sundmaeker H, Guilemin P, Friess P, Woelffle S, editors. *Vision and Challenges for Realizing the Internet of Things*. European Commission, Information Society and Media, March 2010.
18. ITU-T Y. 2002. Overview of ubiquitous networking and of its support in NGN. November 2009.
19. Zouganeli E, Svinnset IE. Connected objects and the Internet of things-a paradigm shift. Photonics in Switching 2009, September 2009.
20. International Telecommunications Union, Telecommunication Standardization Sector Study Period 2009–2012. IoT-GSI – C 44 – E. August 2011.
21. Kreisher K. Intel: M2M data tsunami begs for analytics, security. Online Magazine, October 8, 2012. Available at http://www.telecomengine.com.
22. Lee GM, Choi JK, et al. Naming architecture for object to object communications. HIP Working Group, Internet Draft, March 8, 2010, draft-lee-object-naming-02.txt
23. Machine-to-Machine Communications (M2M); Functional Architecture Technical Specification, ETSI TS 102 690 V1.1.1 (2011-10), ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.
24. Embedthis Inc. Promotional Materials, Embedthis Software, LLC, 4616 25th Ave NE, Seattle, WA 98105. Available at http://embedthis.com.
25. Arkko J. Interoperability Challenges in the Internet of Things. Interconnecting Smart Objects with the Internet Workshop 2011, 25th March 2011, Prague.
26. Dolan B, Baker F. Distributed Control: Echelon's view of the Internet of Things. Interconnecting Smart Objects with the Internet Workshop 2011, 25th March 2011, Prague.