

IoT: Networking Technologies and Research Challenges

Jekishan K. Parmar
Assistant Professor,
Babaria Institute of Technology,
Vadodara

Ankit Desai
PhD scholar, School Engineering & Applied Sciences,
Ahmedabad University, Ahmedabad,
Data Engineer, IQM Co., Ahmedabad

ABSTRACT

This paper gives insight into how IoT networking is a unique combination of wireless personal area networks, like 6LoWPAN, ZigBee, and the IEEE 802.15.4 protocol, which runs the Medium Access Control and the physical layer operations for 6LoWPAN and ZigBee connectivity. In addition, this paper discusses about wireless LAN Wi-Fi technology, i.e. wireless local area network protocol and on a larger scale, mobile communication technology, such as LTE, that is used to provide connectivity to the internet, the wide area network. This paper focuses on how these technologies need to work together to provide IoT connectivity. It showcases important research challenges in said area.

General Terms

IoT, Networking Technologies, Communication

Keywords

IoT, PAN, Bluetooth, ZigBee, 6LoWPAN, Wi-Fi, WLAN, IEEE 802.15.4

1. INTRODUCTION

In an IoT Network, some of the major technologies are wireless personal area network viz. 6LoWPAN, ZigBee, Bluetooth. In addition, on a slightly larger wireless network scale, Wi-Fi, wireless LAN technology, is going to be used and needs to be supported. Then as, on the larger scale network, the backbone, is used in addition to the mobile communication network domain. Then smartphones and mobile communication phones will also be used and they will be connected to the base stations. The base stations will provide connectivity to the wider network, the internet. Considering this, many options are needed to think about. One thing is that smartphones are equipped with Bluetooth and Wi-Fi therefore IoT Network is possible. The most simple topology control will be a wireless PAN which is either like a Bluetooth or some other type of network. That is connected to a smartphone, and the smartphone will bring that signal up and connect it through LTE, or 4G/3G, to the base station, and the base station will connect to that wide area network, which is the internet. It can be observed that one technology linking on a technology of something. Considering wearable IoT Networks, a wearable IoT Network device is something like this as shown in figure 2. Wearable de-

vices such as shoes, watch, glasses, belt, etc. can be used to detect biometric information because they are close and attached to body and they can sense in real time. These devices can send data through Bluetooth technology to the smart phone that rests inside the pocket. In that case, the smartphone will be able to pick up this information and it will be able to use it through mobile communication link to send it to a base station. The base station, which is connected to a wide area network and the Internet, is going to be where the information connects to any other place we need in the world [1, 2, 3]. For example, if you are using your watch and also your shoes as well as your belt or something similar you have attached to self, to monitor your health condition that can be sent wirelessly to your smartphone then, your smartphone will send that information to the base station, which will be connected to the internet and that information can be delivered to a control centre or medical server. If something happens to you, they will know and they will be able to provide immediate support. A smart device can be used to collect the information that communicates with control centres or like a medical centre and this is how everything gets connected together.

2. COMPONENT TECHNOLOGIES

2.1 Wi-Fi

The Wireless Local Area Network. Wi-Fi is a WLAN technology that is based upon the IEEE 802.11 standards. Wi-Fi device, examples are, smartphones, smart tabs, other types of notebook computers and so on and so forth, are all equipped with Wi-Fi. Application areas would include home, school, computer laboratory, office building, and so many other places. Wi-Fi devices and their Access Points have a wireless communication range of about 30 meters indoors. Wi-Fi data range is based upon the protocol type. For example, 802.11a, b, g, n, ac and ad. Their data rates can be 54 Mbps, 11, 54, 150, 866.7 Mbps and 7 Gbps, respectively.

2.2 Bluetooth

It is a Wireless Personal Area Network protocol. It is designed by the Bluetooth Special Interest Group, the Bluetooth SIG. This replaces cables connecting many different devices. The major focus of Bluetooth is to get rid of cables wherever possible. For example, Bluetooth wireless headset. Heart monitors and other medical equipment that can also be connected to a smartphone using Bluetooth link. Thus, in this way Bluetooth connectivity replaces wires.

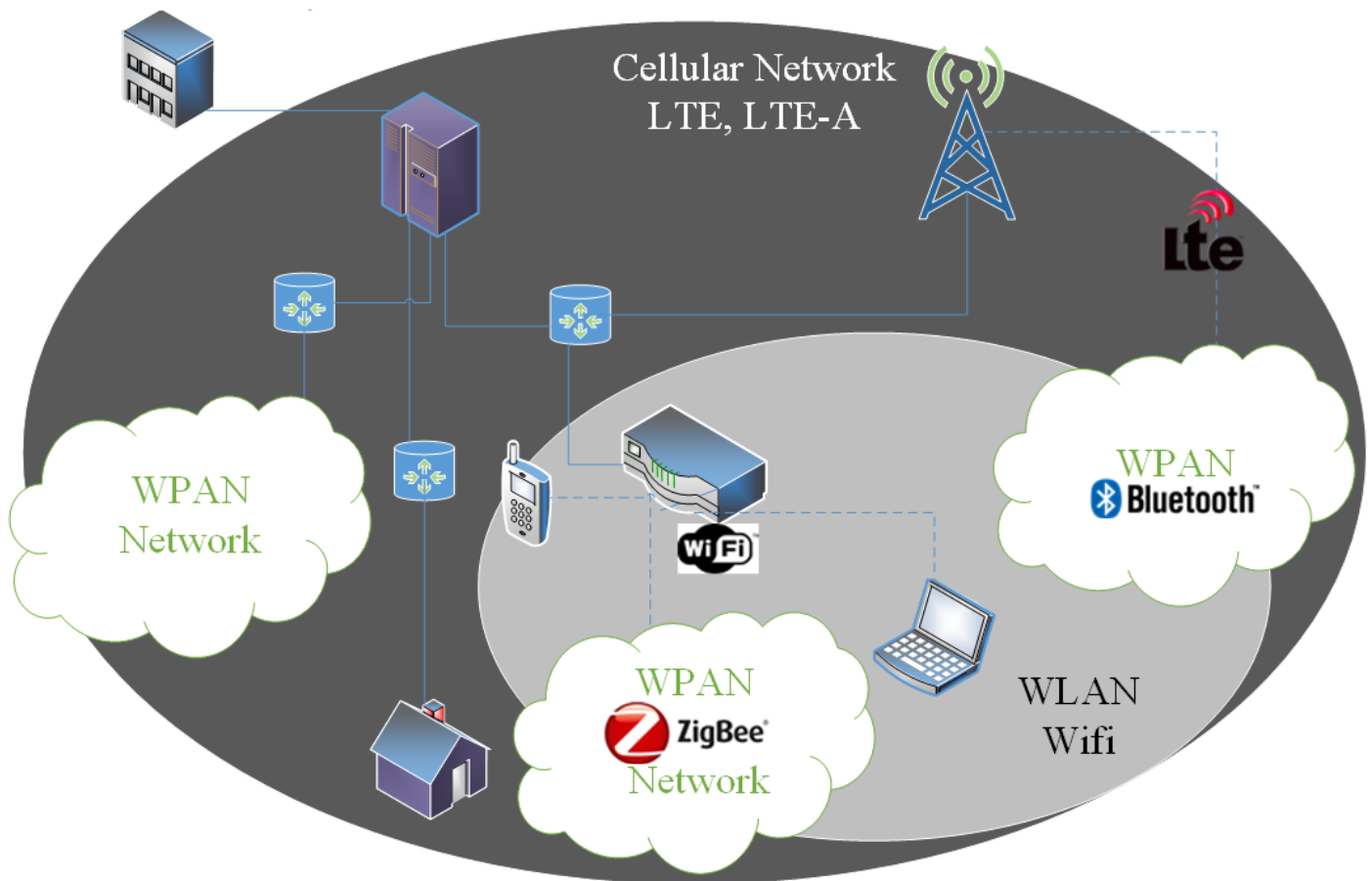


Fig. 1. IoT Networking

Standard area network range of Bluetooth is about 10 meters for indoor applications and related things, but using Bluetooth 4.0 the range is extended up to about 50 meters. Bluetooth Low Energy, which is a part of Bluetooth 4.0 standards, this provides reduced power consumption and cost reduction while maintaining a similar communication range. Just like Wi-Fi, Bluetooth has different data rates as well. Bluetooth 2.0 with EDR, can provide 2.1 Mbps data rate. Bluetooth 3.0 can support 24 Mbps. Bluetooth 4.0 achieves up to 25 megabits per second of a data rate [18, 19].

2.3 IEEE 802.15.4 standards

This is used in ZigBee, 6LoWPAN and all of these other type of applications wireless communication protocols. We are going to focus on two of the most popular ones which is ZigBee and 6LoWPAN. Reasons why 802.15.4 is used are: it is a low cost, low speed, low power, wireless personal area network protocol and it can be used in many ways in IoT.

2.4 Device support for 802.15.4 standard

There are basically two devices. One is a full function device (FFD) and the other is a reduced function device (RFD). An FFD is equipped with full functionality. It can send, receive, route data, and form clusters. It can serve as the PAN coordinator. That does

not mean that it will always be a PAN coordinator. It may elect to or sometimes if it sees somebody else, some other FFD is already doing that role, then in order to save energy, it may not do PAN coordinator operation. It may just work as a full functional device and then later on if that device, which is the PAN coordinator releases its role and some other device needs to take it, then the FFD may volunteer to take that role. Next, type of device is RFD, reduced function device. This has a reduced functional protocol compared to the FFD protocol stack. This can only communicate to full functional devices. It cannot serve as a PAN coordinator, it serves a role as a simple sensor or switch device, and it cannot provide routing functionality. Using, 802.15.4 one can form a star network topology, a peer-to-peer, P2P network topology. In addition, for a large scale network, you can form a cluster tree. Moreover, the role of coordinator is very important [15, 16], it controls the 802.15.4 network. A special form of a FFD needs to be taken, and it is a typical FFD function and added on with network coordination and service features. An FFD will need to take this role of coordinator to play a bigger role in controlling the network [17].

3. NETWORK TOPOLOGIES

First, star topology. As depicted in table 1, the devices that are FFDs are colored in green and the RFDs are colored just in blue. As it is shown below, an FFD in the middle (PAN Coordinator) provides

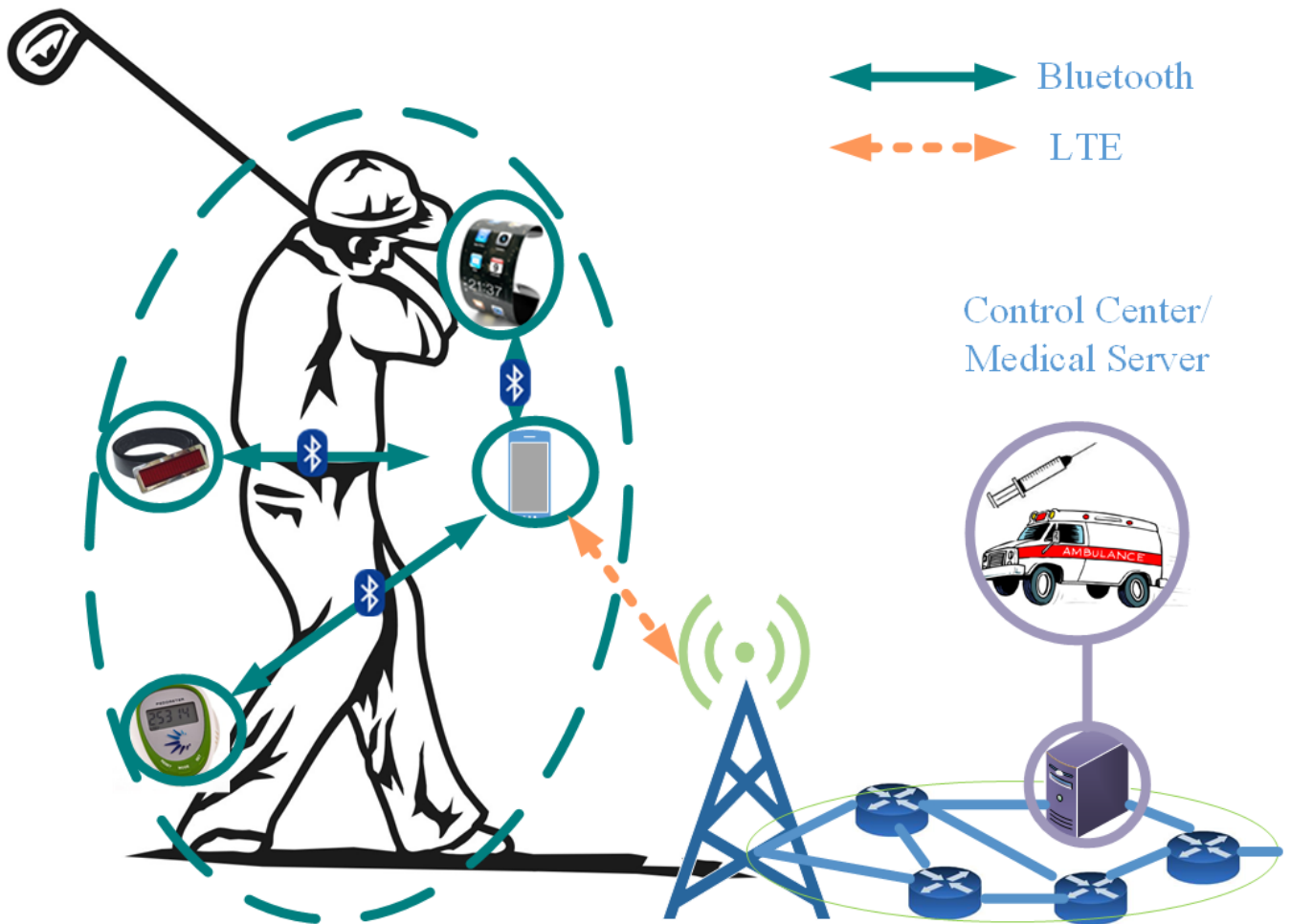


Fig. 2. Wearable IoT Networks

Octets 2:	1	0/2	0/2/8		0/2	0/2/8	Variable	2	
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address		Source PAN Identifier	Source Address	Frame Payload	Frame Check Sequence	

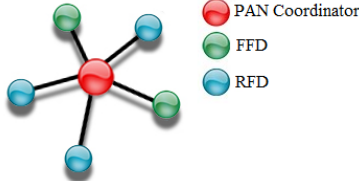
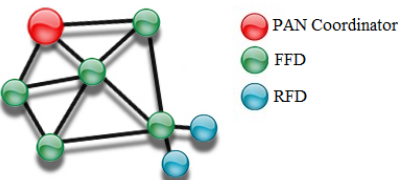
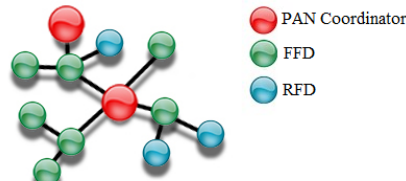
Bits: 0-2	3	4	5		6	7-9	10-11	12-13	14-15
Frame Type	Security Enabled	Frame pending	Ack. Requested		Intra PAN	Reserved	Destination Address Mode	Reserved	Source Address Mode

Fig. 3. IEEE 802.15.4 General Frame Format

the star topology formation. Nodes communicate through a central PAN coordinator, which is the FFD in the middle. Second, P2P topology. It can be observed that nodes communicate through the PAN coordinator, and through point-to-point links that they establish on the sides. Hence, extension of the star topology is basically

what enables the P2P topology to exist. Next is cluster tree topology. Here, among the FFDs, a PAN coordinator takes the major role and as you can see, it is where different clusters are formed based upon the FFDs. Moreover as shown above, the PAN coordinator connects the individual FFDs that are forming the star or P2P

Table 1. IEEE 802.15.4 Network Topologies

Topology	Model	Description
Star Topology		—Nodes communicate via the central PAN coordinator
P2P Topology		—Nodes Can Communicate via the PAN Coordinator and via Point-to-Point links —Extension of the star topology
Cluster Topology		—Cluster trees are similar to stars, through RFDs are only allowed to connect as the outer most branches —Diagram shows that the FFD connect the coordinator and a FFD can have connections to multiple end devices

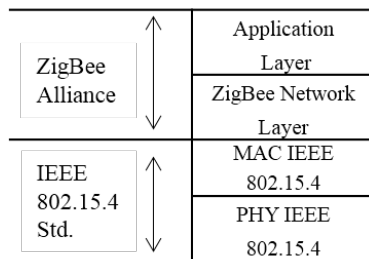


Fig. 4. ZigBee Layered Architecture

networks that are forming the clusters. The cluster trees are similar to stars, though RFD devices are only allowed to connect at the outermost branches. The diagram shows that the FFD connects to the coordinator and a FFD can have connections to multiple end devices [14].

4. FRAME FORMAT AND OTHER TECHNOLOGIES

As depicted, for the overall structure the maximum frame size is 127 octets, 127 bytes, the maximum frame header is 25 octets. The frame control field is expanded out where in the frame control field there is a frame type and various fields. Among these fields, the security enabled field is important. In addition there are, Intra PAN Field, app request, frame pending, destination address mode, and source address mode, and other reserved fields. Now, going back to the general frame format above the frame control field, there is a sequence number and there is a destination PAN identifier, and also there is a source PAN identifier field. Next, the frame contains des-

tinuation address, source address, and this is where the frame payload goes in, and that is a variable field. At the end, for protection, due to errors, there is a frame check sequence. This IEEE 802.15.4 standard frame format is used by ZigBee and 6LoWPAN devices at the lower layers [5].

4.1 ZigBee

This is supported by the ZigBee alliance and ZigBee adds on the upper layers which are the application layer and the ZigBee network layer, on top of the medium access control and physical layer that are established in the IEEE.802.15.4 protocol. ZigBee provides different type of service operations to the upper layers. ZigBee works well in isolated network environments. In other words, if it is an isolated network, ZigBee can be used to form an IoT or a wireless sensor network connection [9, 10]. ZigBee network topology include star, mesh, cluster tree, where the star network is the basic common topology that is formed. Mesh or P2P networks can provide high reliability because they can support multiple routes between nodes. Then there is the cluster tree network which is a combination of star and P2P topologies [4] as ZigBee network topologies are dependent upon the network connectivity that are provided by the IEEE 802.15.4 protocol.

4.2 6LoWPAN

6LoWPAN stands for IPV6 over low power wireless personal area network. It supports IPV6 packets over the IEEE 802.15.4 wireless personal area network. It enables IPV6 IoT wireless network support based upon low power design aspects for good battery operated IoT devices. This means that it is good for battery operated IoT devices. It means that typically, the low power consumption is going to be used to extend the battery life. 6LoWPAN is an Internet

Engineering Task Force (IETF) standard. It is one of the two task forces, the IETF and the IREF. They belong to the Internet architecture board under the United Nations. It uses, the 6LoWPAN standard the IEEE 802.15.4 wireless PAN technology for its two basic layer operations. 6LoWPAN provides wireless PAN direct connection to IPv6 Internet, which is very beneficial and efficient. IPv6 features can be used to support wireless personal networks [6, 7, 8]. Features of IPv6 like security, naming, addressing, translation, lookup, and discovery function are very helpful and can be utilized effectively.

4.3 Characteristics of 6LoWPAN

The small packet size that supports the 16 bit short and the IEEE 64-bit extended Medium Access Control addresses are typically used in 6LoWPAN packets. Also, low data rates of 20, 40, or 250 kbps are the major domain of the data rates. Network topology-wise, Star and Mesh topologies are supported as we are using the 802.15.4 standards and, it is good for low power battery operated nodes. Moreover, relatively low cost devices can be developed from this technology. Header compression also needs to be considered as 6LoWPAN packets and IPv6 packets, are of different sizes. Hence, packet sizes needs to be matched. IPv6 minimum packet size is 1,280 octets. The IEEE 802.15.4 has an MTU of a maximum transmission unit, which has the maximum packet size of only 127 octets and there is a big mismatch of the packet sizes. On the other hand, IPv6 header is a 40 octet minimum length with no option extension fields added. Still it is 40 octets, and that is too big to send over an IEEE 802.15.4 packet because among the 127 octets, that itself is going to occupy too much space. Therefore 6LoWPAN provides header compression technology. It is described in more detail in following sections of the paper.

Compression of the IP address is possible because it can be derived from other header field information. Also, the prefix part for link local addresses can be compressed [11, 12]. It is also possible to totally omit the 128 bit IPv6 address field when it can be provided from the link layer address information. In addition, it is possible to compress other common header fields like the TCP, UDP and ICMP header. It is possible to save a lot of the header information using this technique. It can be kept and used in the operation, but not transmitted over the wireless personal area network every time a packet is transmitted [13].

5. RESEARCH CHALLENGES

With couple of devices in lab, it is fairly easy to utilize IoT network connectivity. Connectivity is low latent and seamless with only few devices and server running in backend. Development of IoT network for millions of simultaneous users at a global scale is challenging. Moreover, IoT is not just a network of homogeneous devices as described in sections above therefore heterogeneity has to be taken care. Inclusion of firewalls, fast connectivity, cell towers, and proxy servers and so on must be considered while designing IoT networks. Following are the major research areas and challenges that needs to be focused in IoT:

—*Signalling*: Stream of data should reach from source A to destination B so reliable bidirectional signalling is essential.

—*Security*: When sending and receiving stream of data needs authorization, listening to open ports out to internet should be forbidden, end to end Encryption for data being sent.

—*Presence Detection*: It is important to identify whether the device is on or off?

—*Power Consumption*: Exhaustive research is required to reduce power consumption while exchanging data between devices.

—*Bandwidth*: For IoT device communication spending bandwidth of cellular network is expensive.

6. CONCLUSION

IoT Networks can be integrated with low energy networks like ZigBee and 6LoWPAN and Bluetooth in order to minimize the power consumption and develop energy efficient IoT Networks. Also, there are topologies like star, mesh-p2p and cluster tree that can be used for implementation of IoT in real world scenario with devices that are supporting low power communication technologies like ZigBee and 6LoWPAN. By year 2020, it is forecasted that 20 to 30 million devices would be connected so emphasis on how these devices would be connected and IoT network will play a vital role in this area.

7. REFERENCES

- [1] J. Bradley, J. Barbier, and D. Handler, "Embracing the Internet of Everything To Capture Your Share of \$14.4 Trillion," Cisco, White Paper, 2013.
- [2] J. Bradley, C. Reberger, A. Dixit, and V. Gupta, "Internet of Everything: A \$4.6 Trillion Public-Sector Opportunity," Cisco, White Paper, 2013.
- [3] D. Evans, "The Internet of Everything," Cisco IBSG, White Paper, 2012.
- [4] S. Mitchell, N. Villa, M. Stewart-Weeks, and A. Lange, "The Internet of Everything for Cities," Cisco, White Paper, 2013.
- [5] O. Hersent, D. Boswarthick, and O. Elloumi, "The Internet of Things.. Key Applications and Protocols. John Wiley & Sons, Dec. 2011.
- [6] "Machine 2 Machine Perspective on Industry Status (Key Challenges and Opportunities)," Frost & Sullivan, Research Paper, Nov. 2011.
- [7] "M2M Sector Map," Beecham Research, Sep. 2011. [Online] Available from: <http://www.beechamresearch.com/download.aspx?id=18> [Accessed June 1, 2015]
- [8] F. Behmann and K. Wu, "Collaborative Internet of Things (C-IoT). John Wiley & Sons, 2015.
- [9] J. Gubbia, R. Buyyab, S. Marusica, and M. Palaniswamia, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, Sep. 2013.
- [10] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805, Oct 2010.
- [11] S. Li, L. D. Xu, and S. Zhao, "The Internet of Things: A Survey," Information Systems Frontiers, vol. 17, no. 2, pp. 243-259, Apr. 2015.
- [12] A. J. Jara, L. Ladid, and A. Skarmeta, "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 4, no. 3, pp. 97- 118, 2013.
- [13] O. Vermesan and P. Friess, "Internet of Things - Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT. River Publishers, 2011.

- [14] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, and P. Doody, "Internet of Things Strategic Research Roadmap," European Research Cluster on the Internet of Things, Sep. 2011.
- [15] IEEE Std. 802.15.4-2006, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE, Sep. 2006.
- [16] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," IETF RFC 4919, Aug. 2007.
- [17] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF RFC 4944, Sep. 2007.
- [18] ZigBee Alliance, "ZigBee specification: ZigBee document 053474r13 Version 1.1." Dec. 2006.
- [19] ZigBee Alliance, www.zigbee.org
- [20] Chaudhary, S., Desai, A. and Parmar, J.K., 2012. Internet of Things: Architecture and Research Challenges. CSI Communications, p.21.