Editorial

Internet of Things – An Evolving Super Highway

Internet of Things is the theme chosen for the current number of the Science Magazine Vidurava. The Editorial Sub-committee has invited four key players in the field to provide an insight of what is referred to as the Internet of Things (IOT) for the benefit of the reading clientele of Vidurava. Internet of Things is a new gateway leading to a super highway in wireless information and data transmission. It is a developing super highway in a technologically inter-linked computer-based network capable of remotely probing a variety of physical devices and sources, and transferring almost an unlimited amount of data and information.

Many definitions and explanations have been given to IOT by the relevant contributors to this publication. One of the simple explanatory definitions that may be considered is that – "The Internet of Things" is a system of interrelated computing devices, mechanical and digital machines, objects, people or animals that are provided with "unique identifiers" with ability to transfer data over a network without requiring human-to-human, or human to computer interaction.

Among the "Things", referred to in IOT are devices or sensors such as human heart monitoring implants, biochip transponders (a device for receiving a radio signal for automatic transfer in a different signal, and attached to farm animals), electric clams in coastal waters, automobiles with sensors for automation, DNA analysis devices, environmental, food, pathogen monitoring or field operation devices that assist firefighters in search and rescue operations etc.

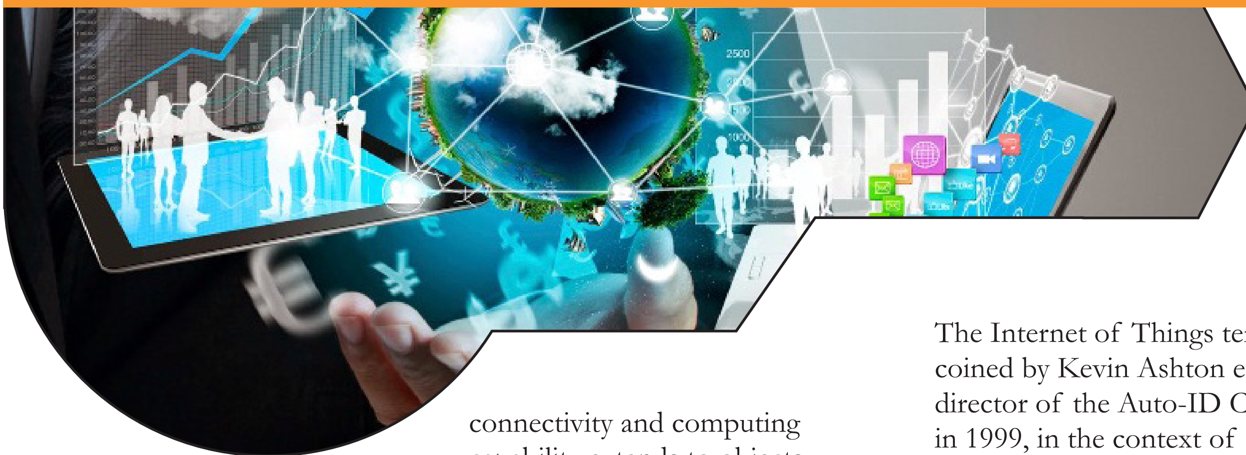
Although the phrase Internet of Things was first coined in1999, by 2013 the vision of IOT had evolved into a convergence of multiple technologies ranging from wireless communication to the internet, and from embedded systems to micro-electro-mechanical systems. This would technically mean that the traditional fields of embedded systems, including wireless sensor networks, controlled systems, automobiles and others all contribute to enabling the Internet of Things. The expansion of internet connected automation into a plethora of new application areas, generating large amounts of data from diverse locations with the necessity for quick aggregation and collation of information which would then require indexing, storing and processing, is considered to be one of the platforms of the concept of Smart Cities.

Finally, discussing large scale deployment of IOT, Wikipedia in a recent note claims that South Korea has embarked on a fully equipped and wired Smart City, considered to be the first of its kind in the world. Here nearly everything in this City is planned to be wired, connected and turned into a constant stream of data that would be monitored and analysed by an array of computers, with little or no human intervention. It is likely that the Ministry handling Sri Lanka's first Megapolis development plan in the Western Province may have taken note of this development.

M. Asoka T. De Silva

Theme article : The Internet of Things : The Big Picture

Prof. Dileeka Dias



1.What is the Internet of Things?

The term Internet of Things (IoT) generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.

The Internet of Things term was coined by Kevin Ashton executive director of the Auto-ID Center in 1999, in the context of supply chain management. Around the same time, Neil Gershenfeld was speaking about similar things from the MIT Media Lab in his book When Things Start to Think.

The IoT extends the Internet and

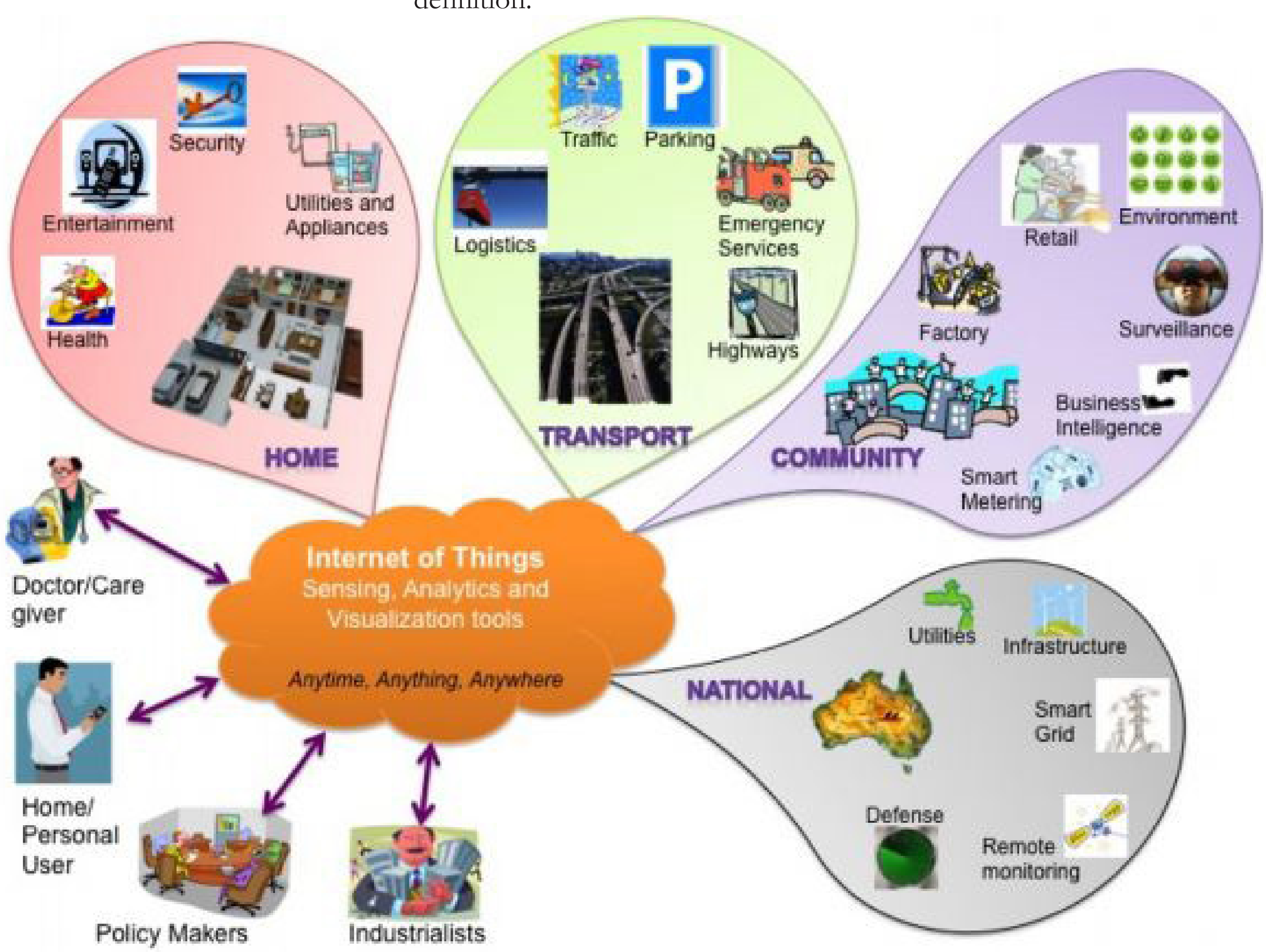


Fig. 1 : Possible application areas of IoT

the Web to the physical world, through the deployment of devices with embedded identification, sensing and/or actuation and communication capabilities. The devices are linked through information and communication technologies based on the Internet Protocol (IP), and will enable Internet connectivity for everyday objects in homes, roads and vehicles, utilities, factories, battlefields, the environment, and even on our bodies. Such objects are generally referred to as smart objects, and the applications they make possible smart scenarios.

The IoT thus builds on three pillars, related to the ability of smart objects to: (i) be identifiable (anything identifies itself), (ii) to communicate (anything communicates) and (iii) to interact (anything interacts) – either among themselves, building networks of interconnected objects, or with end-users or other entities in the network. It is a complex concept that cuts across multiple disciplines, and that depends on synergetic efforts from several communities such as telecommunication industry, device manufacturers, semantic Web, and informatics for its success. The IoT offers a platform for everyone from garage hobbyists to technology giants to innovate.

Combined with powerful data analytic capabilities, the IoT is envisioned to enable entirely new areas of applications and services having great technical, social, economic and political significance. It promises to transform the way people work, live and play, and the way governments make policies and decisions. Projections for the impact of IoT on the Internet and the economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025. Figure 1 illustrates some possible application areas.

This article provides an overview of the Internet of Things. To make it easier for the reader to understand the IoT paradigm, we initially illustrate some IoT applications being implemented, proposed or researched. Next we look at IoT systems in detail, in terms of their key components. Finally we present some challenges for the real-life deployment of the IoT and its acceptance by potential users.

Several articles in this issue to follow, will highlight specific aspects of IoT such as applications and devices, communication and networking, and security and privacy.

2.IoT Applications

The IoT enables us to create a self-aware environment where we know exactly what is happening around us. From personal health to home security, from agriculture to urban traffic control, from utility metering to law enhancement, from entertainment to public safety, the

Table 1. Applications identified by the City of Melbourne

Citizens	
Healthcare	Triage, patient monitoring personnel monitoring, disease spread modelling and containment – real- time health status and predictive information to assist practitioners in the field, or policy decision in pandemic scenarios
Emergency services, defense	Remote personnel monitoring (health, location); resource management and distribution, response planning; sensors built into building infrastructure to guide first responders in emergencies or disaster scenarios
Crowd monitoring	Crowd flow monitoring for emergency management, efficient use of public and retail spaces; workflow in commercial environment
Transport	
Traffic managementInfrastructure monitoring	Intelligent transportation through real-time traffic information and path optimization Sensors built in to infrastructure to monitor structural fatigue and other maintenance; accident monitoring for incident management and emergency response coordination
Services	
Water Building management Environment	Water quality, leakage, usage, distribution, waste management Temperature, humidity control, activity monitoring for energy usage management, D heating, Ventilation and air conditioning (HVAC), Air pollution, noise monitoring, waterways, industry monitoring

Fig. 2 : Elements of an IoT system

applications proposed for IoT are too many to discuss in detail. In this Section we highlight only a few. One of many possible ways of classifying IoT applications is as shown in Figure 1. The Home domain utilizes IoT at the personal level, and the Transport and Community domains at the enterprise level. Application examples in the National domain include infrastructure, defense, utilities and public services. Whatever classification we adopt for IoT applications, there is a significant overlap in applications and the use of data between domains. The Internet and widespread mobile connectivity enable sharing of data between different applications in a seamless manner creating multiple business opportunities. For instance, Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company, which can in turn optimize the supply and demand with its national level utility IoT applications.

2.1.Personal and Home IoT

A number of possible IoT application concepts and their benefits are listed below. A number of electronic manufacturers as well as all mobile device platforms offer applications of this nature supported by mobile data communication technologies. However, a common platform and standards for this type of services is yet to emerge.

• Healthcare in the home, utilizes body area sensors measuring physiological parameters and smartphones to collect heath information at an IoT back-end, through which a variety of ubiquitous healthcare services can be provided.

• Care of the elderly in their homes which may use IoT for monitoring people in their home environments, providing early intervention and treatment.

• Control of home equipment such as lights, air conditioners, refrigerators etc. to better manage home energy utilization.

• Home security is an area where we find a growing range of IoT application, integrating a variety of sensing mechanisms for intrusion detection.

• Individual devices ('things') in the home can periodically send notifications via social media such as Facebook and Twitter. This is envisaged to be a transformation of social networking due to the IoT.

2.2.Enterprise IoT

Enterprise IoT applications can be broadly termed Smart Environments, which may include buildings, infrastructure,

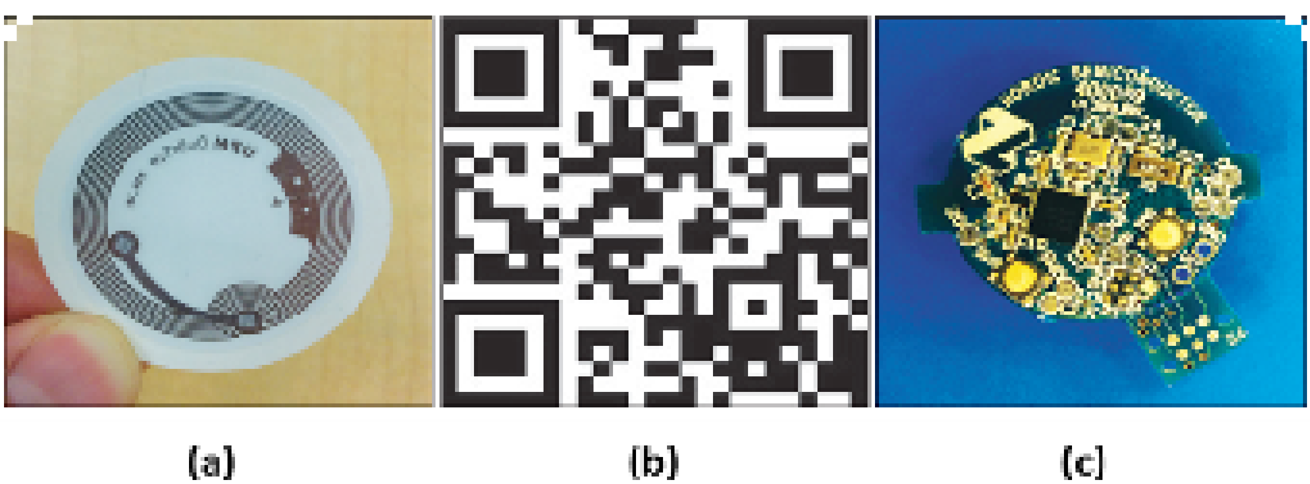


Fig. 3 : Tagging technologies for identification of IoT devices. (a) NFC, (b) QR code, (c) BLE tag

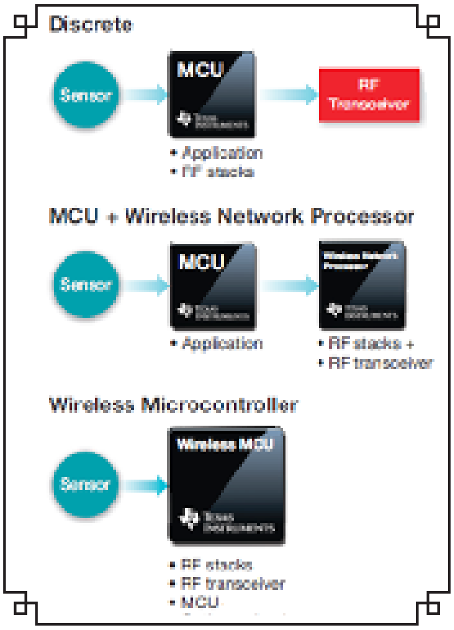


Fig. 4 : IoT device electronics

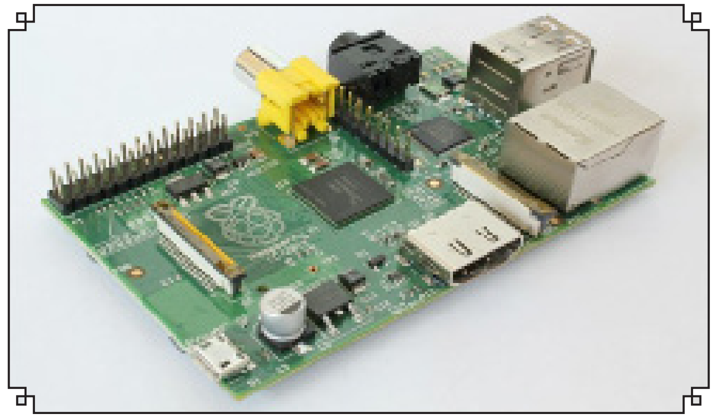


Fig. 5 : The Raspberry Pi, a credit - card sized single board computer

traffic, utilities, and the general environment. As examples, some applications identified by the City of Melbourne are listed in Table 1 below. These applications are grouped according to their impact areas: citizens (health and wellbeing), transport (mobility, productivity, pollution), and critical community services managed and provided by the local government to city inhabitants. Here too, applications share data among them for mutual benefit.

2.3.Utility IoT

Utility IoT applications target service optimization, i.e., for resource management in order to optimize cost vs. profit. These applications are envisaged to be made up of very extensive networks operated by large organizations on a regional or national scale. Applications involving electricity and water supply management are of high priority in the utility IoT arena.

Smart grid and smart metering are key utility IoT applications being rolled out around the world currently. The benefits of these applications are two-fold. First, they help consumers to achieve energy efficiency by modifying their electricity consumption patterns. Secondly, they help the electricity companies to maintain the load balance within the grid, ensuring high quality of service .

Water network monitoring is another valuable IoT service. Sensors measuring critical water quality parameters installed at key locations will be able to ensure the quality assurance of drinking water. This may avoid or provide early warning of contamination of water supplies. Along similar lines, agriculture-related monitoring applications are growing in pilot level IoT implementations. Among the functions offered by these include soil moisture monitoring, automatic watering and fertilization.

3.Elements and Enablers of IoT

The six main building blocks

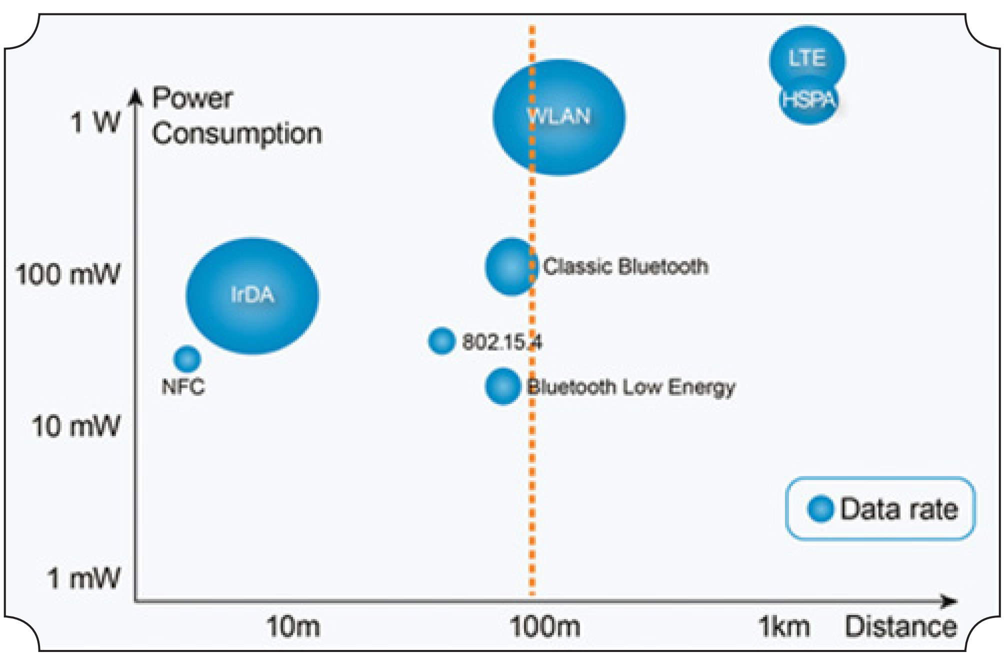


Fig. 6 : Comparison of power consumption, range and data rate of short-range communication technologies

	Bluetooth Low Energy	802.15.4	WLAN
Cost	✓	✓(✓)	✓
Security	✓	✓	✓
Power consumption	✓	✓	×
Ecosystem	✓	×	✓
Reliability	✓	✓	✓
Ease of use	✓	✓	✓
Range	✓	✓(✓)	✓

	Bluetooth Low Energy	802.15.4	WLAN	NFC
Remote control	✓	✓	✓	×
Security	✓	✓	✓	✓
Health and Fitness	✓	✓	✓	×
Home and Building	✓	✓	✓	×
Industrial	✓	✓	✓	×
Positioning	✓	✓	✓	×
Payment	✓	×	×	✓
Automotive	✓	×	✓	✓
Comments	Largest ecosystem (phones, tablets, ...). Low power.	Low power but closed ecosystem. Established in some use cases e.g. Smart Energy	Large ecosystem but higher power. Infrastructure use.	Low power but very short range

Fig. 7 : Silent characteristics of short - range communication technologies and their suitability for different applications

needed to deliver the functionality of IoT are illustrated in Figure 2. This section looks at these building blocks in detail, along with examples of available technologies and realizations in each case.

3.1. Identification

Identification is essential in the IoT to name and match services with their demand. Electronic Product Codes (EPCs) is an example of a universal identifier that gives a unique identity to a specific physical object that it is attached to. EPCs are encoded on Radio Frequency Identification (RFID) tags which can be used to track all kinds of objects including trade items, fixed assets, documents, or reusable transport items. A reader would transmit a query signal to the tag and receive the reflected signal containing the EPC. RFID tags can be passive, active or semi-passive. Passive tags are very cheap, but depend solely on the electromagnetic energy supplied by the reader. Active tags self-powered, and thus have a longer reading range, but is higher in cost than a passive tag.

RFID was considered one of the most likely technologies to accelerate the formation of the IoT. Though RFID has become very popular in logistics applications, it has not been successful in the wider arena of IoT for identification, perhaps the major reason being the absence of support for it in mobile phones, thus needing a special reader. A more advanced and secure form of RFID, Near Field Communication (NFC) is strongly promoted for applications involving electronic payments. Smartphone manufacturers are now integrating NFC into their devices, adding to the potential of this technology as a key enabler for IoT.

Another contender for low-cost tagging is the optical or printed tag. The most popular is the Quick Response (QR) code. The QR code can be read by an ubiquitous mobile application and a camera found in all modern smartphones. QR codes are widely used on many products, newspapers an advertising material.

A promising new technology in the device tagging space is Bluetooth low energy (BLE). All smartphones released in the last few years have BLE built in. With BLE, small low cost electronic tags can be implemented, which can signal their presence wirelessly.

Figure 3 shows the three tagging technologies discussed above.

An object's identity may not be

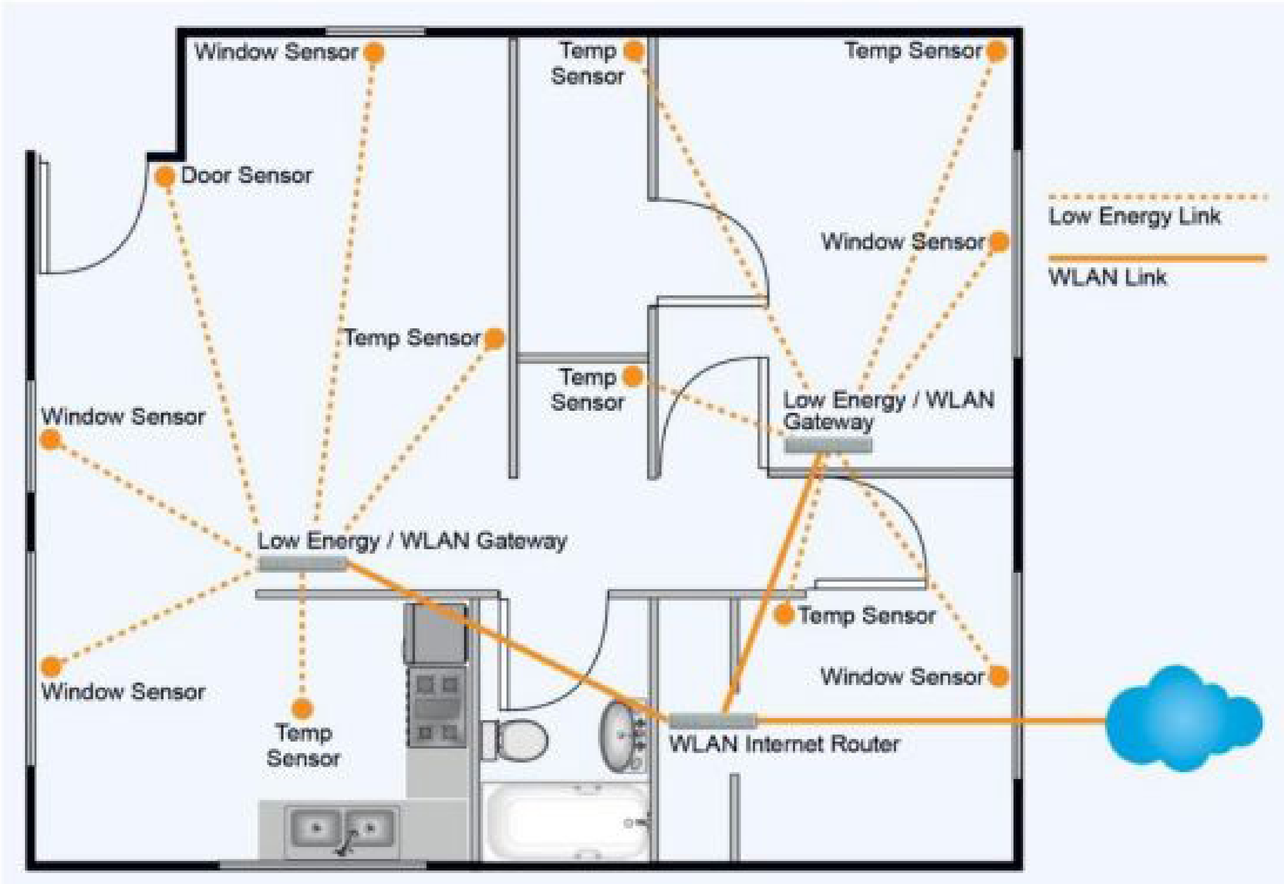


Fig. 8 : Networking architecture for IoT in a typical Smart Home application supporting several communication technologies

always globally unique. In such an event unique address is needed to identify objects within the communications network. IPv6 has been proposed as an addressing scheme for IoT objects, due to the very large number of objects expected to be connected in future.

3.2.Sensing

Sensing in the IoT is done by smart sensors and actuators. IoT devices are of different levels of integration, and contains sensing elements, actuator elements, data processing and control subsystems (a microcontroller) and a wireless communication mechanism (an RF transceiver). The devices are programmable, allowing the designer the flexibility to build in the functions required of the device. Figure 4 shows different levels of integration available in popular electronic devices. In the Discrete option, the microcontroller and the RF transceiver are two separate devices. The Wireless Microcontroller on the other hand is capable of interfacing to the sensor, data processing and control functions as well as wireless communications. At a more sophisticated level, IoT devices may be built around single board computers (SBCs) integrated with single-board computers and built-in security and communications protocols. The Raspberry Pi shown in Figure 5, is an increasingly popular SBC among IoT enthusiasts. Many other hardware platforms too have become available to implement IoT devices such as Arduino, Friendly ARM, Intel Galileo, Gadgeteer, BeagleBone, WiSense, T-Mote Sky etc. Though the high cost of such devices prevent them from being used extensively, they are suitable for special purpose applications and lend to quick prototyping and application development due to the availability of a wide variety of developer tools and standard interfaces. However, expert electronics designers will be able to develop their own devices from scratch, better optimizing cost, power and other resources specific to their application.
RFID, originally intended for simple, passive identification of objects has been proposed as a generic sensing platform for IoT applications in healthcare. This technology promises low cost, reconfigurable, disposable sensors

Table 2. IoT Services

Service Class	Description	Examples
Identity-related services	These are the most basic type, and are used in other types of services.	Every application that needs to use real world objects has to identify these objects.
Information aggregation services	These collect and summarize raw data that need to be processed and reported to the IoT application.	• Smart healthcare systems embed sensors and actuators in patients' and their medicine for monitoring and tracking purposes. Clinical care personnel monitor physiological statuses of patients through data collected, analyze them and forward to relevant persons for action.
Collaborative aware services	These act on top of Information aggregation services and use the obtained data to make decisions and react accordingly.	• Smart grids use the IoT to connect millions of electricity meters to the network of energy providers. These meters collect, analyze and control energy consumption, reduces potential failures and increase efficiency • A smart home can automatically close windows based on the weather forecast. • A smart building system can detect when an appliance is faulty and send maintenance requests automatically. • Self-driving cars are future examples of future ITS. • Industrial automation systems work by allowing groups of machines to produce products quickly and more accurately. IoT is utlized to monitor and control production line functions.
Ubiquitous services	These aim to provide Collaborative-aware services anytime, to anyone, and anywhere.	The ultimate goal of all IoT applications is to reach the level of ubiquitous services. However, there are many remaining challenges that have to be addressed. • A smart city can be seen as an application of ubiquitous services. This aims to improve the quality of life in the city in a variety of ways. Various systems employing smart technologies are interconnected to provide required services (health, utilities, transportation, government, buildings and homes)

for future IoT systems.
IoT devices currently available, and the applications they make possible will be further illustrated in a later article in this issue.

3.3.Communication

The IoT communication technologies connect different types of devices together and/ or to a central facility to deliver specific services. The important communications requirements for IoT include energy efficient operation , reliability and scalability.

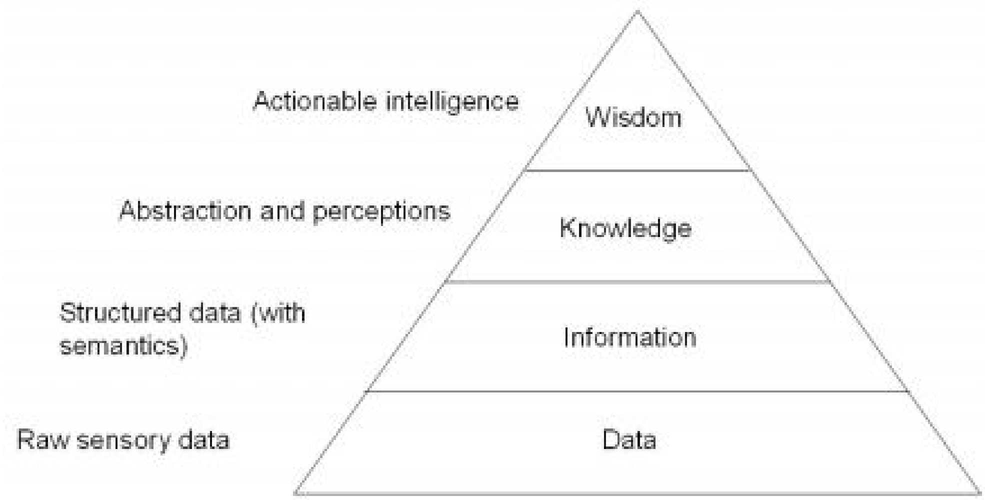


Fig. 9 : The "Knowledge hierarchy" in the context of IoT

Depending on the application, factors such as range, data requirements, security and power demands and battery life will dictate the choice of one or some form of combination of technologies.
There is a wide choice of communication options for engineers and application developers working on products and systems for the Internet of Things (IoT). Many technologies are well known, such as WiFi, Bluetooth, ZigBee (IEEE802.15.4) and 2G/3G/4G cellular. There are also several new emerging networking options such as Thread as an alternative for home automation applications, and low-power, long-range technologies such as LoRa.
In this article we look at three technologies WiFi (WLAN), Bluetooth, including Bluetooth Low Energy (BLE) and IEEE802.15.4 as options for low-power, short-range communications for IoT devices. Further information will be available in a later article in this issue.

Figure 6 compares the three most important features, power consumption, data rate and communication range of the above technologies. These provide connectivity in the "Last 100 Meters" of an IoT network.
It is clearly evident that each technology has its unique strengths and weaknesses. WiFi has the advantages of being available in mobile devices (the availability of an 'ecosystem') and high data rate, while the key disadvantage is high power consumption. BLE on the other hand is able to support lower data rates, but with significantly less power consumption. Zigbee (802.15.4) is similar in these characteristics to BLE, but has the added advantage of being able to extend network range by working in a mesh configuration. The salient characteristics of each technology and the type of applications they are most suited for are highlighted in Figure 7.

In order to enable a variety of devices with different communication technologies to communicate in an integrated manner, the evolving networking architecture for IoT is illustrated in Figure 8 for a typical Smart Home scenario. The home has an Internet router from a service provider, which provides WiFi access to devices within the home. However, WiFi is not a suitable option for IoT devices, due to its high power consumption. Therefore, the home is equipped with two miniature gateways, each communicating via BLE in the downstream with the IoT devices, and via WiFi in the upstream with the Internet router. Through this network configuration, the IoT devices are able to send/receive data to the Internet, to be used in suitable Smart Home applications. Gateways having technologies such as BLE, Zigbee and Z-wave in the downstream and WiFi in the upstream are becoming available, along with a multitude of IoT sensors/actuators.

3.4.Computation

Computation in the IoT may take place either in the devices or centrally in the cloud, or both. In the devices, computation is supported in hardware by the internal processor units (microprocessors, microcontrollers, FPGAs etc.) and memory and in software by operating systems where available. The cloud provides facilities to process big data collected from a large number of devices in real-time, and extract knowledge that is useful for all users. Thus, the Computation component powers the "brain" of the IoT system, the "brain" itself being the Semantics component to be described later.

There are several Real-Time Operating Systems (RTOS) that are suitable for IoT applications. Contiki and TinyOS are such

operating systems that have been widely used in wireless sensors, even before the arrival of the IoT paradigm. These are lightweight operating systems suitable for resource constrained (enbattery life, memory, processing power) IoT environments. Google, along with a consortium of automobile manufacturers has recently released Android Auto, to allow mobile devices running the Android operating system to be operated in automobile dashboards, to accelerate the adoption of the Internet of Vehicles (IoV) paradigm.
Cloud platforms form the other important computational part of the IoT. Connecting a large number of physical objects equipped with sensors to the Internet generates what is called "big data". Big data needs smart and efficient storage. Due to its large volume, big data needs special hardware environments and software tools to capture, manage and process them within an acceptable time. Cloud services allow users to access remote facilities to do these, and extract knowledge by complex processing of data captured through the IoT. Therefore, cloud computing presents a good choice for IoT's computational requirements.
There are many free and commercial cloud platforms and frameworks available to host IoT services such as ThingWorx, OpenIoT, Google Cloud, Amazon, GENI etc.

3.5.Services

IoT services are made available to applications. Services can be categorized under four classes, and are summarized in Table 2.

3.6.Semantics

A primary goal of interconnecting devices and collecting/processing data from them is to create situation awareness and enable applications, machines and human users to better understand their surroundings. Data collected by devices is usually multimodal (temperature, light, sound, video etc.) and diverse in nature (e.g. quality of data can vary). These make the task of processing, integrating and interpreting real world data a challenging task. This data transformation process may be illustrated using the "knowledge hierarchy" as in Figure 9.

To exploit the full potential of the IoT, we need to transform raw data into actionable intelligence (wisdom).
While "big data" solutions and cloud platforms can provide infrastructure and tools for handling and analyzing huge volumes of IoT data, we still need efficient methods and solutions that can structure, annotate, share and make sense of the IoT data and facilitate turning it into actionable knowledge in different application domains. These issues naturally lead to a semantic-oriented perspective

Table 3. Technologies for the IoT

IoT Elements		Samples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, , LTE-A
Computation	Hardware	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, Smart Phones
	Software	OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc.)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)
Semantic		RDF, OWL, EXI

towards the IoT.
The suite of technologies developed in the Semantic Web, such as Linked Data, the Resource Description Framework (RDF) and the Web Ontology Language (OWL) and semantic web services, can be used as principal solutions for IoT. Thus, semantics represents the "brain" of the IoT.
In this section, we have reviewed the main component building block of the IoT, , along with examples of available technologies and realizations in each case. Table 3 summarizes these technologies in each component.

4.Challenges of IoT

Despite the potential, positive predictions, and the glamour surrounding the Internet of Things, there are significant challenges that could stand in the way of realizing its potential benefits. Some key challenges are presented below.

4.1.Security and Privacy

The most serious of IoT challenges are security and privacy. The Physical Web could enable hackers to control our devices unless precautions are taken. It is unclear if conventional, well-established security measures that exist for the Web are suitable or even adequate for IoT applications.

Social threats can occur when information is inferred in unexpected ways. For example, the energy consumption information of a house would indicate the times at which the house is unoccupied. This information may be used to turn off unnecessary appliances in the house to save energy, and also to break into the house. Thus, it is important that the information obtained via the IoT does not fall into unauthorized hands. Movements can be tracked and activities inferred, though multiple streams of data collected from devices with and around a person without the individual being aware of it. Features of IoT that may provide a benefit to an informed user can pose a privacy problem for those who are unaware of the presence of the devices or have no influence on how the information is collected and used.

4.2.Regulatory and Legal

The IoT also poses a wide range of challenges and questions from a regulatory and legal perspective. In some cases, it may even create new legal and regulatory situations and concerns over civil rights that didn't exist prior to these devices. For instance, data collected by IoT devices on jurisdiction may be stored and/or processed in another jurisdiction. These devices use the Internet to communicate across jurisdictions, often with no technical roadblocks. Ownership and protection of data, some of which may be personal or sensitive is an issue which needs careful consideration.

4.3.Standardization

IoT solutions deliver the most value when they are connected to a web of interlinked services. For instance, a smart home solution can deliver significant value only when it integrates the electrical, safety and surveillance systems. However, IoT solutions available today, are highly proprietary, providing little support for integration of devices and services from third parties. The reason for this is the lack of standards spanning industries, vendors and products. The true potential of the IoT can only be exploited to the fullest only when such standards are available.

5.Summary and Conclusion

The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. The recent confluence of several technology market trends, however, is bringing the Internet of Things closer to widespread reality. These include Ubiquitous Connectivity, Widespread Adoption of IP-based Networking, Computing Economics, Miniaturization, Advances in Data Analytics, and the Rise of Cloud Computing.
This article attempted to provide an overview of the Internet of Things paradigm, with an emphasis on the above aspects. Elements of an IoT system, applications, and concerns/ challenges were discussed.
Subsequent articles in this issue will deal in more detail, with emerging applications, communications, networking and security aspects surrounding the IoT.

Prof. Dileeka Dias
BSc.Eng.(Moratuwa),M.S.(Calif.), Ph.D(Calif), MIE(SL), C.Eng., MIEEE
0777688861

Devices for Enabling IoT Applications

Udari De Alwis

Introduction

IoT refers to the networking of physical objects through the use of sensors, actuators, and other devices that can collect or transmit information about the objects. The term networking generally refers to connecting computers and other IT peripherals. Networking enables resource sharing and remote accessing. In IoT we are not only looking at the connecting computers about also everything around us even not limiting to physical things. IoT enable us to create a self-aware environment, very much like a Central Nervous System for the Planet Earth.

IoT technologies can be applied in almost everywhere to make the environments in which we live, work and play, smart, from smart light bulbs to net connected thermostats and from smart refrigerators which know when the supplies are running low to smart cars which can drive themselves. Healthcare/ personal care, building and home automation, smart cities, industrial automation, automotive are some of the major sectors that IoT is being applied. Figure 1 illustrates the primary application domains of IoT and possible applications within each.
This article focuses on major application areas of IoT, some emerging deployments, examples of services they can offer, and devices that are emerging to enable such applications.

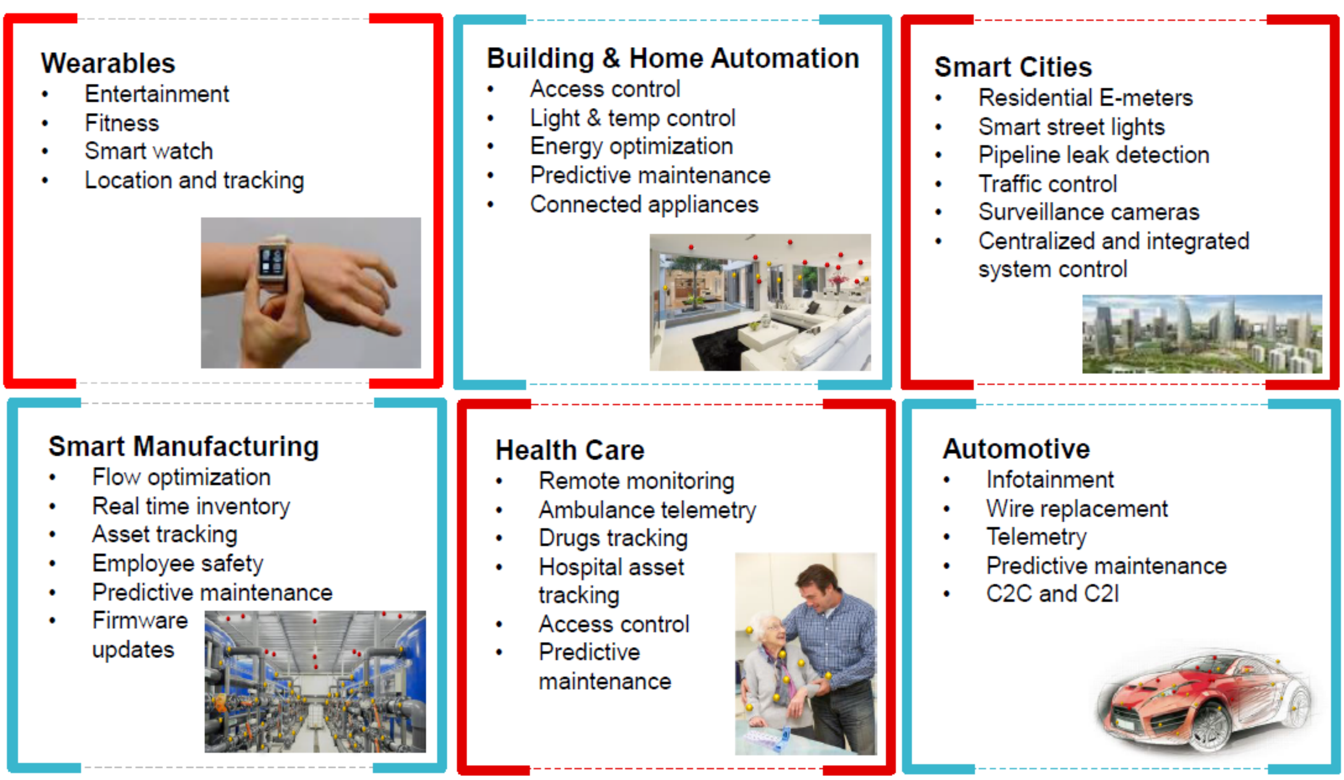


Fig. 1 : IoT Domains of Application

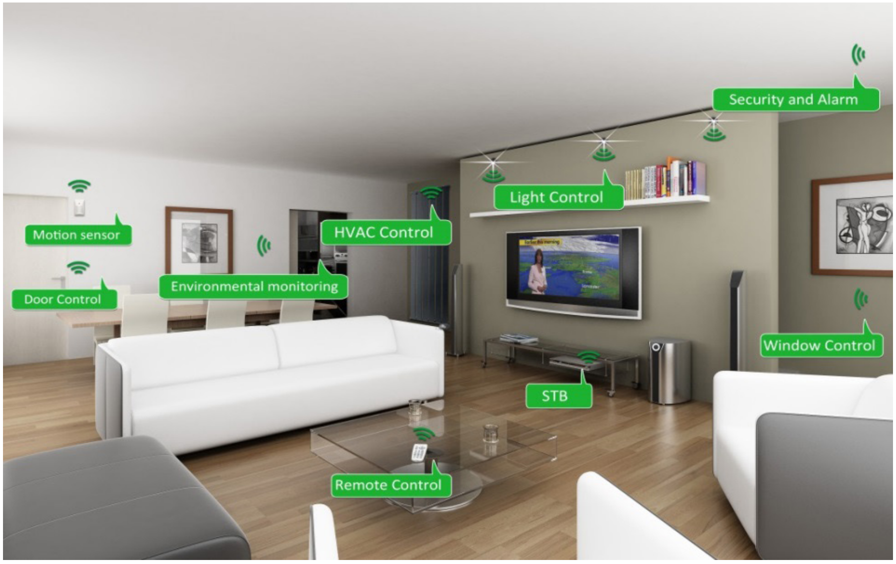


Fig. 2 : SMART home

Fig. 3 : Nest Thermostat

Fig. 4 : Philips Hue Bridge : Homekit ready

Fig. 5 : AmbiClimate: Smart add -on for your air conditioner

Fig. 6: Footbot : Indoor air quality monitor

Fig. 7 : Vivint

Devices That Enable Smart Homes

Imagine you are coming home from a long day's work. The moment you enter through your front door, the lights immediately turn on a shade past dim – just the way you like it. Your home AC has started at the time you left your office and now as you enter your home you are feeling the cooling air refreshing your body. By the time you remove your shoes, watch etc, and your clothes, your phone will beep, it's your bath room; the hot water bath has been prepared - just the way you want.

You have spent a couple more minutes in the bathroom than usual, and your favorite TV show has begun. The television has turned on and detecting your absence, has automatically started recording the program. You start to walk to the living room, but a beep from the kitchen stops you and persuades you to go there instead. It is your refrigerator, reminding you that there are some snacks readily available. You open the fridge and grab a snack. But a beep again from your wrist band interrupts you. It seems you have exceeded your calorie goal for the day, so better to go for a fruit juice. You pour out a glass of juice and something to eat. You see that a display on the outside of the fridge informs you that milk and eggs are over. You tap a button on the display and your refrigerator dials the local store on your mobile phone, for you to place an order. You place your order and make your way back to the TV and settle down to watching your program. A little while later you see a second notification that informs you that you've forgotten to activate your security system, but that it has been done for you. You silently marvel at how simple life has become as you sit back to enjoy the TV show. Speaking about this kind of a domestic bliss may once have been purely within the realm of science fiction, but with the introduction of IoT to homes/ building this is set to become a reality in the not-too-distant future. Figure 2 shows a smart home environment with numerous IoT devices to support services of the kind described above. Figures 3 to 10 show

Fig. 8 : Philips Hue : Dimmer switch

Fig. 9 : Maid : Smart Microwave oven

Fig. 10 : Pantelliget : Smart frying pan

some IoT-enabled devices that are already available in the marketplace. The benefits of the smart home are not limited to convenience, it has a great potential in making our homes greener and cheaper. Home automation systems offer us time saving: the time we can spent with our loved ones rather than attending to routine chores. Water and energy-monitoring tools, and programs to optimize energy consumption could help us lower our water and energy usage, which could in turn, lower our bills and reduce our carbon footprint.

Energy Management and IoT go hand-in-hand. In today's building eco systems, a major portion of the power is used for lighting, heating and cooling . A well connected network of smart devices which have the capability of monitoring, reporting and controlling the light, cooling and heating fixtures can not only cut down the energy consumption, but also optimize the user experience of the inhabitants by effectively using the resources.

Wearables for Health, Fitness and Safety

Longer life is a global triumph as well as a global challenge. Worldwide, the number of persons over 60 years of age is growing faster than any other age group. The number in this age group was estimated to be 688 million in 2006, and is projected to grow to almost two billion by 2050. Automation and centralized control have significant benefits for family caregivers. By integrating home healthcare equipment such as monitoring and diagnostic tools, smart homes could simplify the caregiving process for hundreds of millions of adults worldwide who care for their elderly persons Furthermore, smart homes could

Fig. 11 : Withings Activité : Activity tracker

Fig. 12 : Fitbit Flex : Activity tracker

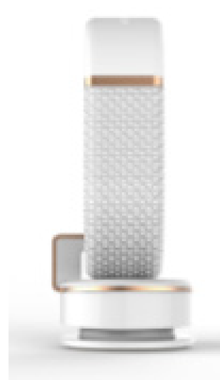


Fig. 13 : Olive bracelet :Stress management tool

Fig. 14 : MisFit : Activity tracker

Fig. 15 : FILIP : Wearable phone and locator for kids

assist independent living of the elderly and provide peace of mind to their relatives through continuous remote monitoring. Non Communicable Diseases (NCDs) are posing a great threat to human health. The busy life style with reduced peace of mind and increased consumption of fast foods have been identified as main causes for the growth of NCDs worldwide. Even though most of us know these facts, we are reluctant to change the way we live. A gentle reminder or just the impression of someone monitoring you can create the prtdusyion that one needs to change his habits towards a healthier lifestyle.

Wearable technology empowered by the IoT has created a range of applications which enable us to monitor our bodies as never before. The parameters under observation can be simple as the number of steps that you take or as complex as your blood glucose level.

Activity tracking devices have evolved from mere wrist bands to fashionable jewelry with elegant designs and sophisticated technologies to harness every movement of the body. With the use of miniaturized components such as accelerometers, gyroscopes and altimeters, these trackers have become an add-on to the daily attire for measuring the activeness of a person. The development in communication technologies such as Bluetooth Low Energy

Fig. 16 : iBabyMonitor : Digital video monitor

(BLE) has paved a pathway for these devices to engage in energy efficient communications. The advances in cell chemistry has created more compact, long lasting and lightweight batteries for wearables. Figures 11 to 14 illustrate some commercially available wearable health and fitness devices.

Like the elderly, the child population is another segment of society who needs continuous supervision from their parents. With the advancements in IoT

Fig. 17 : Mimo : Baby sleep monitor

technologies, every parent who owns a smartphone has the ability to monitor their children around the clock. A web connected camera streaming instant information on how well your baby is at home can provide peace of mind for a busy mom at work. Connected sleep monitors, temperature, humidity sensing devices can alarm the parents with the early sense of

Fig. 18 : Scully: Connected Moto cycle helmet

signs. Wearable devices specially designed for young children can be pinned to a shoe, bag or worn as a watch to enable patents to monitor their movements outside the home.

Wearables equipped with outdoor localization techniques and hazarders environment detection

Fig. 19 : Athos : Smart appeals

Fig. 20 : FieldWiz: performance measuring system for outdoor team sports

Fig. 21 : FitBark : Activity monitor for Dogs

Fig. 22 : E-Trakka : Equine Fitness Monitor

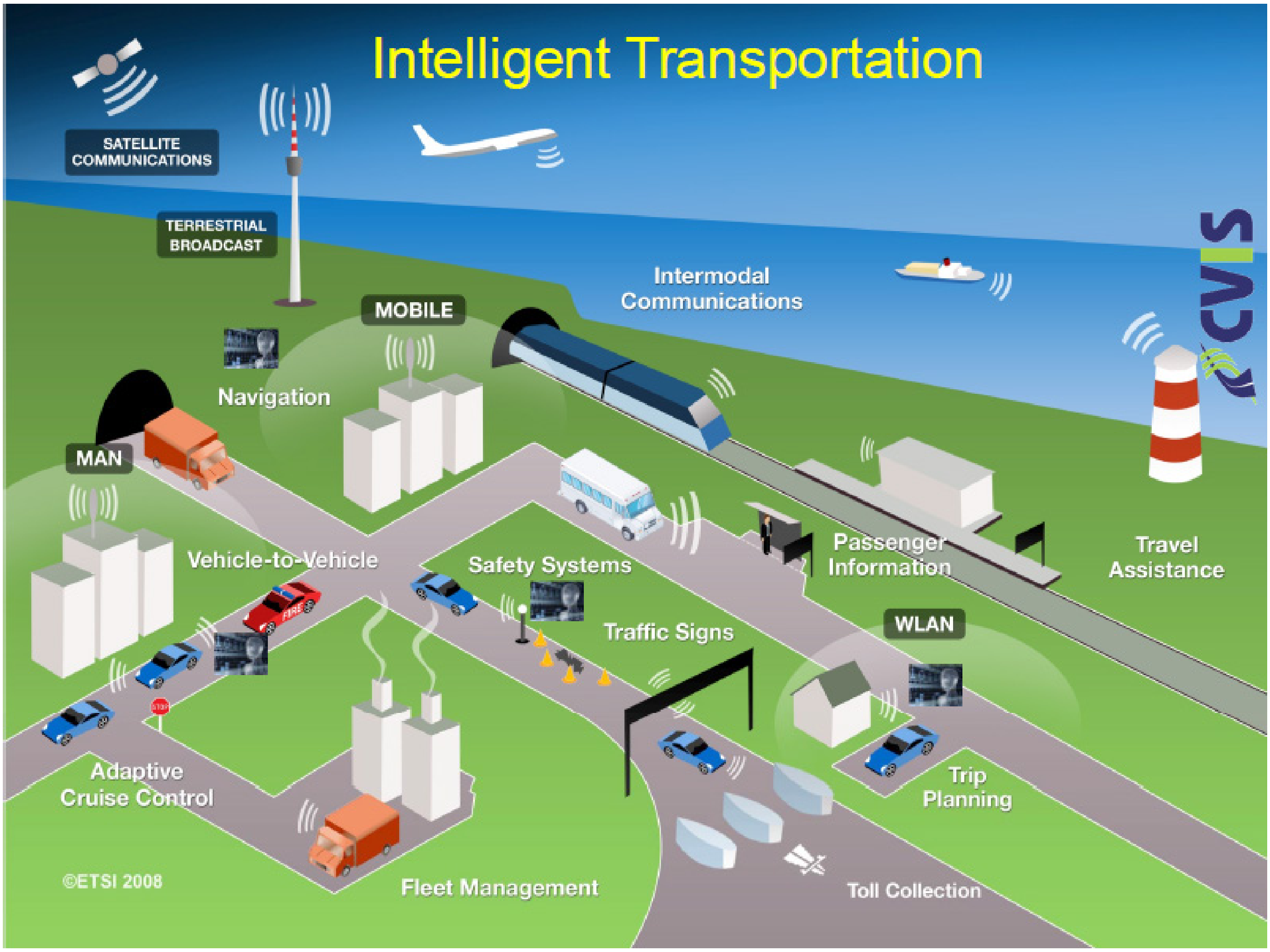


Fig. 23 : Smart Transportation system

capabilities (e.g., impact detection) combined with WiFi or cellular communications technologies can be used in applications that communicate a message that your child has had a fall at school, or that the school van's driving characteristics are unsafe, or automatically alarming early responders in case of road accidents. Figures 15 and 16 show IoT devices for infants, and Figures 17 and 18 for young children.

Miniaturization of sensors and communication hardware and advances in conductive fabric technologies have opened a new pathway to integrate electronics into the clothes that you wear. Revolutionary smart wear products have created a new era in analysis of muscle activity and heart rate in real time in everyday life. Algorithms turn this data into guidance on movement and posture which are designed to provide detailed feedback to athletes, perfecting a tennis serve or golf swing, or physiotherapy patients recovering from injuries.

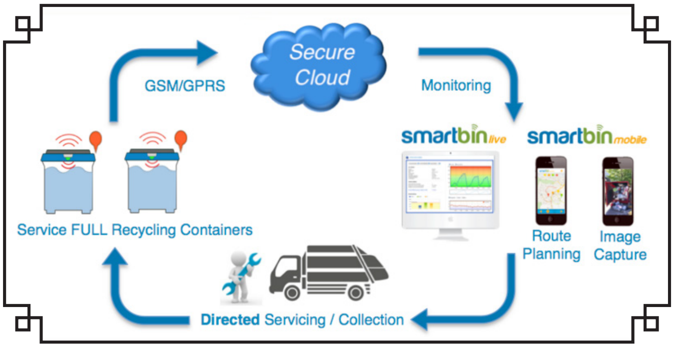
Some examples of smart wear, where the devices are integrated into clothes are shown in Figures 19 and 20. Wearables are not limited to humans. Figures 21 and 22 show wearables for dogs and horses respectively. Such devices keep track of your pet, monitor its level of activity and wellbeing, or can perform more complex analysis on animals used in sports.

Devices and Applications for Smart Transportation

Vehicles, highways and transportation are also fast becoming part of the Internet of Things, in emerging Intelligent Transportation Systems (ITS). Components of ITS include vehicle-to-vehicle and vehicle to roadside communications. Figure 23 shows an ITS scenario. On-board devices include navigation devices enabled by GPS receivers, inertial components, a variety of sensors to facilitate on-board diagnostics (OBD), proximity sensors etc. Roadside devices include traffic sensors, cameras, digital signage etc.

IoT technologies have spread to all sectors of transportation. This transformation creates many new and exciting opportunities to help save lives with improved safety on our roads, rails, waterways, airways, and public transit systems. Better asset and vehicle use, increased ridership and market share with faster travel times, and on-time delivery of people and goods are all possible today. Electric vehicles which are gaining a popular share in the market completely depend on smart devices and connectivity to provide better performance and added functionality to their owners. Smart sensors have also contributed to increasing the safety in mass transit systems such as railways. GPS enabled collision avoidance systems monitor trains in the local network and informs conductors if a train is approaching on the same track, helping the railways become even safer. Looking for a safe parking space in busy urban centers is frustrating, intensifies congestion on the roads, and increases pollution from circling cars. Sensors fixed in parking spaces can determine the availability of the parking space and transmit that information to a centralized system which can distribute the information directly to drivers, helping to guide them more quickly to an available spot, or to cities, which can use the data to adjust pricing based on demand. Of all the forms of transportation, driving remains the most dangerous. Governments around the world are exploring ways to leverage IoT to make the roads safer by connecting the vehicle and the driver with the surrounding environment. The US Department of Transportation is testing

Fig. 24 : Smart cities



the uses of vehicle-to-vehicle communication, enabling cars to sense and respond to possible risks on the road. Cities are also connecting to drivers within their cars: Walnut Creek in California has implemented a system that connects with drivers' smartphones, pushing alerts when the light changes from red to green to discourage distraction while driving.

Smart Cities, Applications and Enabling Devices

The number of urban residents is growing by nearly 60 million every year. In addition, more than 60 percent of the world's population will be living in cities by 2050. As a result, people occupying just 2 percent of the world's land will consume about three-quarters of its resources. Moreover, more than 100 cities of 1 million people will be built in the next 10 years. Today's cities face a variety of challenges, including job creation, economic growth, environmental sustainability, and social resilience. Given these trends, understanding where we are in the evolution of the Internet is critical to future city-planning processes. Smart City scenarios are shown in Figure 24. Chicago's Array of Things and Dublin's CityWatch are models for the deployment of citywide sensor networks. Partnering with research institutions and corporations, these cities are installing sensors on lampposts to monitor environmental conditions including temperature, noise, and air quality. The data collected through the urban sensor network can be analyzed in expert analysis tools to identify patterns in microclimates, and make predictions about vehicle and pedestrian congestion. Moreover the data is used to give a self awareness to the general public about the impact they are making on the environment.

Many cities face severe problems with water, irrespective of the amount of rain they get. Irrigation planning using IoT is not limited to plan and manage irrigation, but also covers areas like flooding and wastewater management during storms.

Although waste management is traditionally a hands-on service, IoT companies are developing two-way communication tools to reduce labour and increase the efficiency of waste management systems. Sensor-enabled trash receptacles measure waste levels in public bins and compact trash to reduce overflow. The bins share the data with local authorities, allowing them to enhance efficiency by planning collection routes when and where pickup is needed.

The smart grid is one of the most well-developed and widely recognized IoT systems. Smart metering is the prime component of a smart grid, which enables self-awareness among the consumer. The information collected on buildings' energy usage is fed back to a central management system, in order to efficiently allocate resources.

Concluding Comments

As IoT technologies expand, the world around us becomes smarter. However the prime question is, "is it smart enough?" In architecting these solutions, power consumption, connectivity, data security, ergonomics are some of the challenges that the designer must face. Connecting each and every object around us poses new threats to one's privacy, and doubts have arisen about organizations spying on their employees through connected devices. Technology is the only way of providing solutions to the problems created by technology itself. Today, technology is developing at a rapid pace, and there is much hope for addressing these challenges successfully.

With smart and forward-looking leadership, IoT has the potential to create a revolution in the way we live. By embracing the potential of IoT, policy makers going hand in hand with technology creators can improve service delivery, increase sustainability, and make the world safer and a more livable place for all living beings.

Udari De Alwis
B.Sc. Eng. (Moratuwa)
Research Engineer,
SYNERGEN Technology Labs (Pvt) Ltd.
Sri Lanka.
0774324231

Low Power Wireless Communication for the IoT

Nadee Seneviratne

According to the Internet Society, we can to have 100 billion connected IoT devices with a global market value of more than $11 trillion by 2025. The IoT, which strives to utilize the advancements in computational power, miniaturization of electronics, and network interconnections to create newer capabilities, will have a strong transformation in the way we live. This article introduces several wireless technologies that enable the IoT.

One of the key challenges of IoT is the requirement of low power wireless communication with the connected devices. Through this article, the reader will be able to understand the need for low power wireless communications and the related emerging wireless technologies to satisfy this need. It will also discuss the suitability of these technologies in various scenarios using several case studies.

Why low power wireless communication?

The range of applications proposed for the IoT is impressive. While it is obvious that to enable all these applications ranging from smart cities to personal health, wireless connectivity among the objects are needed, a common attribute for all is the limited power available in the devices to maintain their functions. Most of the sensing devices run on battery power and thus, the ultimate objective would be to maintain a longer battery life, preferably the life time of the device. Also, the available power should be consumed optimally. Therefore, it is necessary that, communication protocols being deployed in these networks operate under low power and with efficient energy consumption.

There are a number of emerging connectivity technologies that are promising for deployment in IoT networks. Yet, careful consideration should be paid to the context of the application. Low power wireless communication standards are emerging day by day to support the varying range of requirements for the IoT, in terms of security, data rate, and transmission distance requirements. Energy harvesting is another option being looked at in IoT applications to further optimize energy utilization in devices.

Low Power Wireless Communication Technologies

A network's range is typically categorized into four classes as Personal Area Network(PAN), Local Area Network (LAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN). PANs usually cover a range of 10m whereas, LANs could go up to a range of 100m. NANs can reach a range over 25km and as the name implies, WANs spread across a very large area as big as the entire globe. Wireless communication protocols are available to cater to the demands of all these types of networks.

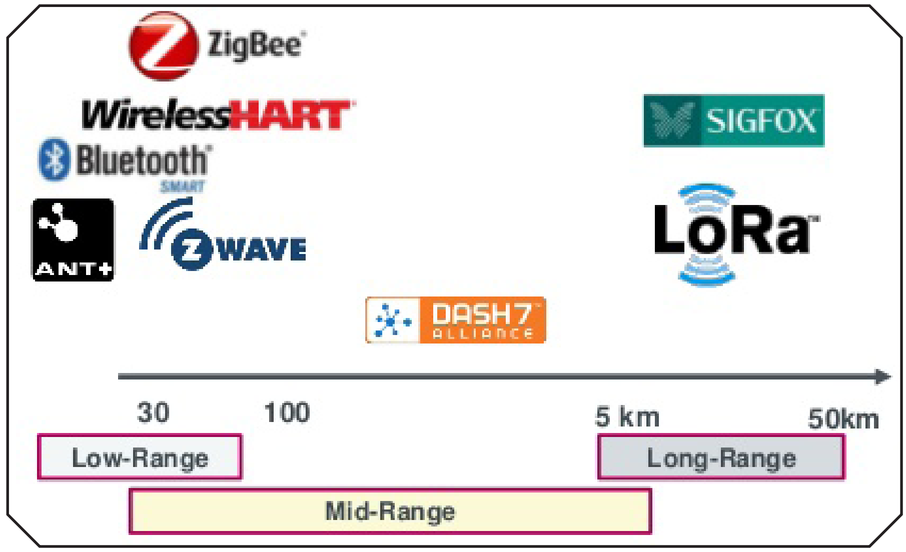
Among the most commonly heard wireless connectivity protocols is the Wi-Fi technology (for LANs), developed based on the IEEE 802.11 standard. Wi-Fi standards are so prevalent around the globe due to its favorable features like mostly operating in the ubiquitous unlicensed frequency band of 2.4 GHz, strong indoor coverage helping homes and enterprises connect a number of devices wirelessly, and the typical data rates of 150-200 Mbps. However, these benefits come at the cost of high power consumption. Wi-Fi may not be the feasible solution to operate a battery powered device in an IoT application. On a positive note, several silicon devices are being developed now to integrate Wi-Fi

into IoT applications with limited power consumption (e.g.: Texas Instrument's CC3200)
The following technologies are popular low power wireless communication protocols and thus are ideal candidates to be deployed in suitable IoT scenarios.

Bluetooth Low Energy (BLE)

BLE, also known as Bluetooth Smart, is the latest addition to the classic Bluetooth standard which has been available since 1994. This is specifically designed to cater to the demand of low power wireless connectivity among IoT devices. Bluetooth is a short range wireless communication standard. The conventional usage of Bluetooth includes tasks such as audio or data streaming, where a large amount of data is transmitted and frequent communication happens between the two connected devices. BLE helps to expand its applications in short range communications where it can now be deployed in power constrained devices such as wireless sensors and controls which on the other hand transmit small amounts of data and communicate infrequently (Eg: Wearable health tracking devices).

Life time of a low power device is increased by BLE via 3 mechanisms. It uses a simple device discovery method, maintain power efficient peak, average and idle modes and ensures reliable transmission of data. BLE supports



only 40 channels compared to 79 in Bluetooth Classic, which results in significant reduction time in connection set up. Out of the 40 channels of BLE, 3 are advertising channels which helps to discover devices and establish the initial communication between the devices. Robustness of the advertising channels are maintained by selecting the channels which have the least amount of interference from Wi-Fi channels. As a result, BLE has to be switched on for just 0.6 to 1.2ms to scan for other devices. BLE generally uses a client/server model where in order to connect the devices, when the client receives an advertisement packet, it sends a connect request to the server. Once the advertiser receives that, the devices will be connected enabling data exchange.

BLE uses a modulation technique which has low power consumption. Data channels can perform bidirectional communication between the connected . BLE can cover a range of about 150m (open field). As BLE is specifically designed to small amounts of data from time to time, unlike Classic Bluetooth, BLE remains in sleep mode until a connection is initiated.

The actual connection times of BLE is said to be very low around 3ms, whereas for Classic Bluetooth it can take up to around 100ms. BLE maintains a lower packet overhead which also contributes to lower power consumption.

Internet Protocol (IP) support was added to Bluetooth Smart in its latest version, allowing BLE sensors to access the internet directly via 6LoWPAN connectivity (described later). As a result, existing IP infrastructure could be used to manage Bluetooth Smart 'edge' devices.

Some applications suitable for BLE include blood pressure monitors, wearable activity and performance trackers (e.g. Fitbit), industrial monitoring sensors, geography-based, targeted promotions (iBeacon), and Public transportation applications. A major strength of BLE is that it is supported by smartphones.

ZigBee

The specialty of ZigBee, which is implemented based on the IEEE 802.15.4 standard, is that it can work in a mesh network configuration. In a mesh, data can 'hop' from one device to another throughout a large scale network until it reaches the destination. ZigBee is known to be a low-throughput, low-power and low-cost technology which operates in the 2.4 GHz ISM band. It is most commonly used for personal or home area networks and also in a wireless mesh for networks that operate over longer ranges. According to specifications, ZigBee can deliver a throughput of 250 kbps, yet typical usage is at lower data rates. ZigBee's ability to maintain very long sleep intervals and low operation duty cycles benefit the IoT devices to be powered by coin cell batteries for years. The technological enhancement to ZigBee standards are now enabling even energy harvesting techniques for battery-less operations. The coverage range of ZigBee could be from 10m to 100m.

ZigBee Remote Control (RF4CE) profile is said to provide several advantages to complex designs as a result of its favorable features such as low-power operation, high security, robustness and high scalability with high node counts. In fact, it is said that any device in a ZigBee network can connect to a maximum of 254 devices where the size of the entire network could be up to 655535 nodes. These features have paved the way to make ZigBee a popular candidate for applications such as smart energy, home automation and in lighting control applications. As ZigBee is not supported in mobile phones, and cannot easily communicate with IoT protocols, it requires an application-level gateway connect to with TCP/IP networks.

IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)

This standard has utilized the larger addressing space of IPV6 which offers approximately 5 x 1028 addresses so that even the smallest devices with limited processing ability can transmit information wirelessly using an internet protocol. Also, a 6LoWPAN device can communicate with any other IP based device on the internet including Ethernet and Wi-Fi. Another reason to use IPV6 over IPV4 is its capability of built-in support for network auto configuration.

Created by the 6LoWPAN working group of the Internet Engineering Task Force, this was formalized in 2011. 6LowPAN is an open network protocol (similar to HTTP, UDP and TCP etc.) that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. Utilizing the advantages of 802.15.4 such as mesh network topology, large network size, reliable communication and low power consumption along with the added benefits of IP communication, 6LowpAN is well suited for the designs with Internet-connected sensors and other low data throughput and battery-operated applications.

LoRaWAN

As the acronym 'LoRaWAN' is derived from the term 'Long Range', it implies that it caters to a crucial concern in the context of IoT which is enabling communications over long ranges at very low power levels. LoRaWAN™ specification comes under low power wide area network (LPWAN) category, which makes it ideal to be used for battery operated wireless devices in regional, national or global levels. While the range of LoRaWAN in urban areas will be 2-5km, in suburban areas it can be extended up to a distance of 15km. The network architecture of LoRaWAN is a star-of-stars topology where gateways act like bridges which relay data between end devices and a central server. Gateways and central network server is connected via IP connections whereas end devices perform single hop wireless communication to one or many gateways.

Different frequency channels and data rates are there for communication between end devices and gateways. The selection of the proper data rate is based on the compromise of message duration and the communication range. Data rate of LoRaWAN varies from 0.3kbps to 50kbps.

Technology (IEEE standard)	ZigBee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11a/b/g/n	UWB 802.15.3
RF frequency	868/ 915 MHz, 2.4 GHz	2.4 GHz	5.8 GHz-a 2.4 GHz- b/g/n,	3.1 to 10.6 GHz
Data rate (Mb/s)	0.25	1″3	11″105	110″1600
Range (m)	10″100	10	10″100	4″20
Useful BW (MHz)	0.6	1″3	20-40	120″1000
Power consumption	Very low	Low	High	Low
Advantages	Power, Cost	Cost, Convenience	Speed, Flexibility	Data capacity

The battery life of end devices and the network capacity is optimized by means of an Adaptive Data Rate (ADR) scheme, in which the network server manages the data rate and RF output for each end device individually.

With low power and long range capabilities along with the ability to connect millions of devices, LoRaWAN is a promising technology to be applied for various IoT applications. Very few proposed examples are, smart metering, inventory tracking, vending machine data and monitoring, automotive industry, and utility applications.

Among the pioneering technologies being developed upon the base of LoRaWAN is the Symphony Link by Link Labs which currently supports up to 250,000 end points.

Z-wave

A strong competitor to ZigBee, Z-Wave is another RF communications technology designed specifically for control, monitoring and status reading applications in residential and light commercial environments. Z-Wave can support full mesh networks. As it operates on the sub-1GHz band, it is less vulnerable to interference from wireless technologies operating the ubiquitous band of 2.4 GHz (Wi-Fi, Bluetooth, and Zigbee etc.). Z-Wave supports data rates up to 100 kbps and is optimized for reliable and low-latency transmission of small data packets. The typical range covered by this protocol is about 30m while it is highly scalable to enable control of up to 232 devices.

Summary

This article discussed five wireless technologies considered to be prime candidates for the IoT in different situations. All have low power communication as a basic feature, while each has its own additional strengths as summarized below.

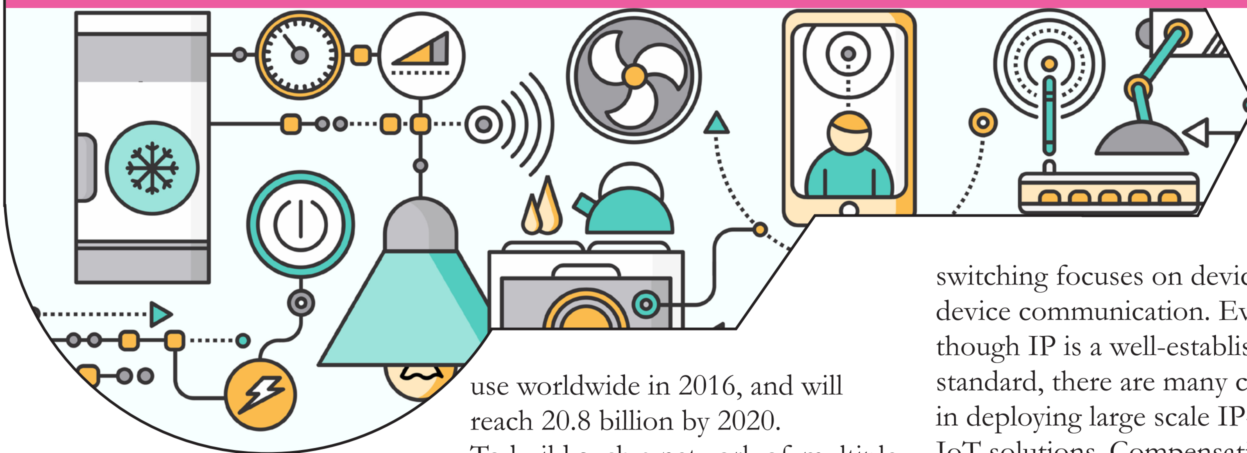
• Bluetooth Low Energy (BLE) has the strength that it is supported by all modern smartphones. Hence IoT devices have a convenient gateway to the Internet through smartphones.

• The strength of Zigbee lies in its support for mesh networking. Multi-hop networks can be implemented covering a long range, with each node supporting only short range communications.
• 6LowPAN has the advantages of addressing a huge number of devices through IPv6, and being able to directly communicate over the Internet without the need for a gateway.
• LoRa's special strength is long distance communication at low power.
• Z-wave has a large commercial device base, and operates outside the 2.4 GHz ISM band, thus avoiding interference from a multitude of applications operating in this band.

Nadee Seneviratne
Lecturer
Department of Electronic and Telecommunication Engineering
University of Moratuwa
0716261687

Information Centre Networking for the Internet of Things

Shashini De Silva



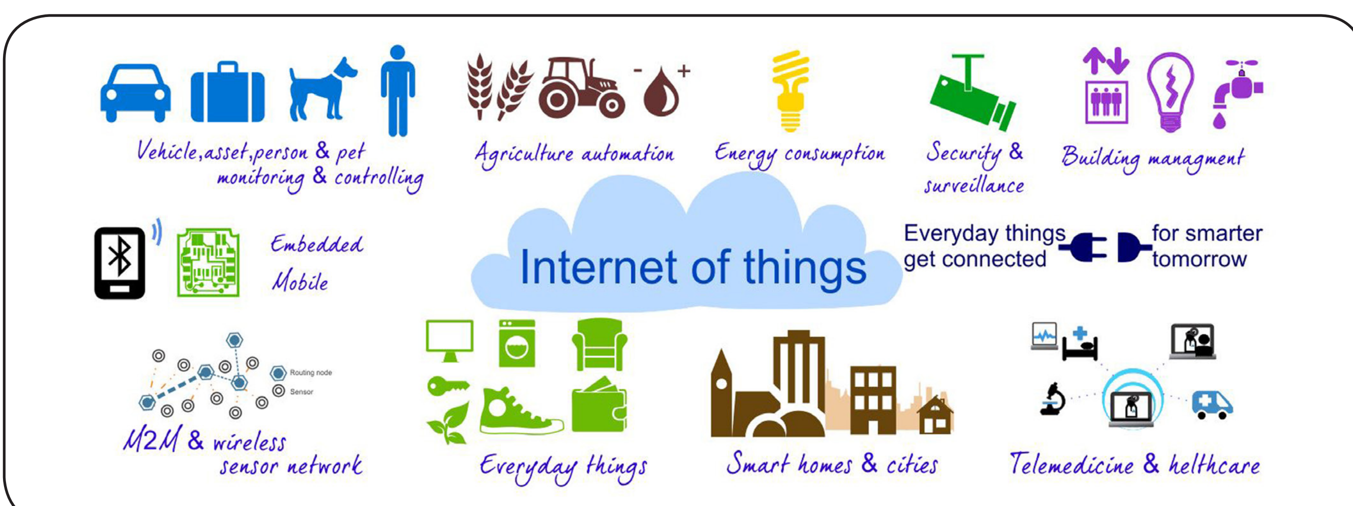
Introduction

Internet of things (IoT) is the network of physical objects embedded with electronics and software which enable them to exchange data. IoT turns these every-day physical objects into smart "things" which sense, understand and react to certain phenomena. Due to low cost sensors/actuators, and the advancement in wireless technologies, the number of "things" connected have rapidly increased over the past few years. According to forecasts of Gartner Inc. the world's leading technology research advisory company, 6.4 billion connected things will be in use worldwide in 2016, and will reach 20.8 billion by 2020.

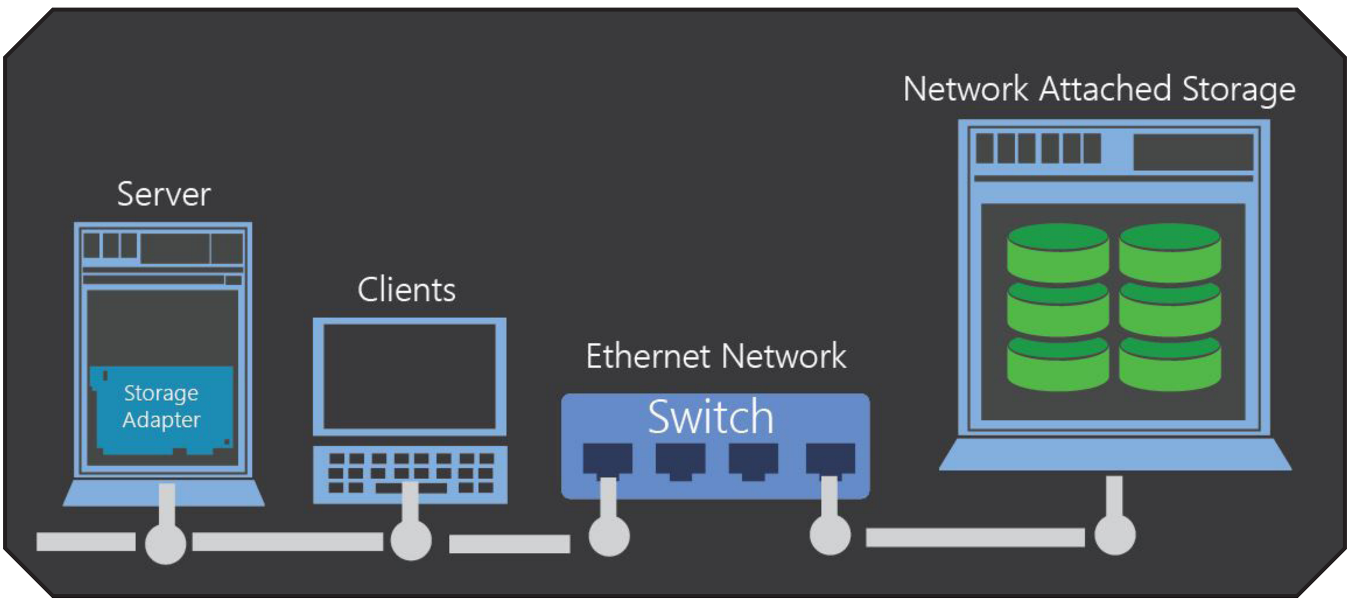
To build such a network of multiple things, many different networking solutions have been proposed. The most common approach is using packet switching networks based on the Internet Protocol (IP). Each device in such networks has a unique numerical label assigned to it called the IP address. Packet switching breaks data into suitably sized blocks, called packets. Each packet is composed of a header containing destination IP address and payload which is the data block required to be transmitted. At the receiver, all the packets are collected in the order they were sent from the transmitter and the payload is bundled together in order to retrieve the original transmitted data. Hence packet switching focuses on device to device communication. Even though IP is a well-established open standard, there are many challenges in deploying large scale IP-based IoT solutions. Compensating mobility, scalability, device to device communication security are a few of them.

The Information Centric Networking Concept

Information Centric Networking (ICN) is the most recently considered networking approach for IoT to overcome such challenges. With IoT, networks are more concerned with connecting people to information such as video, audio & web sites rather than connecting people with other devices. Their requirement is to access specific content, rather than identifying a server where that content resides. In contrast



to packet switching where packets are the basic unit of work, ICN consider content as the basic unit of work. Each piece of content has a unique name which makes content directly addressable and routable. Hence end points communicate using named content instead of IP addresses.
Each content object has a name and a custodian, a known location where content resides. When a content request is first generated by an end point, it is forwarded among content routers towards



the custodian. Each router has a separate memory called cache to store pieces of content which pass through the router to their content requesters. Hence before forwarding content requests to their custodian, routers first check whether the requested content is available in its cache. If so, the router itself provides the required content to the content requester. If not, the request will be passed on towards the custodian. When content is transmitted from custodian to requester, it is cached at content routers along the path. Fig. 1 shows a simple 5 node network which uses the ICN approach. Node 'D' and node 'E' are custodians who permanently store content 1 and content 2. Here node 'A' requests for content 2 from custodian node 'E'. This content request is first sent to router 'C'. Since content 2 is not available in 'C' router's cache, it forwards the request to node 'E'. Node 'E' will send required content to node 'A' through router 'C'. On this return path content 2 will be stored in 'C' router's cache. Now if another content request was generated from node 'B' requesting content 2 from custodian node 'E', router 'C' will provide requested content directly without forwarding the request to custodian 'E' because content 2 is already stored in its cache.

Benefits of ICN in the IoT

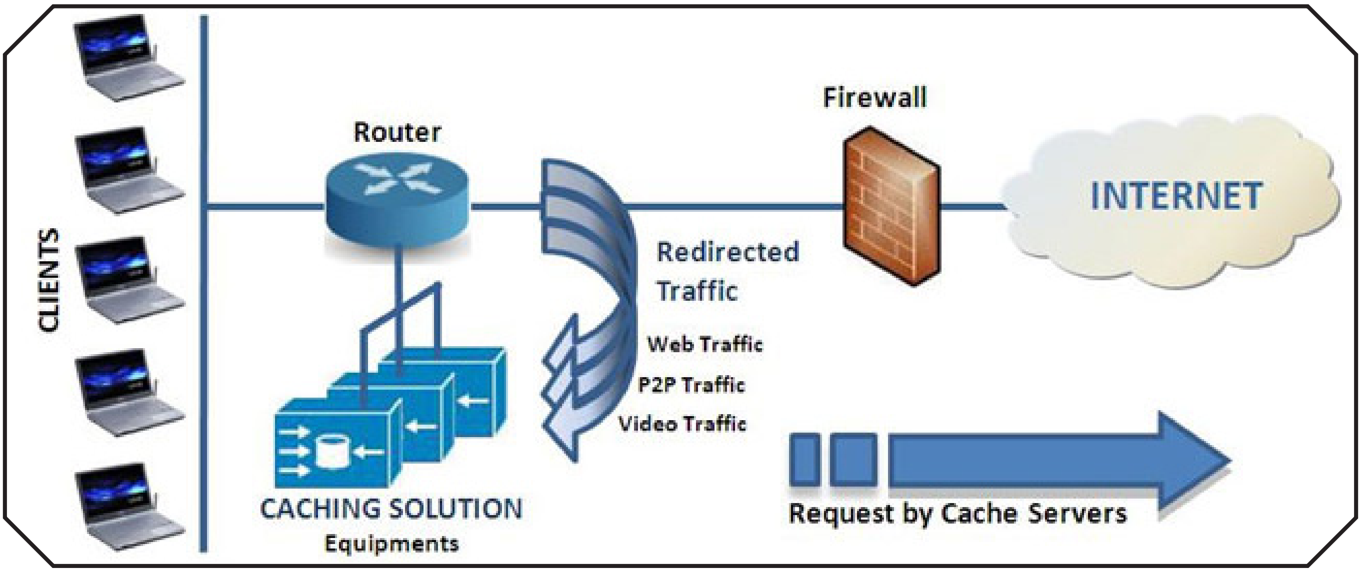
Since the IoT is a dynamic system of interconnected devices with ever increasing intelligence that generates massive amounts of data, it is naturally inclined towards the concept of centralized content. There are many benefits as well as challenges identified by research done on integration of ICN and IoT.
Location independent routing and in-network storing are the two major features in ICN which is advantageous when deployed in the IoT.

Location Independent routing:

Due to ICN's ability to name data independently from the location at which it is stored, routing in network happens based on named content requests rather than location addresses. This is beneficial in IoT since it focuses mainly on distributing content in a heterogeneous network instead of establishing communication links between two devices. This makes it easy to distribute constantly generated streams of data from a group of sensors among a variety of devices.

In-network storing:

ICN routers include cache memory to store traversing content while it is transmitted from its permanent



location to content requester. Such stored content can be used later if the same content is requested again by another device in the network. This prevents unnecessary data transmission in the network which in turn decreases the energy consumed by the devices in the network. On the other hand, in-network storage decrease end to end delay which occurs when retrieving data. Hence using the ICN approach in the IoT saves wireless bandwidth, battery power of devices and decreases transmission delay.

Both of these features together support mobility and scalability in a network. The IoT network may contain many dynamic devices and data objects. Consumers or sensors/actuators might relocate or can be constantly moving (e.g. vehicle traffic monitoring). When ICN is used in IoT, content requests of dynamic "things" can be satisfied without the need to perform registration or configuration. This also simplifies scaling up the network. Adding or removing a node becomes easy with ICN. The distributed nature of content in the network also establishes reliable communication when a few nodes in network are malfunctioning or when channel conditions are poor.

Challenges of Using ICN in the IoT

On the other hand, there are several challenges in using ICN in IoT applications.

Naming:

For proper operation of the ICN network, it is important to have a unique, pertinent name to identify devices in the network as well as content generated by those devices. Identifying each device uniquely is required in an IoT network in order to control and monitor them individually (e.g. switch on/off actuators, administrative operation).These names must relate to location, task/service or other relevant attribute.

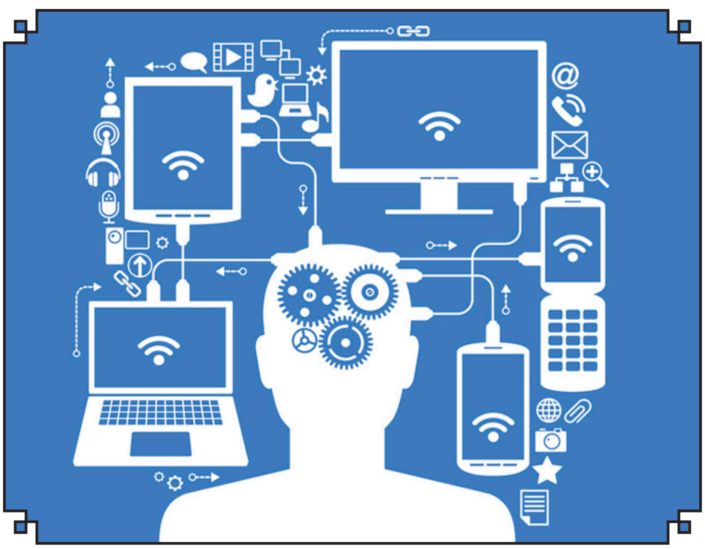
For example in the naming scheme for a smart home has defined two different sub classes for namespaces: (i) Configuration and management namespace, identified by prefix/conf. This is used for home network initialization, configuration updates and management operations. (ii) Task namespace, identified by prefix/task, used to identify and enable control and monitoring operations. Here each home is given a 'homeID' which is related to either the location of the house or owner identification number.

A configuration and authorization manager is in charge of registering devices to the network by assigning namespaces under which they can operate. A content object with the name bobHouse/task/action/light/on/kitchen is issued to require the kitchen light fixture to turn on in bob's house. When the task is completed, the end device can also send packets with the same name with the payload indicating whether the task is successfully completed or not.

This unique naming might cause unacceptable size of content names. Usually in IoT, sensors and actuators generate/use very short amounts of data (e.g. Boolean value to switch on/off an actuator, integer containing a temperature reading). For this reason, many existing naming schemes assign longer names to the content object than the actual data encapsulated inside it. In this has been overcome by keeping a dictionary to store long names and map them in to shorter name versions to be used locally in the network.

Caching Management:

As mentioned earlier, distributed caching is a key opportunity with ICN based IoT network. But it must be carefully designed to fit with IoT network application, type of data exchanged and the capabilities of IoT nodes. When the same content is requested frequently by many consumers, the network can benefit from caching.



However distributed caching mechanism is not useful if content is requested only once.
Another issue with caching occurs when data is frequently updating. Caching such data with short time validity might cause distribution of outdated content. For example, temperature of an oven may change rapidly, generating temperature content objects every second. If routers cache temperature content objects, the temperature value contained in the payload might not be the current temperature value of the oven. In using a time-stamp field when naming content object or appending a version tag to the name has been suggested to overcome this challenge.

Depending on the type of service required, even the same sensor can send content objects to different consumers at different rates.
As mentioned in, a temperature sensor in a smart home can send temperature information every 20 seconds to the fire alarm system, every 5 minutes to the heating system and a few times in a day to the house owner. Here it is suggested that it is reasonable to keep a single node in charge of caching data originated by set of devices under its control. This node will supply necessary content on its devices to applications which requests them.

Security:

The information-centric approach is based on the idea of securing information objects rather than securing the communication channel between a pair of nodes. ICN naming strategies guarantee data integrity since given data corresponds to the name with which it was addressed. Apart from this signed data, some sort of authentication is required to make sure that devices in the network are handled only by authenticated users. Especially when content is used to operate devices in the network it is essential that only trusted people do so. This issue has been addressed in the lighting control system in. It sends commands to operate lighting fixtures as content objects protected with a private key. If it is successfully verified, the task can be performed. As in the case with assigning long names to short content messages, here also there is a cost of authentication in terms of computation and delay.

Summary

This article introduced the concept of Information Centric Networking, and its use in the Internet of Things. While the IoT is enabled by a large number of versatile devices, applications deal with information (i.e., content, rather than the devices in the network. As such, ICN is well suited for IoT. ICN has the ability to convey information over the IoT in a bandwidth-efficient manner and with low delay. However, naming of content/devices, in-network caching of dynamic information, and security of the content remain as challenges.

Ms. Shashini De Silva
Lecturer
Department of Electronics and Telecommunication Engineering,
University of Moratuwa
0715647126