IETE Technical Review

ISSN: 0256-4602 (Print) 0974-5971 (Online) Journal homepage: http://www.tandfonline.com/loi/titr20

Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges

Bhagya Nathali Silva, Murad Khan & Kijun Han

To cite this article: Bhagya Nathali Silva, Murad Khan & Kijun Han (2017): Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges, IETE Technical Review, DOI: 10.1080/02564602.2016.1276416

To link to this article: http://dx.doi.org/10.1080/02564602.2016.1276416

IETE TECHNICAL REVIEW, 2017
http://dx.doi.org/10.1080/02564602.2016.1276416

Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges

Bhagya Nathali Silva, Murad Khan and Kijun Han

School of Computer Science and Engineering, Kyungpook National University, Daegu, Korea

ABSTRACT
Internet of Things (IoT) has become a continuously growing concept with the advancements of ubiquitous computing, wireless sensor networks, and machine-to-machine (M2M) communication. IoT connects heterogeneous physical devices and enables communication among them over the Internet via uniquely addressable identifiers. This paper delivers an overview of IoT in the context of the architecture and related technologies. However, IoT does not adhere to a universal architecture. Hence, it describes widely accepted architectural designs, further elaborated with the corresponding communication protocols and standards. Moreover, highly prevalent protocols and standards are summarized, so that the reader can gain an overall view of IoT. Furthermore, it describes some identified solutions and future directions towards overcoming the challenges present in the IoT paradigm. Finally, the paper concludes with some applications of IoT, in order to realize the feasibility of IoT concept in real-world scenarios.

KEYWORDS
Heterogeneous devices; IoT; Ubiquitous computing; Wireless sensor network

1. INTRODUCTION

Internet of Things (IoT) has become a buzzword in the modern era of wireless telecommunication. Since it is an emerging area of interest, further investigation in all corresponding concepts and factors would be beneficial for the evolution of IoT notion. The fundamental idea of IoT is to enable ubiquitous computing with the use of uniquely addressable devices to identify information and to enhance the information exchange without or less human interaction [1]. This concept is facilitated by smart objects, which are produced by embedding electronic components into regular objects, such as mobile devices and home appliances. The connected devices make them recognizable in the network and they become capable of contextual decision-making as they share their information, while accessing information generated by other connected devices [2]. In fact, connectivity with existing networks and proactive operation based on different factors (context-aware computation) are mandatory in IoT. The conventional explanation of the Internet has been changed into an innovative notion, since it has become the backbone of many interconnected typical networks and network of smart objects for information sharing and circulation [3].

In terms of the research community, the major disadvantage to the advancement of IoT can be considered as scattered interest of scholars, which leads to working on the specific domain rather than considering the holistic development of IoT. Thus, it degrades the holistic development of the notion, while hindering the realization of IoT in physical world [4]. Many research works have been conducted in the field of IoT, under varied interests. Atzori et al. have conducted a survey on IoT, with the aim of elaborating main communication technologies [4]. A cloud-centric architecture for IoT applications and enabling technologies were taken into account by Gubbi et al. in their findings on IoT [1]. Similarly, Gluhak et al. stated the challenges to bridge the gap between research and real-world aspects [5]. Moreover, many open challenges have been identified by various researchers in terms of security of information exchange within IoT [5]. In addition, enabling a complex sensing environment, power supply, multiple connectivity options, privacy, evolving architecture, and the complexity of IoT itself has been identified as other confronted challenges [6]. The unique addressing of objects, storing and representing the exchanged information has become a huge challenge in IoT [4]. Apart from the technical difficulties, the adoption of the IoT paradigm is obstructed by lack of a clear and widely accepted business model that can attract investments to promote the deployment of these technologies [7].

The above-mentioned challenges can be overcome up to a certain extent, with the aid of a variety of wireless and wired connectivity options, such as Bluetooth, WIFI, Radio Frequency Identification (RFID) and Near-Field

Communication (NFC). In order to support mesh networks and to attain a wider coverage, the existing WIFI networks should be modified accordingly [8]. Furthermore, the emphasis on communication pathway of IoT is essential to understand the information exchange within IoT. It uses various standards, protocols and techniques to distribute information. Aforementioned connectivity options are categorized into three broad types considering the geographical area coverage, i.e. Wide Area Network (WAN), Local Area Network (LAN) and Personal Area Network (PAN) [9]. Figure 1 depicts the categorization concisely. In order to facilitate information sharing within the IoT, it is essential to support device-to-device (D2D) communication, interaction between devices and the server architecture (D2S), and share device data among server architecture (S2S) [10].

Multiple protocols and standards are involved with IoT communication. Among them, Internet Protocol version 6 (IPv6), Internet Protocol version 4 (IPv4), IPv6 over Low power Wireless Personal Area Network (6LoWPAN), Constrained Application Protocol (CoAP), Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) take a higher priority. However, constrained device developers have stated UDP is advantageous and cost-effective, due to its smaller size and performance [11]. An attempt was made to propose a model, which arranges these protocols into constrained and unconstrained stacks according to the TCP/IP network layer architecture. The unconstrained stack contains common standards Extensible Markup Language (XML), Hypertext Transfer Protocol (HTTP), and IPv4, whereas the constrained stack holds protocols with similar functionality but replaced with those in which the complexity is significantly reduced, i.e. Efficient XML Interchange (EXI), CoAP, and 6LoWPAN [7]. IoT has been rapidly developed and deployed in the real life with the enormous contribution from the research centres and companies [12]. The IEEE 802.3, IEEE 802.11 and IEEE 802.15.4 are the most common standards related to IoT [11]. Moreover, the Internet Engineering Task Force (IETF) protocol suite has a vital contribution towards IoT, and it has been evaluated by Sheng et al. to determine the challenges for IoT [13].

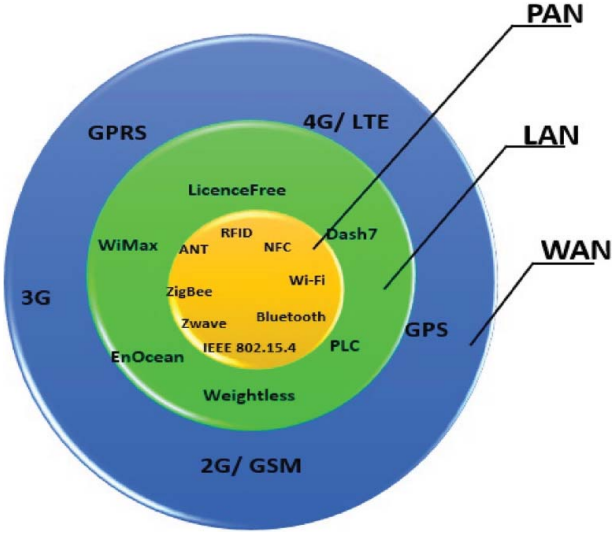

Figure 1: IoT communication technologies

2. IoT ARCHITECTURE

IoT has been introduced as the third wave of the web after static pages web (WWW) and social networking web. It is the worldwide network, which connects disparate types of objects anytime anywhere through the IP. Scalability, interoperability, data storages reliability, and quality of service (QoS) are the key areas to be considered, when defining an architecture for IoT [14]. In order to attain these key features, multiple interest groups have attempted to define a universal architecture for IoT.

Among many proposed architectures, the conventional IoT architecture has been divided into three layers, i.e. perception layer, network layer, and application layer [15]. The perception layer is acting as the bottom layer of the architecture, which is responsible to extract information from things and to transform it into a digital format. Subsequently, the network layer transports the digital signals via the network, while the application layer is liable for the application of transferred digital signals into different contexts [16].

2.1 Perception Layer

As the initial phase of IoT, the perception layer collects data from environment, i.e. temperature, humidity, etc. as well as from heterogeneous devices and objects. Wireless Sensor Networks (WSN – consists with large number of small and resource-constrained sensors) plays a major role in collecting and processing various types of data in the perception layer [17]. These sensors and other real-world objects in IoT, i.e. actuators, cameras GPS terminals, etc. communicate with each other using ZigBee, Wifi and many other protocols specialized for short-range communication. The inner most circle of Figure 1 depicts widely used short-range communication technologies. IoT is an extensively broad network, connecting heterogeneous devices. Therefore, it is essential to identify and address each object, device or thing uniquely. In order, RFID, NFC, and Bluetooth are used

as identification technologies in addition to the communication. Moreover, recent endeavours on 6LoWPAN have facilitated these devices to be addressed uniquely within the network and seamlessly integrate to the network without any extra hassel [14].

2.2 Network Layer

The network layer is considered to be the brain of the IoT architecture. It facilitates secure data transmission between the perception layer and the application layer. The network layer delivers information collected at the perception layer to multiple applications and servers. In fact, the network layer is a convergence of communication networks and Internet. Numerous studies performed on communication technologies and Internet make the network layer to be the most developed layer of the IoT architecture. Data processing takes place at the network layer as a result of IoT management and data centre. Hence, the "core layer" of IoT – the network layer improves the ability of information operation. Moreover, unique addressing and routing ability ensure seamless integration of innumerable devices into a single collaborative network, realizing the universality of the IoT notion. Wired, wireless and satellite technologies have contributed immensely towards this phenomenon, i.e. Wi-Fi, Bluetooth, xDSL, PLC, etc. Simultaneously, a great effort has been invested by IETF for the implementation of 6LoWPAN protocol, to forward IPv6 traffic in IoT architecture assuring unique addressing of each connected device within the network.

2.3 Application Layer

Application layer is the most top layer of the IoT architecture, which bridges the gap between the applications and the users. The application layer is the IoT technology combined with industry expertise to achieve a broad set of intelligent application solutions [15]. For example, it integrates IoT system functions to build practical applications, such as the ecological environment and natural disaster monitoring, intelligent transportation, building health monitoring for heritage conservation and cultural dissemination, fortune medical and health monitoring [18]. Most importantly, the application layer handles the global management of IoT applications [14]. Indeed, application layer conforms to specific standards and protocols as shown in Figure 2. According to the survey conducted [19], IETF's CoAP has been identified as the only protocol that runs over UDP, thus making it the most lightweight, followed by HTML 5s Websocket that significantly reduces the communications overhead.

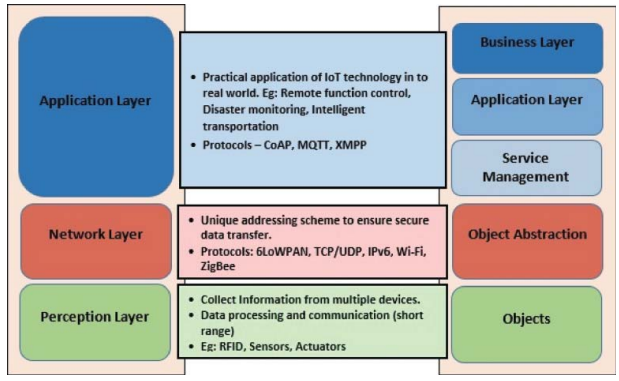

Figure 2: The IoT architecture

However, in recent literature, authors have discussed a five-layer architecture, in order to facilitate more generalization [4,15,16]. Multiple attempts were made to define the five-layer architecture focusing on numerous aspects. However, the majority can be outlined into objects, object abstraction, service management, application layer and business layer as shown in Figure 2 [20].

The object layer is responsible for the collection of data from heterogeneous devices. Furthermore, it processes and digitizes collected data. Consequently, it transfers the processed data to the upper layers [21]. This layer is replicating the services of perception layer in three-layer architecture. The object abstraction layer is mediating between the objects layer and service management layer using communication technologies such as RFID, 3G, and WIFI [21]. The network layer functionalities are handled by the object abstraction layer. The service management is in charge of pairing the requestor with the requested applications while facilitating information processing and decision-making [22]. The application layer provides high-quality smart services as per request by the customers [21,22]. The business layer is the topmost layer which constitutes a business model and graphical representations according to received data from the application layer. In the three-layer architecture, the application layer represents the responsibilities of service management layer, application layer, and business layer of the five-layer architecture as shown in Figure 2.

3. IoT ENTITIES

The realization of IoT relies on the required components. According to the high-level functionalities, these components are categorized into hardware, middleware and presentation. However, few more taxonomies are available for the categorization of IoT components. In this section, the components are categorized in line with the components' contribution towards IoT, i.e. data

acquisition, communication, computation, services and visualization.

3.1 Data Acquisition

It is essential for IoT to gather differed types of data from various types of devices, objects, etc., in order to share them among other devices and applications of IoT. This is facilitated by many technologies, i.e. RFIDs, sensors, barcodes, GPS terminals, cameras, actuators, etc. However, among these, RFID and sensors are widespread due to its advantages over the other data collection modes. In general, the information sharing among heterogeneous devices within the IoT environment is facilitated via short-range communication modes. Table 1 summarizes widely used short-range communication technologies.

RFID is a technology that incorporates a radio frequency (RF) portion of the electromagnetic spectrum to identify uniquely an object, animal, or person [31]. RFID technology is similar to barcode reading, even though the performance is efficient than barcodes. RFID consists with a transceiver, antenna, and the transponder. The antenna transmits a RF signal to activate the transponder. Then, the activated tag sends back the data to the antenna. These data trigger the programmable logical controller to perform a particular action. RFID tags are advantageous than barcodes, since it is readable from a considerable distance, rewritable, efficient, and rugged [27]. However, RFID can be disadvantageous due to the reader and tag collision, which is a common technical issue [26]. On the other hand, sensors are experiencing a renaissance as microelectromechanical systems (MEMS) technology becomes less expensive and further miniaturized [28]. Many IoT devices consist of sensors to identify changes and behaviour of temperature, humidity, pressure, motion, etc. However, to perform a specific task, these sensors are paired with an application via hardwired programming.

Table 1: Common short-range communication technologies [23–30]

Technology	Range	Identify	Com. Mode	Applications
RFID	3–10 m	✓	One-way	Indoor continuous moving navigation Smart parking Battery less remote control
NFC	≤10 cm	✘	Two-way	Smartphones Parking meter E-ticket booking
Bluetooth	Up to 100 m	✘	Two-way	Home automation Communication with peripherals

NFC is a set of communication protocols used to communicate between two devices within the range of 10 cm [29]. In general, one device is portable for the purpose of getting the appropriate proximity. Full NFC-enabled device can read information stored in passive NFC tags, exchange information between two NFC-enabled devices and act as a smart card to perform transactions. Thus, it can be stated that NFC acts as an identification and communication technology [32]. Bluetooth is a technology that uses short wavelength radio signals to communicate among devices in a narrow proximity while reducing the power consumption [30]. Bluetooth works according to the master–slave architecture, and is primarily designed for low power consumption. The communication range varies with the propagation conditions, antenna configuration, battery conditions, etc.

3.2 Communication

Subsequently, gathered data will be transferred via the network, to be consumed and processed by the applications. Accessing the network was facilitated by the backbone developed using a variety of communication technologies [33]. Bluetooth, RFID, NFC, Ethernet, xDSL, WIFI, WiMax, PLC (power line communication) and cellular networks are playing a major role in accessing the network. Among these, Ethernet and xDSL are wired communication modes, which are capable of transmitting data at a higher rate. However, the superiority within the communication paradigm is acquired by wireless technologies such as WIFI, WiMax, and cellular networks, due to their higher flexibility [17].

WIFI uses radio waves to communicate among devices according to the collection of IEEE 802.11 standard [34]. RFID, NFC, and Bluetooth contribute as short-range communication modes, which are widely used to retrieve environmental data from physical devices. PLC is another important technology, which enables network access via the electrical power system. This is advantageous over other wired mechanisms due to the cost-effectiveness. However, it is affected from coexistence interference, since it operates on 2.4 GHz frequency band with other technologies, i.e. Bluetooth and ZigBee [35]. Table 2 Illustrates a brief summary related to common communication technologies in use.

3.3 Computation

IoT is connecting a variety of data sources, which generates an enormous amount of data. IoT is considered to be a computational grid, as it consists with a number of devices and software applications that are capable of

Table 2: IoT communication technologies

Tech.	Medium	Max coverage	Limitations
WIFI	Wireless	Up to 100 m	Interference with WIFI communications
Ethernet	Copper cables	Up to 50–70 km	Physical medium
Wimax	Wireless	Up to 50–70 km	Low data rate in the real world Sensitivity to weather conditions
Cellular	Wireless	10 m to 100 km	Restricted wireless spectrum
xDSL	Twisted pair, copper cable	1.3 km	Asymmetric communication
PLC	Electrical power system	1500 in premises 100 m between devices	Mutual interference with other technologies

processing those data [36]. Various hardware components and platforms, i.e. Panstamp, Arduino, XinoRF, Raspberry PI, Beaglebone Black, UDOO, etc. host these IoT applications [37]. In addition, operating systems such as RTOS, TinyOS, LiteOS, and RiotOS are vital software platforms, which are used to utilize the IoT functionalities [38–40]. In order to enhance the efficiency of the computation power, an architecture has been proposed to get full advantage of proximal devices in [38]. IoT computation and analytics immensely vary across a wide range from agriculture to health care. Moreover, several computational areas are identified by the researchers to enhance the working capabilities of the IoT communications [36].

3.4 Services

IoT services are categorized into four major sections, i.e. (1) identity-related services, (2) information aggregation services, (3) collaborative-aware services, and (4) ubiquitous services [41,42]. The identity-related services can be either active or passive. In general, the identity services have two major components namely identifier and read device. The reading device reads the identifier and request for more details of the encoded device information from the name resolution server [42]. Meanwhile, the information aggregation acquires data from various sensors, process, transmit and report the data to the application via IoT [41]. As the next stage, collaborative-aware services use aggregated information for decision-making, followed by an action corresponding to the decision made. Ubiquitous, as the name implies provides collaborative services to anyone, anywhere during any time [42]. The ubiquitous network is a fully connected, reliable, and an intelligent network, which contains integrated content technology, microtechnology, and biotechnology [41].

3.5 Visualization

In IoT, many applications emphasize on acquiring data, to apply computations and visualize later [43]. Visualization is vital in IoT applications, since it provides interaction with environment and users. Moreover, it holds both event detection and visualization of the raw and modelled data according to the user preference [1].

4. IoT STANDARDS

TCP/IP was considered to be promising for realizing IoT, since it is the baseline standard for computer networking. However, the usability of IPv6 was restricted due to the low power and low bandwidth. Hence, many interest groups have laid their effort to define standards for IoT, in order to support and to simplify IoT application development. World Wide Web Consortium (W3C), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), and EPCglobal have given the major contribution towards IoT Standards. An overview of few common standards is presented in this section.

The IEEE 802.15 PAN working group has extended their contribution towards IEEE 802.15.4, which is dedicated for low power, low data rate, low cost and short-range communications [44,45]. Consequently, a larger percentage of mobile devices were developed to be compliant with IEEE 802.15.4 [13]. The standard allows 1280 bytes of maximum transmission unit (MTU) size for IPv6 packets. However, the physical layer has a maximum frame size of 127 bytes, which is further restricted by 25 bytes of maximum frame overhead. Hence, IPv6 packets cannot be fit into IEEE 802.15.4 packets [46]. Due to this fact, usable space for upper layer protocols is restricted for 86–116 bytes. Although it ensures fully handshake protocol for data reliability, it reaches only up to the maximum of 250 kb/s in 2.4 GHz, resulting in reduced scalability and inefficient traffic load balancing [13,47]. IEEE 802.15.4 specifies both physical (PHY) and media access control (MAC) layers, with permission of altering according to the application requirement. However, in multi-hop settings, the reliability of this protocol becomes unpredictable, due to the single-channel nature of the MAC protocol. Unavailability of a built-in frequency hopping technique leads IEEE 802.15.4 MAC layer prone to failure, due to interference and multi-path fading. Therefore, the MAC protocol of IEEE 802.15.4 has been enhanced to utilize time slotted access, multi-channel communication, and channel hopping via Time Synchronized Channel Hopping (TSCH) in IEEE 802.15.4e. Consequently, IEEE 802.15.4e MAC layer mitigates the adverse effects interference, and multi-path fading, while improving the reliability issues that existed in the MAC layer of IEEE 802.15.4 [48].

Table 3: Standards related to IoT [55,56]

Standard	Implemented by	Accessing layers	Influential protocols	Features
IEEE 802.15.4	IEEE	PHY and MAC layers	IEEE 802.15	■ Low power data transfer ■ Low data rate ■ Low cost
IEEE 802.15.4E	IEEE	PHY and MAC layers	IEEE 802.15.4	■ Modification in MAC layer of IEEE 802.15.4 ■ High reliability in multi-hop settings
ZigBee	ZigBee Alliance	Upper layers (Network, Transport, Application)	IEEE 802.15.4	■ Built on PHY and MAC layers of IEEE 802.15.4 ■ Self-forming ■ Self-healing
6LoWPAN	IETF	Network layer	IPv6	■ Carry IPv6 datagrams on IEEE 802.15.4 ■ Neighbour discovery in overlapping broadcast domain
RPL	IETF	Transport layer	IPv6 6LoWPAN	■ Maintain routing topology ■ Update routing information

ZigBee is another important standard for IoT applications. It is a property of the ZigBee Alliance, which is a group of companies joined to create and promote the new standard. ZigBee shows similarity to IEEE 802.15.4 as it is self-forming, self-healing, and supports star and mesh topologies [49]. It defines upper layers of the architecture on top of PHY and MAC layers of IEEE 802.15.4 standard. The ZigBee standard is tailor-made for monitoring and control applications. Thus, it suits for applications such as building automation, personal health care, industrial control, and lighting and commercial control.

IETF has contributed the IoT evolution with 6LoWPAN standard, established based on IPv6. It indicates IPv6 over low-power wireless personal area network (IEEE 802.15.4). IPv6 was considered to be the base model for 6LoWPAN, due to its extensibility, universality, and stability [13]. 6LoWPAN working group of IETF was focused to overcome the drawbacks in IPv6 datagrams while transmitting over a low-power WPAN. The considerations were how to carry IPv6 datagrams in 802.15.4 frames (due to the huge mismatch between MTU of IPv6 and IEEE 802.15.4 as mentioned before) and how to perform necessary IPv6 neighbour discovery functions (e.g., address resolution, duplicate address detection) in a network with overlapping broadcast domains [50]. 6LoWPAN has three primary elements, namely header compression, fragmentation and layer-two forwarding [51].

Routing is a challenging task for 6LoWPAN due to many reasons. They can be identified as low-power lossy networks (LLN), battery-powered nodes, and frequently changing mesh topologies resulting from mobility [52]. IETF proposed a Routing Protocol for LLN (RPL), considering IPv6 behaviour and 6LoWPAN mechanism. It supports to build a robust topology in a lossy network, with minimal routing requirements [20]. The building block of RPL is a Destination-Oriented Directed Acyclic Graph (DODAG). In a converged LLN, each router has identified stable set of parents, which could be the next hop on the path towards the root [53]. RPL has separated packet processing and forwarding from the routing optimization, in order to be used by a variety of application domains [54]. These standards are summarized in Table 3.

5. COMMUNICATION PROTOCOLS

IoT supports multiple communication protocols, which are either open or proprietary. Some of the protocols were readily available and others were specifically implemented with the purpose of extending IoT capabilities. According to [20], IoT communication protocols can be classified into four major categories, as to application protocols, service discovery protocols, infrastructure protocols, and other influential protocols. An overview corresponding to application protocols, infrastructure protocols, and service discovery protocols will be discussed later in the next section. Moreover, Figure 3 gives a summarized view of the IoT communication protocol stack.

5.1 Application Protocols

The application layer is at the top of the architecture, bridging the IoT application and the underlying

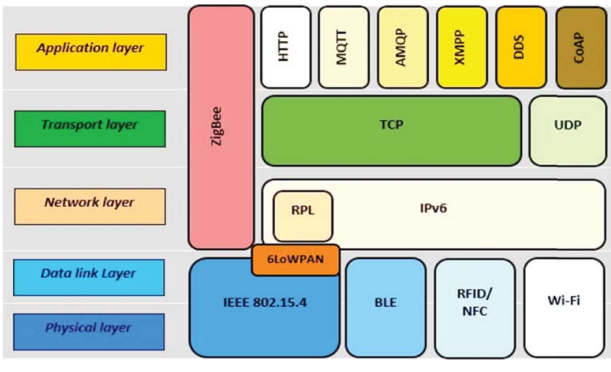

Figure 3: IoT communication protocols stack

platform. There are many communication protocols defined for the application layer. CoAP, MQTT, XMPP, HTTP-REST, and DDS are some of the common protocols. The following paragraphs give a brief description about CoAP and MQTT application layer protocols.

CoAP is a stateless protocol developed by IETF for IoT applications. CoAP is Representational State Transfer (REST)-based protocol; therefore, CoAP-REST proxy translation can be done directly [20]. It was defined by means of replacing HTTP for lightweight and resource-constrained devices [57]. In order, slight modifications were made in HTTP to enable low power consumption. Since it is bound to UDP, it reduces TCP overhead and reduces bandwidth requirements, thus making it an excellent fit for IoT communication [19].

UDP does not provide reliability, CoAP has defined four types of messages, namely confirmable (CON), non-confirmable (NON), reset (RST) and acknowledgement (ACK). The reliability is gained by a combination of confirmable and non-confirmable messages, together with datagram transport layer security (DTLS). The reliable transmission process of CoAP sends CON message with a message ID and it is retransmitted to the receiver until the sender receives an ACK message with the same ID. At the failure of processing CON message at the receiver end, it sends RST message instead of ACK. Non-confirmable messages are sent, whenever reliable transmission is not enforced for the message [58].

MQTT (Message Queue Telemetry Transport) was introduced by IBM, aiming to connect embedded devices and networks with applications and middleware. It uses TCP as the transport layer protocol. The lightweight broker-based nature of MQTT makes it simple and easy to implement [59]. MQTT is appropriate for constrained devices connected to a low bandwidth or unreliable network. MQTT consists with a subscriber, broker, and a publisher. In order to become a subscriber, a device needs to be registered for a specific topic. Then, the publisher generates information and transmits information to subscribers via brokers. MQTT determines the Quality of Service (QoS) depending on the message delivery reliability. It assigns QoS value from the pre-defined three levels [60].

5.2 Infrastructure Protocols

Infrastructure layer can be further categorized into physical layer, link layer, network layer, and routing layer. Specific protocols have defined for each of these layers. These infrastructure layers can be mapped into the layers of IoT architecture previously mentioned in Section 2. The physical and link layer protocols are operating on the perception layer of IoT. Meanwhile, the network and routing layer protocols functioning on the network layer of the generic IoT architecture. The layer hierarchy is shown in Figure 3.

RPL is an infrastructure communication protocol, which is functioning in the routing layer. IETF quickly recognized the need for an IPv6-based lightweight routing protocol for IP smart object networks. The ROLL working group of IETF then came up with the RPL specification. RPL is a distance vector protocol, which describes on building a DODAG [61]. Similarly, it uses four types of control messages. The first type of message is DODAG Information Object (DIO) messages which indicate the rank of the device after considering calculations and matrices. The DIO rank is helpful to find the preferred parent path, where device rank is higher than the potential parent ranks. The Destination Advertisement Object (DAO) messages are used to support upward and downward traffic to a specific parent. The DODAG Information Solicitation (DIS) messages are used to acquire DIOs from nodes in proximity. The last message type is DAO Acknowledgement (DAO-ACK), generated as a response to DAO message [53]. There are two modes of operation (MOP) in RPL, storing and non-storing modes. The *non-storing* mode directs downward traffic using source routing while in the *storing* mode messages are directed based on destination IP address [53].

6LoWPAN is another protocol developed by IETF, which is operating in the network layer of the infrastructure. Since 6LoWPAN was built taking IPv6 as the base, it facilitates interoperability with other IP networks, as well as with other wireless devices on IEEE 802.15.4. 6LoWPAN allows each constrained device to be accessed uniquely within the network, making the administration tasks easier. Moreover, it is responsible for fragmenting and reordering of IPv6 packets, compressing protocol stack headers, enabling stateless addressing, providing a basis for "mesh-under" routing and assuring consistency with the upper layers [62]. In IP routing over 6LoWPAN, additional header information is not a mandatory field, so that it reduces unnecessary packet overhead while saving more space for data to be transferred [63]. Moreover, 6LoWPAN has a mesh address header to support routing of packets in a mesh network, but leaves the details of routing to the link layer [64]. 6LoWPAN header is identified by the type field represented in the first two bits of the header. There are four types of headers defined for 6LoWPAN communications, i.e. (1) If

the packet is not for 6LoWPAN processing, the header is set to *No 6LoWPAN (00)*; (2) If the header is set as *Dispatch (01)*, it indicates that the packet is ready for IPv6 header compression; (3) The *Mesh-Addressing (10)* header-type forward IEEE 802.15.4 frames to the link layer as required, to create multi-hop networks; and (4) *Fragmentation (11)* header is used if the packet size exceeds IEEE 802.15.4 frame size [65].

The IEEE 802.15.4 defines 16 channels between 2.4 and 2.48 GHz, where each channel is 2 MHz wide and separated by 5 MHz from each other. The rationale is to ensure that channels will not get interfere with one another [52]. This protocol is capable of supporting star and mesh topologies [47]. The devices of IEEE 802.15.4 can be of two types, i.e. (1) *Full functional devices* (FFD) and (2) *Restricted functional devices* (RFD). The FFDs are capable of creating, maintaining and coordinating the network (PAN Coordinator) and can communicate with any other device in the network. However, the RFDs are devices with limited resources, and allowed to communicate only with the coordinator. However, IEEE 802.15.4 comes across reliability issues of the MAC layer as mentioned in Section 4.

In order to overcome the drawbacks of IEEE 802.15.4, the IETF has made modifications in the MAC layer and released it as IEEE 802.15.4e. This protocol defines how the MAC layer executes a schedule. The schedule execution can be either *Centralized* or *Distributed*. In the centralized approach, the schedule is created by a manager node. Similarly, the connected nodes periodically inform the manager about the other nodes, which are generating data. Then manager creates the schedule considering received information. In fact, centralized scheduling is very efficient, since the manager is aware of the activities of the whole network. In the distributed scheduling, nodes locally determine the schedule with adjacent nodes, and scheduling a link for each neighbour would be the easiest mechanism. However, the distributed scheduling is applicable for highly dynamical networks, i.e. networks with mobile nodes, networks with many gateway nodes [48].

In order to be active for a longer duration, the Bluetooth Low Energy (BLE) was introduced, which operates over a short-range radio with lower power characteristics. The BLE is a promising technology in IoT, due to its ultra-low power consumption and lower latency compared to the classical Bluetooth. The BLE uses a client-and-server model where a client connects and accesses one or several servers. In this scenario, the data generators such as sensors and actuators act as the servers, while laptops, smartphones, and other application devices act as the clients. In order to achieve low power consumption, it keeps the radio turned off during idle periods. Similarly, it turned on the radio to send or receive smaller data packets.

5.3 Service Discovery Protocols

Service discovery protocols are essential to have a proper mechanism to register and discover devices and services dynamically and efficiently. Multicast Domain Name System (mDNS) and DNS Service Discovery (DNS-SD) are the prominent protocols with this regard. However, these protocols should be modified accordingly, in order to use with the resource-constrained devices in IoT.

mDNS is used to resolve records in local network without a central DNS server [66]. mDNS packets show an extreme similarity of 99% to the DNS packet format. mDNS is fitting for smart devices on IoT as it does not need manual configuration, capable of running without infrastructure and has ability to continue to work at a failure of infrastructure. mDNS sends IP multicast message to all nodes in the domain requesting for a reply from the node that has the mentioned name. As shown in Figure 4, the corresponding node replies to all the other nodes in the domain including the requestor, so that all other nodes update the local cache with the given name and the responded IP address.

DNS-SD is used to discover services on a network. This protocol is compatible with mDNS, but independent from it. DNS-SD facilitates zeroconf networking (point-to-point communication without external configurations). DNS-SD does not require external administration or configuration to connect new machines. The service discovery is achieved in two steps: (1) Discover host names of the requested service, and (2) IP pairing corresponding to the host names.

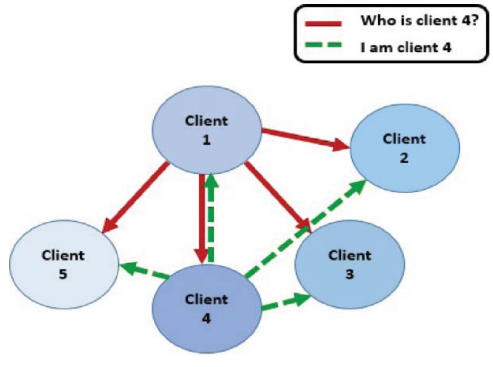

Figure 4: mDNS protocol request and response scenario

6. IoT CHALLENGES AND FUTURE DIRECTIONS

Even though IoT is widely accepted and practically in use, there are many areas to be considered for further improvement. This section describes a few IoT challenges and future directions.

Among IoT challenges, availability, performance, security, reliability, scalability, interoperability, and mobility can be identified as major challenges.

IoT is defined with means of facilitating information anytime, anywhere to any person who requests for it [14]. Thus, availability is highly critical for IoT realization. In order to achieve high availability, the IoT network needs to ensure high availability of physical devices as well as IoT applications, which connects the user to IoT. Redundant maintenance of vital hardware devices and programs is a feasible solution to this issue. So that, at a failure, the redundant device or the program can be used to perform load balancing [67]. Even though redundancy increases complexity, there are situations where simplicity is compromised to achieve availability. Thus, redundant hardware components can be a feasible solution to achieve availability. In [67], two redundancy models are proposed. The passive redundancy model performed better compared to the active redundancy model. Moreover, in the passive model, spare components are activated only when the primary component fails. During the other times, those components will be at sleep mode or partially loaded mode. The reference provided claims a mathematical model based on Markov Chain, which estimates availability and reliability.

The performance of IoT cannot be evaluated using a simple mechanism, since it depends on components and performance of involving technologies. Moreover, huge amounts of data, network traffic, and heavy reliance on the cloud are the other factors that influence the performance of IoT [68]. Cloud facilitates resource-sharing, which is a vital requirement of IoT environment. In addition, the convergence of IoT and cloud enables the users to access the services irrespective of the location via an Internet connection. The convergence of IoT and cloud follows cloud-based IoT approach or IoT-centric cloud approach. In either ways, new challenges are foreseen, i.e. dynamic resource management, orchestration techniques, and dynamically offloading from clients/hosts to cloud, while overcoming existing individual challenges of cloud and IoT [69]. Matrices are available to measure the processing speed, cost and communication speed. However, there are only few studies on performance of 6LoWPAN [70,71], RPL [72–74], IEEE 802.15.4 [75] and application layer protocols; a complete IoT evaluation has not taken place to date. Hence, this gap needs to be filled up in near future, taking into account holistic view of IoT.

Security is an essential requirement of most of the applications. Therefore, relevant mechanisms should be adapted in order to meet user expected security level. In terms of security scope, it includes rarely addressed tasks such as trusted sensing, computation, privacy, communication and digital forging [76]. However, the security has become a critical issue, since IoT does not adhere to common security standards and an architecture [20]. IoT connects enormous amount of heterogeneous devices, resulting in increased vulnerability, due to the increased number of malware entry points. Therefore, traditional security architectures cannot fully satisfy the security requests of IoT. In order to mitigate the existing security issues in an IoT architecture, a scheme has been proposed based on a dynamic defense security mechanism by applying a biological immunology approach [77]. Furthermore, the attempts were made to secure the IoT communications by ensuring the security of IoT devices in [76]. As the initiation, the authors have proposed to adopt computer-aided design (CAD) techniques to design IoT devices, which are highly optimized in both energy and security. Importantly, CAD techniques can be used to implement strong and ample security with a low cost compared to expensive hardware-securing concepts proposed recently. Similarly, literature consists of several approaches to tackling the security issues in the current IoT paradigm. However, still many challenges are unresolved such as securing links during a dynamic mobility environments and authentication of the devices. Authors of [76] have suggested that securing IoT devices would secure IoT communication. Hence, they have proposed CAD-based model to design IoT devices as the initial step of securing them. However, it is practically not in use until date. Thus, the authentication of IoT devices in real-world scenario still has unresolved issues.

Reliability is not just passing information reliably, but being able to bear up changing environmental conditions, be resistant to security problems and long-term usability [78]. Availability and reliability go parallel, but reliability is considered to be vital in critical applications [79]. Reliability needs to be guaranteed in all aspects of software; hardware belongs to the architectural layers of IoT. Attempts were made to explain clearly the reliability consideration for link, transport and application layers together with the architecture considerations [78]. Moreover, a probabilistic approach was proposed to formally describe and analyze reliability and cost-related properties of the service composition in IoT [80].

The development of embedded technologies leads to increase the number of smart devices. The rapid growth of smartphones and tablets has increased the devices to person ratio up to 1.84 in 2010 [81]. Similarly, the client requirements from applications increase time to time. The ability to add more devices and services to IoT without degrading the QoS can be defined as the scalability of IoT. This task becomes hectic due to the heterogeneity of devices and underlying technologies. A distributed, interoperable architecture was proposed for IoT, which enables unified addition of new devices via a layered architecture to address the scalability issues in [82]. In general, QoS degrades when introducing new services and devices to IoT environment, consequent to the heterogeneity of them. Hence, it is vital to address the scalability issues without degrading the QoS for the realization of IoT notion. Thus, a scalable, distributed architecture has been proposed in [82]. The IoT infrastructure is categorized into three layers (1) virtual object layer (VOL), (2) composite virtual object layer (CVOL), and service layer (SL). The functionalities of the three layers, i.e. object virtualization, service composition and execution, and service creation and management, are put together to form the base structure "IoT daemon" of the distributed architecture. Every object hosts its own IoT daemon based on its processing power and memory. The three layers of IoT daemon unify various applications. VOL digitally represents each object's properties and functionalities. However, multiple objects work in collaboration to perform a task. Thus, during runtime, CVO is created as a mash-up of VOs corresponding to the task. In order to create a mash–up, potential VOs should be identified, which is done at the CVOL. Since all the devices are not centrally connected, it is a distributed architecture. With the aid of uniform representation of objects (VO), addition of new objects to the IoT network does not degrade QoS. The increase of network elements (NE) in the Internet leads to scalability issues in the network. Attempts were made by Barbosa C. Souza et al. to compensate the scalability issues with a service-oriented path computation element (S-PCE) instead of conventional host-oriented PCE. The comparison between results obtained and DNS server's logs confirmed that the proposed model supports more network elements than host-oriented PCE [83].

Interoperability is another major concern with regard to IoT, since various types of devices are connected to each other via IoT. Hence, IoT should facilitate services to all these devices regardless of the type, as interoperability is a necessity. This can be achieved to a certain level at the network and application level by adhering to standardized protocols. However, achieving interoperability is challenging due to ambiguous interpretations of the same protocol. Therefore, interoperability of IoT would become more realistic by avoiding such ambiguities. The authors proposed a solution to address IoT resources using web protocols via IoT hubs in [84]. Thus, the interoperability challenges reduced to presenting hub catalogues and data formats.

Most of the devices connected to IoT are mobile devices, and makes the scenario complex, since IoT applications need to deliver services considering the mobility factor as well. The sensor nodes in IoT facilitate mobility by using available standard management protocols, i.e. Mobile IPv6 (network layer) and TCPmigrate (transport layer), in order to facilitate mobility. However, these standards are too complex to be used in IoT nodes. A CoAP-based mobility protocol (CoMP) was found to be suitable for constrained devices in IoT [85]. Moreover, a group mobility management (GMM) mechanism is shown to be promising to ensure mobility [86]. In this context, machines are grouped according to mobility patterns and leader machine does mobility management for the group.

7. IoT APPLICATIONS

The concept of IoT has uplifted the opportunities to use capabilities of heterogeneous devices, which are connected, thus leading to the enhancement of innovating novel applications. This section gives an overview of common IoT applications such as health care, smart home, and smart cities, as shown in Figure 5. It illustrates the major applications of IoT and the interconnection among them.

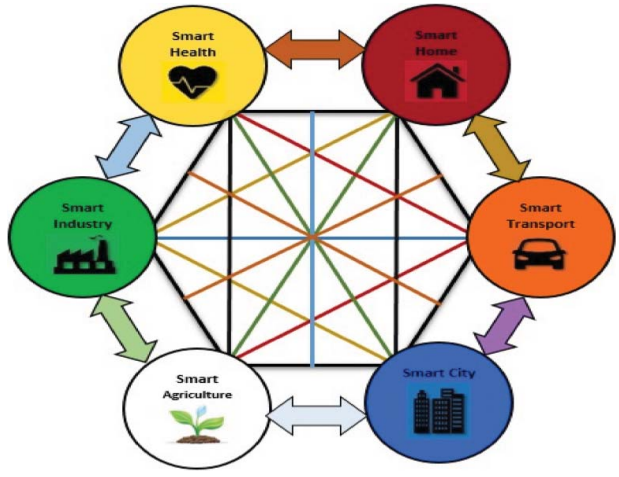

Figure 5: IoT applications

Currently, the health care has started moving towards home-centric health care services, from hospital-centric services [87]. Hence, it is crucial to use technological advancements in the health care sector. IoT technologies are widely applied in assisted living solutions. The body temperature, blood pressure, and breathing patterns are monitored through sensors placed on the body. Moreover, another use of IoT in health care is to monitor the patients from a remote location. With regard to elderly health care, fall detection is another important application of IoT. In hospital settings, hygiene of the hospital and equipment monitoring can be facilitated by using various types of sensing and actuating mechanisms.

The smart home is an innovative concept, which supports the residents to central controlling of lights, enhance security, heating ventilation and air condition controlling (HVAC), monitor the resource consumption and patterns of consumption, so that it leads towards maximum resource utilization of household. Moreover, IoT concepts can be applied to control home appliances remotely, to feed pets, and to detect intrusion and smoke. The internal network, intelligent control, and home automation are crucial for realistic, smart homes. An architecture was proposed to merge the smart home into the cloud architecture, so that smart home applications can provide many services, while gathering more information from the cloud [88].

The advancement of IoT has laid its roots to transportation as well. In general, smart transportation helps prevent/monitor accidents and also used to location-finding. Moreover, smart transportation can be extended to airlines, logistics, and trains. In addition, it includes smart parking, package monitoring, traffic routing, and insurance adjustments as supporting services.

Another emerging application of IoT is the implementation of smart cities. Smart cities are defined with the aim of making a better use of the public resources, increasing the quality of the services offered to the citizens, while reducing the operational costs of the public administration [7].

Al-Hader et al. proposed a five-level pyramid architecture for smart cities. The bottom layer is the smart infrastructure layer including electronics, water, natural gas, fire protection, electronic communications, and network, as shown in Figure 6 [89]. Street lighting, waste management, maintenance, surveillance, emergency and building health monitoring are some of the major functionalities that can be included in smart cities.

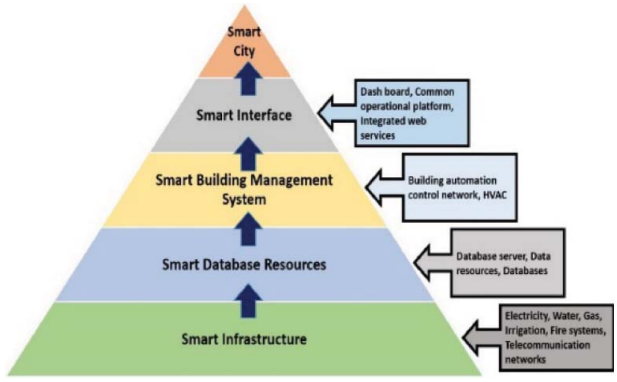

Figure 6: A pyramid architecture for smart cities

IoT is still evolving due to the integration of novel concepts as well as the adaption of existing technologies. Thereby, it supports the development of more realistic, competitive, and advanced IoT-based applications. The development of IoT applications based on the client requirements evolves according to the needs of the users. Moreover, many organizations and interest groups are geared to standardized IoT-related technologies to ensure more effective and secure applications.

8. CONCLUSION

IoT is a maturing concept, which connects various types of devices seamlessly to generate an enormous amount of data, and shared among the devices. The processed information is used for critical and non-critical decision-making so that it improves the quality of life.

This paper has presented a basic overview of IoT, followed by a summarized description regarding available architectural models of IoT. Moreover, some important standards and protocols were discussed in terms of IoT communication technologies. These standards and protocols are presented in a very simple and concise way so that it can help the reader to understand the basic concepts easier. Moreover, various applications of IoT have been identified to ensure the better use of these applications in our daily lives. The latter part of the paper presented some issues and attempts made by the researchers to overcome these challenges. The main challenges of an IoT environment are security, availability, and performance. Indeed, it is vital to address these challenges to ensure the growth of IoT applications. Therefore, IoT applications can be integrated with advanced security mechanisms to detect threats and anomalies, while occupying predictive analysis to evolve the integrated security mechanisms. Moreover, it is crucial to address the coexistence interference of IoT environment, which consists with multiple communication technologies, i.e. Bluetooth,

ZigBee, and Wi-Fi. Thereafter, the packet loss due to coexistence interference will be minimized. The adoption of optimized channel selection algorithms and hop count-reducing mechanisms such as coordinator/actuator placement are worthy solutions, which enhance the availability and reliability of the IoT environment. Finally, the paper described feasible IoT applications, in order to affirm the applicability of IoT in the real world.

FUNDING

This study was supported by the BK21 Plus project (SW Human Resource Development Program for Supporting Smart Life) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea [21A20131600005]; and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology and National Research Foundation of Korea (NRF) [2016R1D1A1B03933566].

REFERENCES

1. J. Gubbi, R. Buyyab, S. Marusica, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Gen. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

2. O. Vermesan, et al. "Internet of Things beyond the Hype: Research, Innovation and Deployment," in *Building the Hyperconnected Society: Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*, O. Vermesan and P. Friess, Eds. River Publishers, 2015, pp. 15–118.

3. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012.

4. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

5. A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 58–67, 2011.

6. Texas Instrument Organization. (2014, Sep.). The internet of things: Opportunities & challenges [Online]. Available: http://www.ti.com/ww/en/internet_of_things/pdf/14-09-17-IoTforCap.pdf [Accessed September 2015].

7. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014.

8. E. Kasznik. (2015, Apr.). "Internet of things: The third wave of revolution," *World Intellect. Property Rev.* [Online]. Available: http://www.worldipreview.com/contributed-article/semiconductor-focus-the-third-wave-of-revolution [Accessed September 2015].

9. "Internet of things technologies," *Postscapes* [Online]. Available: http://postscapes.com/internet-of-things-technologies%20#communication [Accessed September 2015].

10. S. Schneider. (2013, Oct.). "Understanding the protocols behind the internet of things," *Electronicdesign* [Online]. Available: http://electronicdesign.com/iot/understanding-protocols-behind-internet-things [Accessed September 2015].

11. "Internet of things protocols & standards," *Postscapes* [Online]. Available: http://postscapes.com/internet-of-things-protocols [Accessed September 2015].

12. I. Ganchev, Z. Ji, and M. O'Droma, "A generic IoT architecture for smart cities," in *ISSC 2014/CIICT 2014*, Limerick, 2014.

13. Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, and K. Leung, "A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, 2013.

14. I. Marshal, O. Alsaryraha, T. Chung, C. Yang, W. Kuob, and D. Agrawal, "Choices for interaction with things on Internet and underlying issues," *Ad Hoc Netw.*, vol. 28, pp. 68–90, 2015.

15. M. Yun and B. Yuxin, "Research on the Architecture and Key Technology of Internet of Things (loT)," in *International Conference on Advances in Energy Engineering*, Beijing, 2010.

16. Q. Xiaocong and Z. Jidong, "Study on the structure of "Internet of Things (IOT)" business operation support platform," in *12th IEEE International Conference on Communication Technology*, Beijing, 2010.

17. E. Borgia, "The internet of things vision: Key features, applications and open issues," *Comput. Commun.*, vol. 54, pp. 1–31, 2014.

18. Y. Shi and T. Hou, "Internet of Things key technologies and architectures research in information processing," in *2nd International Conference on Computer Science and Electronic Engineering*, Hangzhou, 2013.

19. V. Karagiannis, P. Chatzimisios, F. Gallego, and J. Zarate, "A survey on application layer protocols for the internet of things," *Trans. IoT Cloud Comput.*, vol. 1, no. 1, 2015.

20. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

21. Z. Yang, Y. Peng, Y. Yue, X. Wang, Y. Yang, and W. Liu, "Study and application on the architecture and key

technologies for IOT," in *International Conference on Multimedia Technology*, Hangzhou, 2011.

22. M. Wu, T. Lu, F. Ling, J. Sun, and H. Du, "Research on the architecture of Internet of Things," in *3rd International Conference on Advanced Computer Theory and Engineering*, Chengdu, 2010.

23. Z. Pala and N. Inanc, "Smart parking applications using RFID technology," in *2007 1st Annual RFID Eurasia*, Istanbul, 2007.

24. E. Nakamori, D. Tsukuda, M. Fujimoto, Y. Oda, T. Wada, H. Okada, and K. Mutsuura, "A new indoor position estimation method of RFID tags for continuous moving navigation systems," in *2012 International Conference on Indoor Positioning and Indoor Navigation*, Sydney, 2012.

25. A. Boaventura and N. Carvalho, "A batteryless RFID remote control system," *IEEE Trans. Microwave Theory Tech.*, vol. 61, no. 7, pp. 2727–2736, 2013.

26. Technovelgy, Problems with RFID [Online]. Available: http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=20 [Accessed September 2015].

27. Technovelgy, Advantages of RFID versus barcodes [Online]. Available: http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=60 [Accessed September 2015].

28. M. Electronics, The role of sensor fusion in the internet of things [Online]. Available: http://kr.mouser.com/applications/sensor-fusion-iot/ [Accessed September 2015].

29. R. Want, "Near field communication," *IEEE Pervasive Comput.*, vol. 10, no. 3, pp. 4–7, 2011.

30. P. McDermott-Wells, "What is Bluetooth?," *IEEE Potentials 02*, vol. 23, no. 5, pp. 33–35, 2005.

31. searchmanufacturingerp, RFID (radio frequency identification) definition [Online]. Available: http://searchmanufacturingerp.techtarget.com/definition/RFID [Accessed September 2015].

32. R. w. world, NFC vs RFID vs Bluetooth [Online]. Available: http://www.rfwireless-world.com/Terminology/NFC-vs-RFID-vs-Bluetooth-vs-wifi.html [Accessed September 2015].

33. P. Du and G. Roussos, "Adaptive communication techniques for the internet of things," *J. Sens. Actuator Netw*, vol. 2, no. 1, pp. 122–155, 2013.

34. E. Ferro and F. Potortì, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," *IEEE Wireless Commun.*, vol. 12, no. 1, pp. 12–26, 2005.

35. S. Galli, A. Scaglione, and Z. Wang, "Power line communications and the smart grid," in *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, 2010.

36. S. Dey, A. Mukherjee, H. Paul, and A. Pal, "Challenges of using edge devices in IoT computation grids," in *2013 International Conference on Parallel and Distributed Systems (ICPADS)*, Seoul, 2013.

37. Postscapes, "Internet of things hardware round-up," *Postscapes* [Online]. Available: http://postscapes.com/internet-of-things-hardware [Accessed September 2015].

38. S. M. J. P. R. P. Levis, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, "TinyOS: An operating system for sensor networks," in *Ambient Intelligence*, W. Weber, J. M. Rabaey and E. Aarts, Eds. Berlin: Springer, 2005, pp. 115–148.

39. Q. Cao, T. Abdelzaher, J. Stankovic, and T. He, "The LiteOS operating system: Towards unix-like abstractions for wireless sensor networks," in *2008. IPSN '08. International Conference on Information Processing in Sensor Networks*, St. Louis, MO, 2008.

40. E. Baccelli, O. Hahm, M. Günes, M. Wählisch, and T. Schmidt, "RIOT OS: Towards an OS for the Internet of Things," in *INFOCOM'2013*, Turin, 2013.

41. X. Xiaojiang, W. Jianli, and L. Mingdong. (2010). Services and key technologies of the internet of things [Online]. Available: http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2010Year/no2/articles/201006/t20100609_186201.html [Accessed September 2015].

42. M. Gigli and S. Koo, "Internet of Things: Services and applications categorization," *Adv. Internet Things*, vol. 1, no. 2, pp. 27–31, 2011.

43. A. Haubenwallera and K. Vandikasb, "Computations on the Edge in the internet of things," in *The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015)*, London, 2015.

44. L. S. Committe. (2003, Oct.). "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for low-rate wireless," *IEEE Comput. Soc.* [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1237559 [Accessed September 2015].

45. N. Kushalnagar, G. Montenegro, and C. Schumacher. (2007, Aug.). IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals [Online]. Available: https://tools.ietf.org/html/rfc4919 [Accessed September 2015].

46. G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. (2007, Sep.). Transmission of IPv6 packets over IEEE 802.15.4 networks [Online]. Available: https://tools.ietf.org/html/rfc4944 [Accessed September 2015].

47. J. Gutierrez (2005). IEEE Std. 802.15.4 – Enabling pervasive wireless sensor networks [Online]. Available: http://www.cs.berkeley.edu/~prabal/teaching/cs294-11-f05/slides/day21.pdf [Accessed September 2015].

48. G. Anastasi. (2014, May). From IEEE 802.15.4 to IEEE 802.15.4e another step towards the internet of (Important) things [Online]. Available: http://www.iet.unipi.it/g.anastasi/talks/2014-Guangzhou.pdf [Accessed September 2015].

49. X. Xu, D. Yuan, and J. Wan, "An enhanced routing protocol for ZigBee/IEEE 802.15.4 wireless networks," in *FGCN '08. Second International Conference on Future Generation Communication and Networking*, Hainan Island, 2008.

50. J. T. A. Ko, S. Dawson-Haggerty, D. Culler, J. Hui, and P. Levis, "Connecting low-power and lossy networks to the internet," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 96–101, 2011.

51. J. Hui and D. Culler, "Extending IP to low-power, wireless personal area networks," *IEEE Internet Comput.*, vol. 12, no. 4, pp. 37–45, 2008.

52. M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (Important) things," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 3, pp. 1389–1406, 2012.

53. T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL)," in *IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Wuhan, 2011.

54. T. Winter, P. Thubert, A. Brandt, R. Kelsey, P. Levis, P. K. Levis, R. Struik, J. Vasseur, and R. Alexander. (2012 Mar.). RPL: IPv6 routing protocol for low-power and lossy networks [Online]. Available: https://tools.ietf.org/html/rfc6550 [Accessed September 2015].

55. C. Links. (2015). Wireless communication standards for the internet of things [Online]. Available: http://www.greenpeak.com/Press/PressKit/2015GreenPeakWhitePaperIoT&CommStandards.pdf [Accessed September 2015].

56. L. Frenzel. (2012, Oct.). "The fundamentals of short-range wireless technology," *Electron. Des.* [Online]. Available: http://electronicdesign.com/communications/fundamentals-short-range-wireless-technology [Accessed September 2015].

57. A. Castellani, M. Rossi, and M. Zorzi, "Back pressure congestion control for CoAP/6LoWPAN networks," *Ad Hoc Netw.*, vol. 18, pp. 71–84, 2014.

58. Z. Shelby, K. Hartke, and C. Bormann. (2014, June). "The constrained application protocol (CoAP)," *Internet Eng. Task Force (IETF)* [Online]. Available: https://tools.ietf.org/html/rfc7252 [Accessed June 2016].

59. D. Locke. (2010, Aug.). MQ Telemetry Transport (MQTT) V3.1 protocol specification [Online]. Available: http://www.ibm.com/developerworks/library/ws-mqtt/ [Accessed September 2015].

60. U. Hunkeler, H. Truong, and A. Stanford-Clark, "MQTT-S — A publish/subscribe protocol for Wireless Sensor Networks," in *3rd International Conference on Communication Systems Software and Middleware and Workshops*, Bangalore, 2008.

61. J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet. (2011, Apr.). RPL: The IP routing protocol designed for low [Online]. Available: http://www.ipso-alliance.org/wp-content/media/rpl.pdf [Accessed September 2015].

62. C. Hennebert and J. Dos Santos, "Security protocols and privacy issues into 6LoWPAN stack: A synthesis," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 384–98, 2014.

63. J. Sarto, "ZigBee VS 6LoWPAN for sensor networks, white paper," *LSR* [Online]. Available: https://www.lsr.com/white-papers/zigbee-vs-6lowpan-for-sensor-networks [Accessed September 2015].

64. A. Ott, "Wireless networking with IEEE 802.15.4 and 6LoWPAN [Online]. Available: http://elinux.org/images/7/71/Wireless_Networking_with_IEEE_802.15.4_and_6LoWPAN.pdf [Accessed September 2015].

65. J. M. E. Granjal and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 3, pp. 1294–1312, 2015.

66. C. Strotmann, New DNS technologies in the LAN [Online]. Available: http://meetings.ripe.net/ripe-55/presentations/strotmann-mdns.pdf [Accessed January 2016].

67. D. Macedo, L. Guedes, and I. Silva, "A dependability evaluation for Internet of Things incorporating redundancy aspects," in *ICNSC*, Miami, FL, 2014.

68. Sevone, (2015). How will the internet of things disrupt your performance monitoring strategy? – White paper [Online]. Available: https://www.sevone.com/white-paper/how-will-internetthings-disrupt-your-performance-monitoring-strategy [Accessed September 2015].

69. A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," in *IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, 2014.

70. B. Enjian and Z. Xiaokui, "Performance evaluation of 6LoWPAN gateway used in actual network environment," in *International Conference on Control Engineering and Communication Technology (ICCECT)*, Liaoning, 2012.

71. R. Khoshdelniat, G. Sinniah, K. Bakar, M. Shaharil, Z. Suryady, and U. Sarwar, "Performance evaluation of IEEE802.15.4 6LoWPAN gateway," in *17th Asia-Pacific Conference on Communications (APCC)*, Sabah, 2011.

72. N. Long, N. De Caro, W. Colitti, A. Touhafi, and K. Steenhaut, "Comparative performance study of RPL in Wireless

Sensor Networks," in *IEEE 19th Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, Eindhoven, 2012.

73. A. Yushev, P. Lehmann, and A. Sikora, "6LoWPAN with RPL performance measurements in an Automated Physical Testbed," in *2nd IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, Offenburg, 2014.

74. H. Xie, G. Zhang, D. Su, P. Wang, and F. Zeng, "Performance evaluation of RPL routing protocol in 6LoWPAN," in *5th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, 2014.

75. X. Cheng, Q. Liang, and J. He, "Analysis of IEEE802.15.4 network performance comprehensive evaluation and prediction," in *International Conference on Measurement, Information and Control (ICMIC)*, Harbin, 2013.

76. T. Xu, J. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Jose, CA, 2014.

77. C. Liu, Y. Zhang, and H. Zhang, "A novel approach to IoT security based on immunology," in *2013 9th International Conference on Computational Intelligence and Security (CIS)*, Leshan, 2013.

78. J. Kempf, J. Arkko, N. Beheshti, and K. Yedavalli, Thoughts on reliability in the internet of things [Online]. Available: https://www.iab.org/wp-content/IAB-uploads/2011/03/Kempf.pdf [Accessed September 2015].

79. N. Maalel, E. Natalizio, A. Bouabdallah, P. Roux, and M. Kellil, "Reliability for emergency applications in internet of things," in *IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, Cambridge, MA, 2013.

80. L. Li, Z. Jin, G. Li, L. Zheng, and Q. Wei, "Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach," in *IEEE 19th International Conference on Web Services (ICWS)*, Honolulu, HI, 2012.

81. D. Evans. (2011, Apr.). The internet of things – cisco White paper [Online]. Available: http://www.iotsworldcongress.com/documents/4643185/3e968a44-2d12-4b73-9691-17ec508ff67b [Accessed September 2015].

82. C. Sarkar, S. Nambi, R. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying IoT applications," in *IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, 2014.

83. V. Barbosa C. Souza, X. Masip-Bruin, E. Marin-Tordera, W. Ramirez, and S. Sanchez-Lopez, "Towards the scalability of a service-oriented PCE architecture for IoT scenarios," in *20th European Conference on Networks and Optical Communications – (NOC)*, London, 2015.

84. I. Ishaq, D. Carels, G. Teklemariam, J. Hoebeke, F. Van den Abeele, E. De Poorter, I. Mo erman, and P. Demeester, "IETF standardization in the field of the internet of things (IoT): A survey," *J. Sensor Actuator Netw.*, vol. 2, no. 2, pp. 235–287, 2013.

85. S.-M. Chun and J.-T. Park, "Mobile CoAP for IoT mobility management," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, 2015.

86. H.-L. Fu, P. Lin, H. Yue, G.-M. Huang, and C.-P. Lee, "Group mobility management for large-scale machine-to-machine mobile networking," *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1296–1305, 2013.

87. Z. Pang, "Technologies and architectures of the Internet-of-Things (IoT) for health and well-being," Doctoral thesis [Online]. Available: http://kth.diva-portal.org/smash/get/diva2:621384/FULLTEXT01.pdf [Accessed September 2015].

88. X. Ye and J. Huang, "A framework for cloud-based smart home," in *International Conference on Computer Science and Network Technology*, Harbin, 2011.

89. M. Al-Hader, A. Rodzi, A. R. Sharif, and N. Ahmad, "Smart city components architecture," in *International Conference on Computational Intelligence, Modelling and Simulation*, Brno, 2009.

Authors

Bhagya Nathali Silva received the B.S. and M.S. degree in Information Technology from Sri Lanka Institute of Information Technology, Colombo, in 2011. She is currently a Ph.D. candidate of School of Computer Science and Engineering in Kyungpook National University, Daegu, Korea. Her area of expertise includes architecture designing for Internet of Things, Machine-to-Machine Communication, Cyber Physical Systems, and Communication Protocols, etc.

E-mail: nathalis@netopia.knu.ac.kr

Murad Khan received the B.S. degree in computer science from university of Peshawar Pakistan in 2008. He is currently a Ph.D. candidate of School of Computer Science and Engineering in Kyungpook National University, Daegu, Korea. His area of expertise includes adhoc and wireless networks, architecture designing for Internet of Things, and Communication Protocols, etc.

E-mail: mkhan@netopia.knu.ac.kr

Kijun Han received the B.S. degree in electrical engineering from Seoul National University, Korea, in 1979 and the M.S. degree in electrical engineering from the KAIST, Korea, in 1981 and the M.S. and Ph.D. degrees in computer engineering from the University of Arizona, in 1985 and 1987, respectively. He has been a professor of School of Computer Science and Engineering at the Kyungpook National University, Korea since 1988.

E-mail: kjhan@knu.ac.kr