Communication Technology That Suits IoT - A Critical Review

Conference Paper · April 2013

DOI: 10.1007/978-3-642-41054-3_2

Aqeel-ur Rehman
Hamdard University
58 PUBLICATIONS **1,239** CITATIONS
SEE PROFILE

Communication Technology That Suits IoT – A Critical Review

Aqeel-ur-Rehman[1,*], Kashif Mehmood[2,**],
and Ahmed Baksh[2]

[1] Faculty of Engineering Sciences and Technology,
Hamdard University, Karachi, Pakistan
aqeel.rehman@hamdard.edu
[2] GSESIT, Faculty of Engineering Sciences and Technology,
Hamdard University, Karachi, Pakistan

Abstract. Communication technologies play an important role in any wireless network. The networks comprise on energy constraint devices require low power communication technologies. Internet of Things (IoT) is a new and progressing concept that provides connectivity to the Internet via smart sensing devices to attain identification and management in a heterogeneous connectivity environment. Various communication technologies for Wireless Personal Area Networks (WPAN) like IoT are available presenting several properties. IoT concept involves all heterogeneous objects around us communication with each other locally and via internet globally. Such kind of network poses several challenges and requirements for choosing the best amongst the available communication technologies. This paper is intended to present a critical study of IoT requirement, issues and challenges and propose the best or suitable amongst the available communication technologies.

Keywords: Internet of Things, Communication technologies, Wireless Sensor Network, Smart Devices, Wireless Personal Area Network.

1 Introduction

Many connected devices are approaching the new communication technologies due to their networks and services approaches as per their limits and available resources. The new communication technologies have a provision to provide seamless connectivity which is the requirement of IoT. Communication technologies used in IoT has low power consumption, low bandwidth used, low computation power, seamless communication with devices in environment due to the concept of IoT is computing for everyone, anywhere, any network and any service. Moreover, these technologies are very much penetrating in e-health, e-traffic management, e-disaster management etc.

[*] Associate Professor.
[**] MS Student.

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 14–25, 2013.

Internet of Things is one of the important new concepts that provides connectivity of sensors and devices to the internet that provides connectivity to everyone, anywhere and anytime. The application of IoT towards home appliance, vehicles and environment demands the availability of Smart objects that are capable to sense other objects and able to communicate and interact with each other without the intervention or involvement of humans.

In this paper, the importance of IoT in terms of different communication technologies has been discussed that will make IoT suitable for different applications in terms of its various challenges and requirements.

2 The Vision of IoT

The Internet of Things (IoT) term was first coined by Kevin Ashton in 1991 [1]. As the technology and implementation ideas are moving forward, the definition of term is evolving [2]. There are two vision of IoT (i) Things Oriented vision and (ii) Internet Oriented vision [3]. The first vision involves RFID as a simple thing to be the part of Auto-ID Lab while the second vision was based on network as core technology leading to Semantic Web. The definitions above covered the way to the ITU vision of IoT, according to which: “from anytime, anyplace connectivity for anyone, we will now have connectivity for anything”.

After computer, Internet and mobile communication networks, IoT is a new wave in Information world. Internet of Things affirms to a huge network involving Internet and multiple sensor equipments to collect information [4-6]. The purpose to build such network is to recognize, locate, track, administer, and trigger the relative events.

3 IoT Architecture

IoT architecture is of three layered architecture (refer to Fig. 1). The functionalities of the layers are specified below:

Perception Layer. Object identification and information collection is the main function of this layer. It comprises of sensors, actuators, RFID tags, RFID readers/ writers and information display units (like PDA, Tablet PC, cell phone etc.)

Network Layer. Information transfer that is collected via perception layer is the main objective of this layer. Wireless Networks, wired networks, Internet, network management systems are the major components of the network layer.

Application Layer. Event detection, intelligent solutions and to perform user required functions is the responsibility of this layer.

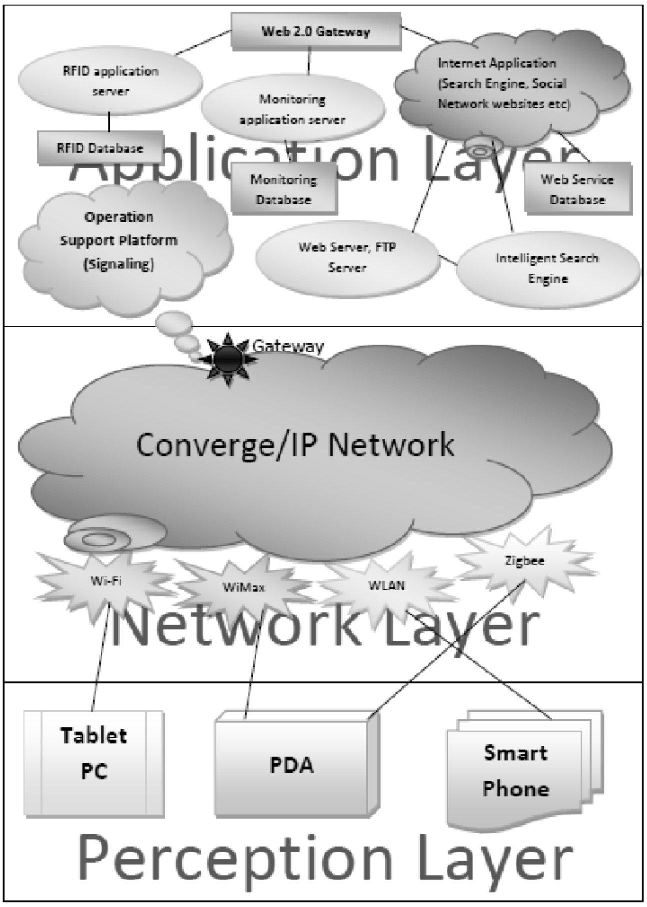

Fig. 1. Internet of Things (IoT) Architecture

4 Challenges

There are many challenges that are linked with the IoT highlighted below:

Standards. There is no standard available for the deployment of IoT globally that may make it conventional for the people [7].

Network Foundation. Limitations imposed due to the current Internet architecture for mobility, scalability, manageability and availability, IoT network establishment is facing difficulties [8].

Security, Privacy and Trust. The crucial areas in IoT are Security, Privacy and Trust. In Security area, IoT domain is facing the following challenges [8-9]:

- Security to be ensured at design time and execution time for the architecture of IoT
- Proactive identification and protection of IoT from arbitrary attacks (e.g. DoS and DDoS attacks) and malicious software.

Privacy is the second major concern. The main challenge in acceptance of IoT globally is the privacy of quantity of connected objects. The term of privacy in IoT means user/ object privacy that is facing specific challenges that are:

- There is no privacy control over personal information and location privacy of individual's physical location and movement.
- Unavailability of Standard Operation Procedures (SOPs)/methodologies and tools, privacy enhancement technologies and relevant protection laws.

Trust is having the specific following challenges:

- The System must provide the environment for easy and natural exchange of critical, protected and sensitive data e.g. smart objects may communicate with the available trusted services on behalf of users /organizations.
- The IoT System design must provide built-in trust facility for each available service.

Managing Heterogeneity. Must be able to overcome applications, environments and devices heterogeneity. The management of heterogeneity posses the major challenges that are [8]:

- Need of useful services for managing large amount of data
- Required affective mechanisms for sensor data discovery, senor data querying, publishing and subscribing; and design architecture for sensor data communication protocols, sensor networking and storage.
- Need appropriate mechanisms for sensor data stream processing, data mining, correlation, and aggregation filtering techniques. For this reason, regulate heterogeneous technologies, devices etc.

Identification and Authentication. In IoT, purpose of identification and tracking entities is to protect identification from tracking by unauthorized attacks in the network. It must be provided to users with right control over the privacy of their personal information [3].

Trust and Ownership. The trust and ownership is most currently discussing issue that how we trust on the information captured and communicate with the global network securely and reliably? Trust involves the authority and integrity of the communicating parities, accurate sensing of the data, and legal reader partnership [10].

Integration and Coordination. The challenge in IoT is how to collaborate with two different type of network, one of them is internet and other is the physical world and they work as a joint venture for meaningful results. In the integration, the major issues are cost, stability, communication speed, bandwidth, trust and security of the physical world and the internet [7]. IoT requires collaboration and teamwork among people, programs, process and services to globally share the data [11].

Regulation. The Regulation means that the processes work under IoT with settled rules. There are three different regulations (i) traditional government, (ii) international agreements and (iii) self-regulations. The Traditional government regulation is being limited in its domain and do not suit the global structure of IoT. On the other hand, self-regulation is cost effective and well-organized but only few interest and righteous thing may take part in it. For international agreements an international body such as WTO may work as legislator [12].

5 Communication Technologies in IoT

The major communication technologies that can be utilized by IoT devices are summarized below:

5.1 ZigBee

ZigBee is IEEE 802.15.4 standard. It is reliable wireless networking technology which developed by ZigBee Alliance. It is designed for limited range network monitoring and controlling due to its low data rate and short range. The main area of utilization of this technology is in Home Automation, Smart Energy devices, lighting, HVAC and security etc. Due to its low-power, high level communication protocol using small digital radios, it comes under wireless personal area network (WPAN). It also has a unique functionality of self-organizing, multi-hop and reliable mesh networking with long battery life time [13-15].

5.2 RF Links

Another preference to connect devices and make them talk is utilize simple radio frequency (RF) boundaries. It can provide communication range between 100m and 1km (depending on the transmission power and the antenna used).

RF communication modules do not provide any implementation of the TCP/IP communication protocol (or any other protocol). Data rates are quite low (up to 1Mpbs) and also need an Internet-enabled gateway that will provide access to the devices for making a complete IoT network.

The Radio Frequency Identification (RFID) technology has been initially introduced for identifying and tracking objects with the help of small electronic chips, called tags. RFID has been originally categorized as the enabling communication power for the Internet of Things, due to its low cost, high mobility and efficiency in identifying devices and objects. Despite RFID is very common for device identification and some information exchange [4].

Drawback. It cannot alone support the creation of IoT networks since it cannot provide any direct or indirect (e.g., through a gateway) communication to the Internet. The device proximity is also another drawback [4].

5.3 Bluetooth

Bluetooth is an IEEE 802.15.1 standard for low cost, short range and cheap devices of wireless radio technology. Bluetooth has been one of the first wireless communication protocols designed with lower power consumption for replacing short-range wired communications (in computer peripherals, mobile phone accessories, etc.), short distance data sharing and devices' mobility support. It has an exceptional property of creating personal area network during communication and discovers and communicates to its neighbor without need to be in visual line of sight. Due to its global standard it is also known as WPAN (Wireless Personal Area Network).

It is very important for the case of IoT since many of the devices that one would like to interconnect to the IoT (sensors, actuators, etc.) having limited power resources.

Drawback. A major drawback of Bluetooth is that it cannot provide direct connectivity to the Internet. Once has to provide an intermediate node, e.g., a PC that will act as a gateway to the outer world [13-14].

5.4 Bluetooth 4.0 LE

Traditionally, Bluetooth is used in a connection-oriented manner and it cannot directly connect to the internet. Once it is connected; a link is maintained even there is no data flow. The new Bluetooth low energy (BLE), old name is WiBree, is a subset to Bluetooth v 4.0. It has new protocol stack and new profile architecture. This version has been adopted as of June 2010. It provides new adverting mechanism, quick discovery and enable connection and uses Asynchronous connection-less MAC for low latency rate and fast communication. Bluetooth 4.0 is users friendly as it introduces New Generic Attribute Profile which is simpler to use [16].

5.5 6LoWPAN

The 6LoWPAN is Wireless PAN with low power and supports IPv6 network. It is a connection oriented technology in which router forward the data to its next hop to the 6LoWPAN gateway which is connected to 6LoWPAN with the IPv6 domain and then forward the data to its respected device correctly.

With IPv6 we have enough address space to identify all the things in the world. In IP based network standard protocols (HTTP, TCP/IP) are directly applied on sensor nodes just as they do with traditional web servers out there in the Internet [11][17].

5.6 Z-Wave

Z-Wave protocol architecture developed by ZenSys and promoted by the Z-Wave Alliance. It is another low power consuming which mostly used in automation and light commercial environment. It has an open communication protocol. The main purpose of Z-wave is for a reliable massage passing from a control unit to one or more nodes in the network. Z-wave have two types of devices, one is poll Controllers which send commands to the slaves, the second type of device, which reply to the controller to execute the commands [6][19].

5.7 WiFi

Wireless fidelity is known as Wi-Fi, the IEEE 802.11x standards, is the most common way to connect devices wirelessly to the Internet. Laptop, Smartphone and Tablet PC are equipped with WiFi interfaces and talk to wireless router and provide two way accesses to the Internet. The Wi-Fi standard family allows establishing wireless network on short distances. Wi-Fi has series types of networks like IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11e: QoS extension, IEEE 802.11f: extension for managing handover and IEEE 802.11i security extension. The Wi-Fi group is working on unlicensed spectrum of 2.4 GHz (ISM) band.

Table 1. Communication Technologies – A Comparision

Standard	**Bluetooth**	**Bluetooth 4.0 LE**	**ZigBee**	**Wi-Fi**	**6LoWPAN**	**RF – Link**	**Z-Wave**
IEEE Spec.	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.11a/b/g/n	IEEE 802.15.4 2006	IEEE C95.1 –2005	Z-Wave alliance
Topology	Star	Star	Mesh, Star, Tree	Star	Mesh, Star	-	Mesh
Bandwidth	1 Mbps	1 Mbps	250 Kpbs	Upto 54 Mbps	250 Kbps	18 MHz	900 MHz
Power Consumption	Very Low	Very Low	Very Low	Low	Very Low	Very Low	Very low
Max. data rate (M bit/s)	0.72	5-10 m	0.25	54	800 m (Sub-GHz)	1	9600 bits or 40 kbits
Bit time (µs)	1.39	-	4	0.0185	-	-	-
Range	<30 m	5-10 m	10-300 m	4-20 m	800 m (Sub-GHz)	<3 m	30 m
Spectrum	2.4 GHz	2.4 GHz	2.4 GHz	2.4-5 GHz	2.4 GHz	2.4 GHz	2.4 Ghz
Channel Bandwidth	1 MHz	2400 – 2480 MHz	0.3/0.6 MHz, 2 MHz	22 MHz	868 – 868.6 MHz (EU) 902-928 MHz (NA) 2400 – 2483.5 MHz (WW)	-	868 MHz

The 802.11e standard will include two operating mode for improving the services of voice (i) Wi-Fi Multimedia Extensions (WME) – Mandatory and (ii) Wi-Fi Scheduled Multimedia (WSM) – Optional.

The commercially available WiFi modules (like the one WiFi communication module in a pluggable form known as XBee series modules) can be directly integrated to an IoT device and provide instant connectivity. The major advantage over the other wireless technologies is the fact that WiFi networks are very easy to establish and thus IoT devices with WiFi modules can have direct connection to the Internet.

Drawback. This technology (which was at no means designed for IoT networks) is more power demanding than the others [14-15].

6 Requirements of IoT

In IoT, heterogeneous devices and communication technologies are used to develop a seamless computing for everywhere. In this regard, we must need improvement in energy, communication, resource constrained, scalability, modularity, extensibility and interoperability among heterogeneous things and their environments that are the key design requirements for IoT [10].

6.1 Energy

Energy problems, in all its phases, from gathering to conservation and usage, are central to the development of the IoT. There is a need to research and grow solutions in this area (nano-electronics, semiconductor, sensor technology, micro systems integration) having as an objective of ultra low power devices, as existing devices seem insufficient considering the processing power needed and energy restrictions of the future.

6.2 Intelligence

Abilities such as self-awareness, context awareness and inter-machine communication are well-thought-out a high priority for the IoT. Mixing of memory and processing power and the ability to endure harsh environments are also a high priority, as are the best possible security techniques. Novel cognitive approaches that leverage opportunistically on the time dependent available heterogeneous network resources can be accepted to support unified continuous access to the information network as well as grip irregular network connectivity in harsh and/or mobile environments. “Intelligent” methods to knowledge discovery and device control will also be important research challenges.

6.3 Communication

New smart antennas (fractal antennas, adaptive antennas, receptive directional antennas, plasma antennas) that can be fixed in the objects and made of new materials are the communication means that will permit new advanced communications systems on chip. Modulation schemes, transmission rates, and transmission speed are also major issues to be undertaken. New advanced solutions need to be defined to efficiently support mobility of billions of smart things, possibly well-found with multiple heterogeneous network resources. Last but not least, network virtualization techniques are key to confirm an evolutionary path for the arrangement of IoT applications with secure Quality of Service (QoS).

6.4 Integration

Integration of wireless identification technologies (like Radio Frequency Identification — RFID) into packaging, or, rather, into products themselves will allow for important cost savings, improved eco-friendliness of products and allow a new dimension of product self-awareness for the help of customers. Integration requires addressing the need for heterogeneous systems that have sensing, acting, communication, cognitive, processing and compliance features and includes sensors, actuators, nanoelectronics circuits, embedded systems, algorithms, and software embedded in things and objects.

6.5 Dependability

Dependability of IoT systems is of supreme importance; so the IoT network structure must ensure reliability security and privacy by supporting individual authentication of billions of dissimilar devices using heterogeneous communication technologies across different executive domains. Reliable energy-efficient communication protocols must also be intended to confirm dependability.

6.6 Semantic Technologies and IoT

IoT requires devices and applications that can easily connect and interchange information in an ad-hoc way with other systems. This will involve devices and services to prompt needs and capabilities in formal ways. To enable the interoperability in the IoT further research into semantic technologies is needed. Examples of challenges are large-scale dispersed ontologies, new methods to semantic web services, rule engines and methodologies for hybrid reasoning over large heterogeneous data and fact bases, semantic-based discovery of devices and semantically driven code generation for device interfaces.

6.7 Modeling and Design

The design of large-scale IoT systems is stimulating due to the large number of heterogeneous components involved and due to the complex duplications among devices introduced by cooperative and distributed approaches. To cope with this issue, original models and design frameworks need to be planned; for example, inspired by co-simulation methods for large systems of systems and hardware-in-the-loop approaches.

7 Requirement of Communication Technologies in IoT

The IoT Communication Technologies should provide a seamless communication and secure access to the internet anywhere, anytime, any network at any bandwidth/speed. We should never feel any difference to its indoor or outdoor communication. It should have unlimited range, zero latency rate and unlimited throughput. On the other hand, it should also cost effective and low energy consumption. It should also ensure the protection of privacy. Some of the requirements discussed for communication technologies in IoT are [20]:

- *Range and dissemination.* Due to walls, window, plants and etc. it is deployed in wide area, but the power consumption and throughput are inversely proportional to the range.
- *Power Consumption.* Low power operated devices for resulting low throughput and range.
- *Throughput.* Need for high throughput means the sustainable power of battery life and better coverage area.
- *Number of devices.* If the more devices used it consumes more resource and performance of computation is affected.
- *Types of network supported.* Due to variable length of topologies used like mesh, tree, peer-to-peer etc. that have their own advantages and drawbacks according to its standardization, throughput and range and other.
- *Globalization usage.* Some of the technologies are used in their boundaries (countries) due to its regulations and issues.
- *Mobility.* Must support the mobility of devices whether it is working in any location and environment.
- *Failover capabilities.* Need to be fast backup solution in case of network fails.
- *Multi-protocol support.* Must support multiple networks for its situation.
- *Security and Privacy.* All the communication is needed to be in secured manner and no unauthorized access to break the privacy of any data.

8 Discussion on IoT Communication Technologies

Following are the technologies amongst the above mentioned technologies (refer to Table 1) that suits most of the requirements of IoT:

Wi-Fi IEEE 802.11x is wireless LAN. It provides point-to-point and point-to-multi point high speed and robust communication. It allows multiple users to connect in the same time period to same frequency band with minimum interference to the other users. Wi-Fi operates on three different non-interoperable technologies i) Frequency Hopping Spread Spectrum (FHSS) ii) Direct Sequence Spread Spectrum, iii) and Infrared (IR). Wi-Fi 802.11n Technology, based on Multiple Input Multiple Output (MIMO) technology is intended to increase the data rates upto 600 Mbps and onwards. IEEE 802.11i is known as (WPA–2) that enhances the cyber security and Advanced Encryption Standard (AES) which fulfill the IoT requirement. It is easy to install, supports mobility of devices, and less expensive. The reliability and availability is achieved by applying proper path engineering and system design techniques. The proper implementation of massage acknowledgement, error correction algorithms, data buffering etc. enhances the reliability of massage transmission over wireless medium. In addition, 802.11ah (working on Wi-Fi on ISM bands below 1 GHz) modify it for ad-hoc, mesh networking, infrastructure-independent and longer-range control of sensor networks therefore, the band new-technologies better suited for certain aspects of IoT communication and be a part in future of IoT.

The low power, cost effective ZigBee is reliable for home area wireless network developed by ZigBee Alliance based on an open global standard. It works on 2.4 GHz unlicensed frequency of IEEE 802.15. 4 standard. The major achievement in ZigBee technology is long battery life cycle but it is depending upon the topology adopted. Due to its high battery life and low power consumption, it is mostly used in home automation but in industrial environments it is not well adapted.

Bluetooth is low power short range radio frequency based Wireless Personal Area Network (WPAN). It can facilitate both point-to-point and point-to-multipoint communication configuration. The advance achievement is Bluetooth 4.0 low energy consumption technology. Bluetooth Low Energy (BTLE) is being used in health care industry for portable medical and lifestyle devices. It's preventing highly influenced by surrounding communication link and may interference in IEEE 802.11 WLAN network technology. The provide security, scalability and reliability authorization techniques are used before transmit or receive any kind of information.

9 Conclusion

IoT is a new and emerging concept that gaining popularity day by day. It involves smart devices available all around us and networked them as WPAN locally while globally as Internet. Such connectivity requires wireless communication technologies like Bluetooth, Wi-Fi, ZigBee, Z-Wave and RF Link. Every concept poses it specialized requirement for optimal utilization. In this paper, we critically analyzed the issues, requirements and challenges of Internet of things (IoT) specifically related to communication technology. Critical analysis presents Bluetooth LE, 6LoWPAN and WiFi as suitable candidates for future IoT but many issues are still to address for which some new technologies are in demand.

Acknowledgement. This work is partly supported by Center of Research in Ubiquitous Computing, Hamdard University chapter from which the authors are associated.

References

1. Ashton, K.: That 'Internet of Things' Thing. RFiD Journal 22, 97–114 (2009)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks 54(15), 2787–2805 (2010)
3. ITU Internet Reports 2005: The Internet of Things, `http://www.itu.int/osg/spu/publications/internetofthings` (accessed on September 19, 2011)
4. International Telecommunication Union UIT. ITU Internet Reports 2005: The Internet of Things[R] (2005)
5. Gustavo, R.G., Mario, M.O., Carlos, D.K.: Early infrastructure of an Internet of Things in Spaces for Learning. In: Eighth IEEE International Conference on Advanced Learning Technologies, vol. 2, pp. 381–383 (July 2008)

6. Sarma, A.C., Girão, J.: Identities in the future internet of things. Wireless Personal Communications 49(3), 353–363 (2009)
7. CERP-IoT: Cluster of European Research Projects on the Internet of Things, Vision and Challenges of Realizing the Internet of Things (March 2010), `http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf` (accessed on May 2012)
8. Internet of Things Strategic Research Roadmap, `http://www.grifs-project.eu/data/File/CERP-IoT%20SRA_IoT_v11.pdf` (accessed on April 2012)
9. Agrawal, S., Das, M.L.: Internet of Things—A paradigm shift of future Internet applications. In: 2011 Nirma University International Conference on Engineering (NUiCONE), pp. 1–7 (December 2011)
10. Newmarch, J., Tam, P.: Issues in Ownership of Internet Objects. In: The Fifth International Conference on Electronic Commerce Reaserch, Montral, Canada (2002)
11. Petrie, C.: The Future of the Internet is Coordination. In: Proceedings of FES-2010: Future Enterprise Systems Workshop (2010)
12. Weber, R.H., Weber, R.: Internet of things: legal perspectives. Springer Publishing Company, Incorporated (2010)
13. ZigBee – The Internet of Things, `http://www.vesternet.com/zigbee` (accessed on November 2012)
14. Doukas, C.: Building Internet of Things with the Arduino. CreateSpace Publishers (2012)
15. Lee, J.S., Su, Y.W., Shen, C.C.: A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In: 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2007), pp. 46–51 (November 2007)
16. Decuir, J.: Bluetooth 4.0: Low Energy, IEEE Annual Report (2010), `http://chapters.comsoc.org/vancouver/BTLER3.pdf` (accessed on October 2012)
17. Ee, G. K., Ng, C. K., Noordin, N. K., Ali, B. M.: A Review of 6LoWPAN Routing Protocols. In: Proceeding of Asia Pacific Advanced Network (2010)
18. The Danish Electricity Saving Trust's concept for energy saving devices, metering equipment and wireless communication
19. `http://www.savingtrust.dk/publications/concepts/dests-concept-for-energy-saving-devices-metering-equipment-and-wireless-communication` (accessed on December 2012)
20. Mainetti, L., Patrono, L., Vilei, A.: Evolution of wireless sensor networks towards the Internet of Things: A survey. In: Software, 19th International Conference on Telecommunications and Computer Networks (SoftCOM), pp. 1–6 (September 2011)
21. Machine-to-Machine Communications: Connecting Billions of Devices. OECD Digital Economy Papers, No. 192, OECD Publishing (2012), `http://dx.doi.org/10.1787/5k9gsh2gp043-en`
22. Bandyopadhyay, D., Sen, J.: Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Personal Communications 58(1), 49–69 (2011)