Australian Journal of Telecommunications and the Digital Economy

Enabling Technologies for Effective Deployment of Internet of Things (IoT) Systems:

A Communication Networking Perspective

Jamil Y. Khan
Dong Chen
Oliver Hulin
School of Electrical Engineering & Computer Science
The University of Newcastle

Summary: The demand for IoT (Internet of Things) systems that encompass cloud computing, the multitude of low power sensing and data collection electronic devices and distributed communications architecture is increasing at an exponential pace. With increasing interests from different industrial, business and social groups, in the near future it will be necessary to support massive deployment of diverse IoT systems in different geographical areas. Large scale deployment of IoT systems will introduce challenging problems for the communication designers, as the networking is one of the key enabling technologies for the IoT systems. Major challenges include cost effective network architecture, support of large area of coverage and diverse QoS (Quality of Service) requirements, reliability, spectrum requirements, energy requirements, and many other related issues.

The paper initially reviews different classes of IoT applications and their communication requirements. Following the review, different communications and networking technologies that can potentially support large scale deployment of IoT systems for different industrial, business and social applications are discussed. The paper then concentrates on wireless networking technologies for IoT systems with specific focus on deployment issues. The deployment discussion concentrates on different IoT systems QoS and networking requirements, cost, coverage area and energy supply requirements. We introduce a sustainable low cost heterogeneous network design using short range radio standards such as IEEE 802.15.4/Zigbee, IEEE 802.11/WLAN that can be used to develop wide area networks to support large number of IoT devices for various applications. Finally the paper makes some general recommendations towards sustainable network design techniques for future IoT systems that can reduce the OPEX and CAPEX requirements.

I. Introduction

The Internet of Things (IoT) concept introduces a new and ubiquitous computing, and communication paradigm where smart objects can exchange information to support intelligent applications in an autonomous manner. Without human intervention, smart objects located in various application domains could interact with each other to accomplish

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.65

many tasks, ranging from health care to a simple ON/OFF activity of a light bulb. According to the Institute of Network cultures, an IoT is defined as "*a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols, where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*" (Atzori 2010: 2787-2805), (Xu et al 2014).

Advances in the semiconductor, computing and communication techniques have empowered embedded wireless computing to support evolutionary new networking architecture that could meet IoT requirements in a seamless manner. It is now evident that in future IoT applications will be deployed in almost all segments of the modern society and industry to carry out a wide range of activities. Hence, it is critical to change the fabric of the key communication infrastructure of the Internet to enable seamless communication among the intelligent devices. Such changes will be a paradigm shift from human-to-human communication towards intelligent machine-to-machine communication. The conventional concept of the Internet as an infrastructure network reaching out to end-user terminals will fade, giving rise to an interconnected scenario where smart objects will use pervasive computing environments (Jin et al 2014: 112-121). IoT applications will spread in many existing and new ICT (Information and Communications Technology) areas including those where the Internet has not yet reached. The application requirements will therefore significantly diversify, requiring embedded intelligent network architecture.

The IoT concept introduces a major shift in ICT areas where, instead of connecting end-user devices, the physical objects will connect with one another and interact with anything. The concept of interconnected objects was developed from the deployment of RFID (Radio Frequency Identification Device) for automatically identifying and tracking objects. The idea was supported with the emergence of wireless sensor networks in the mid to late 1990's where advanced monitoring applications emerged (Miorandi et al 2012: 1497-1516). Embedded computing and low power wireless communication devices efficiently support connectivity among intelligent objects. Recently, the concept of IoT has further advanced into the Internet of Nano Things (IoNT) (Akyildiz & Jornet 2010: 58-63), (Balasubramaniam & Kangasharju 2013: 62-68). The IoNT concept has been labelled as systems where miniature, possibly passive sensors in some cases, interconnected through nano-networks could obtain fine grain data from hard-to-access locations such as the human body or inside complex machines. Some of the leading ICT companies such as Cisco, IBM are now pushing the boundary of the IoT to call the area as the IoE (Internet of Everything), which is a further generalisation of the IoT concept.

Application domains of the IoT or the IoNT are not limited by current-day applications only; they will evolve as the enabling support infrastructure improves. The IoT will be an enabler to many application domains, including supply chain management, transport and logistics, manufacturing, aerospace and automotive, healthcare, security and safety, social services, etc. According to analysts, 50 to 100 billion devices will be connected by the Internet by the year 2020 (Mobile world). The global market for sensors is expected to increase to US$91.5 billion by 2016, representing a compound annual growth rate of 7.8% (Zaslavsky 2013). The IoT application domains will come in different sizes and shapes that generate small to massive amount of data. For example, a Boeing jet could generate 10 TB (terabytes) of data per engine every 30 minutes. In an aircraft, although the physical size of a network could be small, the number of data generators could be massive.

On the other hand, a smart electricity grid system may cover a very large geographical area (distribution area), but the sensor density and data volume may not be as high as that in an aircraft network. This necessitates the development of enabling technologies to support such future systems. One of the key enabling technologies of the IoT is the communication network that allows flows of information among different entities (Kim et al 2014: 61-76). This paper focuses on the design of communication networks for future IoT systems that could be deployed in different industrial and social sectors.

The paper is structured in the following manner:

- Section II reviews several major IoT applications and their deployment scenarios to develop the design needs for communication networks.
- Section III reviews different possible communication network structures based on current and emerging standards for various IoT systems.
- Section IV presents a low cost heterogeneous network for distributed IoT applications. This section also discusses the energy requirements for the IoT communication networks and present a new heterogeneous networking algorithm and firmware design.
- Section V presents some simulation and test bed measurement results for IoT communication systems.
- Finally, conclusions are presented in section VI.

II. IoT Applications and Systems

In 1999 Kevin Ashton first proposed the concept of the Internet of Things (IoT) that quickly gained popularity among researchers and various technical forums (Zaslavsky 2013). The IoT concept came into the industrial limelight when the International Telecommunications Union (ITU) published the first report on IoT in 2005. Since then, the concept of IoT has been embraced by researchers, various standards bodies such as the Institute of Electrical & Electronic Engineers (IEEE), the European Telecommunication Standards Institute (ETSI), the Internet Engineering Task Force (IETF), the ITU and many other national and international organisations.

In recent days, many international research programs have been initiated, e.g., EU framework FP7 program, National Institute of Standards and Technology and National Science Foundation (NIST) in the USA. Rapid development of low-power electronics, communication technologies and data analytic techniques allowed widespread deployment of IoT applications and systems.

According to Gartner, a leading international Information Technology research company, the number of installed IoT connected devices will reach 26 billion by 2020, up from 0.9 billion in 2009 (Gartner IoT 2013). According to Cisco, the number of internet-connected devices has reached 8.7 billion in 2012 (Forbes 2013). Connected IoT devices are utilising the machine to machine (M2M) communication architecture for the connectivity. The first generation of IoT applications was based on the Radio Frequency Identification (RFID) technology for logistics, retail and similar other sectors. The IoT applications later integrated with cloud computing and wireless sensor network architecture. The main components of an IoT system are smart devices, distributed computing capabilities and seamless communications capabilities as shown in figure 1. A smart object can be characterised by the following attributes (Miorandi et al 2012: 1497-1516).

- It has a unique identity, which is addressable by other autonomous devices.
- The object can autonomously connect with other devices and can execute certain tasks.
- It has computing capabilities to accomplish certain tasks either in a standalone or in a cooperative manner.
- It may possess some capabilities to sense surrounding physical environments and/or phenomena or can trigger certain processes based on its sensing capabilities. The triggered processes either could reside within itself or could exist in a distributed fashion.
- Some of the objects may have to roaming capabilities supporting mobile applications.

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.65

The above general attributes could be used in different IoT applications ranging from simple applications such as sensor-based light ON/OFF to control of autonomous connected vehicles on public roads to improve the reliability of future transportation systems. Market sectors and application areas of the IoT are quite large and will expand with time. It is not possible to describe all areas; however, here we can group these applications into a number of major categories and characterise the areas in terms of their communication needs. IoT application and market sectors can be grouped into following seven categories (Atzori et al 2010: 2787-2805). Each of the categories of applications is summarily described below.

- Smart home/buildings
- Smart City
- E-Health and medical systems
- Road traffic and transportation systems
- Environmental monitoring
- Business inventory and product management
- Industrial automation and manufacturing

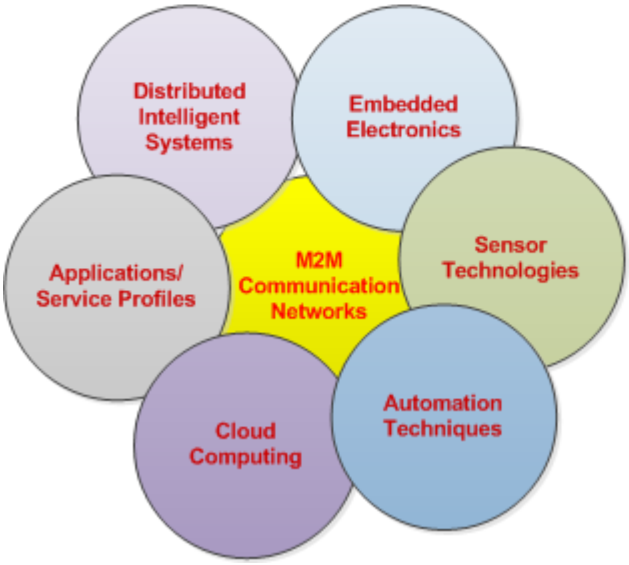

Distributed Intelligent Systems
Embedded Electronics
Applications/ Service Profiles
M2M Communication Networks
Sensor Technologies
Cloud Computing
Automation Techniques

Figure 1: Basic building blocks of IoT Systems.

Smart home/buildings: IoT devices and networks could be deployed in homes and/or in large buildings. Sensor devices can be installed inside homes or buildings to implement energy efficiency, security & safety applications, appliance control using home area networks (HAN) and many other applications (Sterling & Tareter 2009: 281-326). Most of the applications are sensing and monitoring; however new applications are emerging to support network-connected devices as can be seen in a smart grid environment. Some advanced smart home appliances could use connectivity to get locally generated information from onsite renewable energy generators to schedule the operation of appliances. Most of the applications in this environment will operate in either local area or personal area networking (LAN/PAN) environments with short transmission distance between nodes. Appliances within a HAN could use the smart meter as the gateway/router for connections to implement demand management system by exchanging data with the electricity company server.

Smart City: A smart-city based IoT system will encompass many utility services, where many providers could offer advanced services. This environment can be seen as a cyber-physical eco-system where advanced communication and computing infrastructure will be necessary to support services. Services in this environment could include road traffic control, parking administration, pedestrian safety; general safety & security, basic services such as electricity, water and other services management, street lighting control, etc. Smart cities could support fragmented IoT services where different service providers could have their own real infrastructure or use some form of virtual infrastructure by sharing common resources.

Applications in these environments could have multi-level QoS requirements, which may impose many restrictions on the infrastructure design. For example, some safety applications could trigger many sensors requiring low latency data transfer capabilities from its network as well as high transmission bandwidth to transmit video. Similarly an electricity grid control system may require a very low latency transmission link in case of a fault generated within a grid but may not require high transmission bandwidth.

One of the critical issues in a smart city IoT environment is also the sheer number of devices that need to be serviced. From the communication networking point of view, both traditional client server architecture and device-to-device communications support needs to be provided. The smart-city IoT environment could be quite complex; particularly because in future it may be possible to provide many civic facilities in connected modes. For example, various government agencies and companies in the USA and other countries are contemplating the development of connected car systems which may reduce city parking space requirements by transport movements based on the commuter's requirements rather than where currently commuters plan their tasks based on transport schedules. This could be a huge growth area that requires significant research and development effort to develop new infrastructure.

Another significant area within a smart city is the security and surveillance system. IoT enabled devices could significantly enhance the current network of security cameras to track down intruders or offenders. Networked security sensors and automated cameras could work out the movement paths of intruders enabling security services to act more quickly. For example, expensive items could be tagged with active radio transmitters that could emit signature signals while stolen goods are being carried through the mesh of sensors located in buildings and on roads/pathways. Such IoT applications could be part of future municipal or city networks. A smart city network needs to be implemented based on advanced heterogeneous network architecture.

It is necessary to use a heterogeneous network in a smart city due to variable requirements for the likely range of applications. For example, the security applications will require short range high density sensor networks for acquiring electronic signatures but the detected information needs to be transmitted either in a unicast or in a multicast manner over a low latency long distance network to activate appropriate security measure. In this case the sensing network might comprise a Zigbee type network where the low latency long distance network could be an LTE (Long Term Evolution) wide area network (Edson et al 2014).

E-health and medical systems: This is a specialised IoT area serving aged care, indoor/outdoor patient care and ambulatory services. Aged care services could include monitoring people and helping in the diagnostic processes by providing appropriate data in a suitable manner. Use of a Wireless Body Area Network (WBAN) could significantly improve aged patient care in his/her own home or in care accommodation (Yuce & Khan 2011). WBAN devices and sensors can provided appropriate data to care providers to monitor the wellbeing of elderly persons, thus reducing the cost of care and at the same time improving the quality of the care. In other areas, medical systems could connect non-critical patients for statistics gathering from autonomous sensors to improve the quality of life of patients. Such systems require implementation of distributed systems with appropriate mobility support. In future advanced medical systems could be developed where patient monitoring devices could exchange data among themselves to control care activities such as connected drug delivery systems. Hence, e-health systems needs to support personal, local and wide area type networks to implement various systems.

Road traffic and transportation systems: Road traffic systems are currently using basic ICT systems such as automatic traffic signals, online traffic monitoring, Global Positioning System (GPS) based guidance systems, public transport scheduling systems, in network control systems, etc. However, this area could immensely benefit from the application of IoT/M2M communication systems. Recently significant R&D interests have been generated in the automobile sector for connected and autonomous cars where vehicles can exchange information either among themselves or with other entities to enhance and improve route guidance systems, offer enhance transportation services and improve pedestrian safety (Euisin et al 2014: 148-155).

In order to support the connected car environments significant research development activities have started involving the VANET (Vehicular Ad hoc Network) standards based on IEEE 802.11p and Dedicated Short Range Communication (DSRC) standards. Connected car systems could be extended to improve total road traffic systems safety by connecting with pedestrians via their smart phones and also with train systems to avoid crashes at rail crossings. Such systems need to be totally autonomous and should be able support data exchange between different entities with a high degree of confidence. To avoid car/pedestrian collisions, Honda is now trialling VANET based collision avoidance systems in USA in conjunction with the Qualcom (Wu et al 2014). The use of IoT based systems for the transport sector will enhance the reliability and safety of road traffic systems as well as allowing offering new modes of public transport systems. To support vehicular IoT systems it is necessary to work on vehicular industry standard based systems.

Environmental Monitoring: IoT systems can be used to monitor various environmental, weather and agricultural (including livestock) data in order to improve both the environment and farm productivity. Real-time information processing capabilities coupled with the ability to connect a large number of devices that communicate among them could offer an advanced platform to improve early warning systems to reduce the risks to human as well animal life. For example, interconnected sensors over a wide-area network could accurately detect fire or flood danger and inform humans about impending dangers. Current day bushfire systems generate alarms mainly from visual inspection or using satellite monitoring systems. In dense bush when a grass fire starts on the ground the smoke will not be recognised until the fire has advanced so that smoke and flames are visible or detectable from satellite. In such cases ground-based sensors could send early warnings to the nearby population using autonomous systems. Similarly mobile-connected robot based systems or fixed sensor-based systems could be used in the industrial complexes to provide necessary data in case of an accident or to monitor standard environmental data. Hence, connected systems could offer significant advantages for indoor and outdoor environmental monitoring applications.

Business inventory and product management: RFID technologies are significantly deployed in many business sectors for inventory management, throughout the supply and inventory management. The RFID based sensors allows the systems to identify products and provide them tracking abilities. Such RFID based systems are used in many forms, in-house to track product inventory as well as inter-site movements using local and wide area networks. For example, recently satellite based M2M systems are becoming popular for inventory and supply chain management in order to locate and monitor the movement of shipping containers across regions or a country as well as for transcontinental movements. A number of satellite M2M service providers offer advanced services that include ORBCOMM, Iridium, Globalstar, Inmarsat and few others (M2M Satellite). For future applications other type of sensors, including biosensors in combination with RFID technologies could allow control of production processes, improving the quality of product and shelf life, and timely delivery of products.

Industrial automation and manufacturing: Applications of IoT systems in the manufacturing shop floor are in their infancy state. Many industries use sensor-based systems to control manufacturing processes based on tailor-made applications. However, some IoT applications are emerging in the mining and control engineering areas mainly for safety and monitoring applications (Xu et al 2014). Also, the emergence of cloud computing systems will increase the deployment of IoT systems on manufacturing shop floors. Communication requirements for this class of applications could vary from a PAN-sized network to a wide area distributed network.

This section provided a brief overview of different classes of IoT applications. Discussion shows that various IoT applications will require support of different class of communication networks to support their respective QoS and network coverage needs. In the following section we briefly discuss the different communication network architecture and standards to support future IoT systems.

III. Communication Networks for Future IoT Systems

The communication network is one of the key building blocks of the IoT and cloud computing systems. As mentioned in the previous section, the IoT concept has been developed based on the M2M communication architecture. For success of IoT industries it is necessary to develop an open industry standard that is vendor-independent and can easily interwork with other functional modules. Figure 2 shows a functional model of the M2M communication network based on the ETSI (European Telecommunications Standards Institute) model (ETSI TS102 690). Figure shows that the network is divided into three layers: area, access and core networks. The ***area network*** is close to the IoT devices providing direct connectivity to these devices. It is generally assumed that these devices will operate at low power level, hence a network connection is necessary in the vicinity of these basic IoT devices. It is most likely that most of the IoT devices will use wireless connectivity to connect to an area network.

Next level in the network hierarchy is the ***access network*** that connects several area networks as well as some enhanced IoT devices to concentrate data. The access network also connects to the M2M gateway devices that concentrate many M2M functions and capabilities. Most of the M2M service capabilities and applications will be distributed over a large area connected via the core network. Communication between devices need to be offered at different levels to implement many IoT applications. For example, a sensor in an area network may activate a switch in the same or different area network. If the sensor and switch are in the same area network then it may necessary for corresponding applications to provide device to device connectivity. Hence, new device to device and traditional client server connectivity models must be maintained within the M2M communication architecture for the IoT applications.

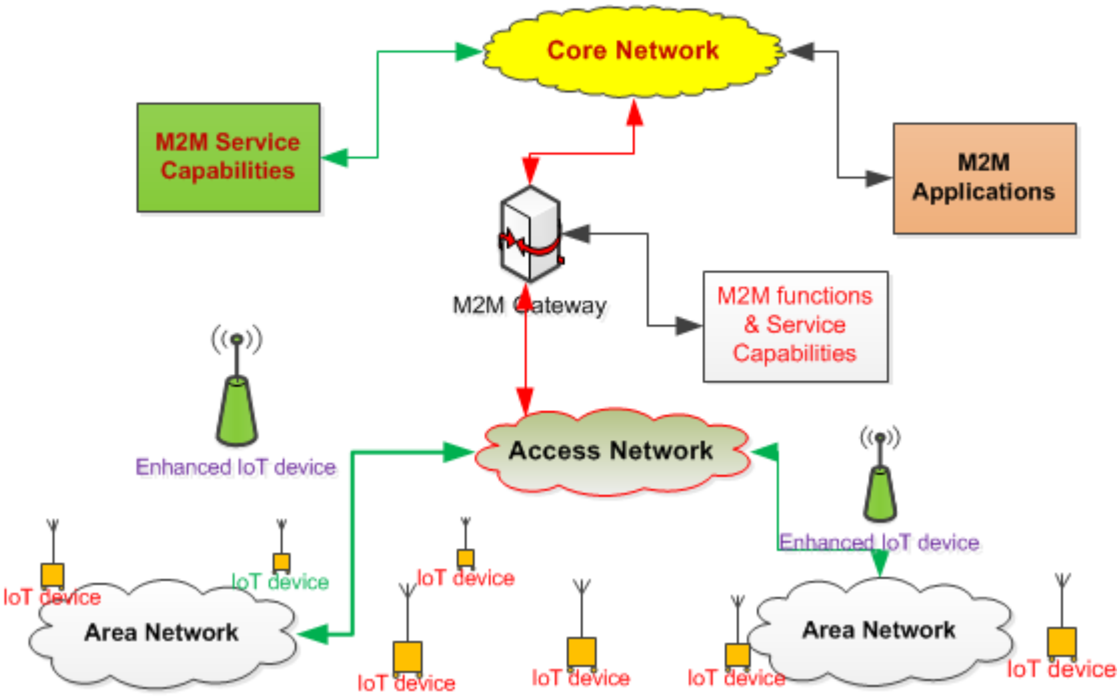


Figure 2: Machine to machine communication architecture for IoT systems based on the ETSI standard.

Considering the IoT categories discussed in Section II and the M2M communication architecture, it will be necessary to use multiple communications technologies to provide connectivity for range of IoT applications. These communication standards are broadly categorised either as wired or wireless communication systems. Wired communication systems also include fibre-based optical networks. Some of the current key communication network standards that could be used for IoT communications are listed in Table 1 (Iniewski 2010). Most of the networks are multi-service networks i.e. these networks can serve multiple types of traffic. Some of the wireless networking standards which are more appropriate for IoT applications are described later.

Table I: Summary of Communication Networking Technologies.

Network Type	**Network Size**	**Standard**	**Main Features**
Wired	Wide area	DSL, FTTN or FTTH	DSL: 2-20 Mbits/sec, FTTN/FTTH: 2 – 1000 Mbits/sec Both standards are infrastructure based
	Local Area	Ethernet: IEEE 802.3 family	Fast Ethernet: 10 Mbits/sec to 100 Mbits/sec Gigabit Ethernet: 1, 10, 40,100 Mbits/sec
		Homeplug: HomePNA/IEEE1901	14 Mbits/sec to 200 Mbits/sec
Wireless (Terrestrial)	Wide area	2G: GSM/GPRS/EGPRS	GPRS data rate: 56 to 114 kbits/sec, EGPRS: up to 236 kbits/sec
		3G: UMTS	Up to 2 Mbits/sec
		3.5G: HSPA, WiMAX (IEEE 802.16)	HSPA: up to 42 Mbits/sec, WiMAX: up to 70 Mbits/sec
		4G: LTE	Up to 100 Mbits/sec
	Local Area	WLAN: IEEE 802.11	2 Mbits/sec to 400 Mbits/sec
	Personal Area	Bluetooth/IEEE 802.15.1 Zigbee/IEEE 802.15.4/6LoWPAN WirelessHART/IEEE 802.15.4/IEC62591 ECMA368 (Ultra Wideband) ISA100.11a	Bluetooth: 1 to 10 Mbits/sec, IEEE 802.15.4: 250 kbits/sec ECMA368: up to 480 Mbit/sec ISA100.11a: 250 kbits/sec
Satellite	Wide area	LEO: Low Earth Orbit Satellite	160 to 2000 km height, constellation of 25 satellites (ORBCOMM), data rate upto 50 Mbits/sec

GSM: Global System for Mobile, GPRS: GSM Packet Radio System, EGPRS: Enhanced GPRS, UMTS: Universal Mobile Telecommunications System, HSPA: High Speed Packet Access, WiMAX: Worldwide Interoperability for Microwave Access, LTE: Long Term Evolution, WLAN: Wireless Local Area Network, 6LoWPAN: IPv6 Low Power Wireless Personal Area Network,

Basic requirements of IoT Networks:

Before developing network architecture it is important to understand basic IoT networking requirements. IoT devices and applications will generate data from various sensors and electronic devices which are generally short data bursts of a few bits to maximum of a couple of hundred bits, generating either in a synchronous or asynchronous fashion. Most of the IoT devices operating in area networks should be operating in a low power environment so that sensor nodes battery or the energy source could last for very long time. Frequent energy source replacement could be the main impediment towards the mass deployment of these devices and applications.

In order to operate in low power environments it is necessary to provide network access to these devices in the vicinity of their deployments. Hence, it is very likely that short range wireless standards such as IEEE 802.15.4 based standards will be more frequently used in the area networks. Some area networks may also use the IEEE 802.11 based WLAN standards, particularly when longer transmission range is required. The access network will require different networking standards. Access networks could use the IEEE 802.11 WLAN standard to support enhanced IoT device support; also using a mesh network architecture can offer backbone networking capabilities to the area networks. Wide area networking standards such as GPRS, HSPA, LTE, and WiMAX etc. could also be used to connect gateways and/or sparsely distributed IoT devices.

Alternatively, it may be possible to use satellite-based systems in the access network to support remote devices or mobile devices. For example, ORBCOMM is now one of the largest M2M satellite companies offering services for supermarket chains and logistics companies worldwide. Finally, the core network within the M2M network hierarchy could be implemented using either wired or wireless based wide area networking standards or based on satellite networks.

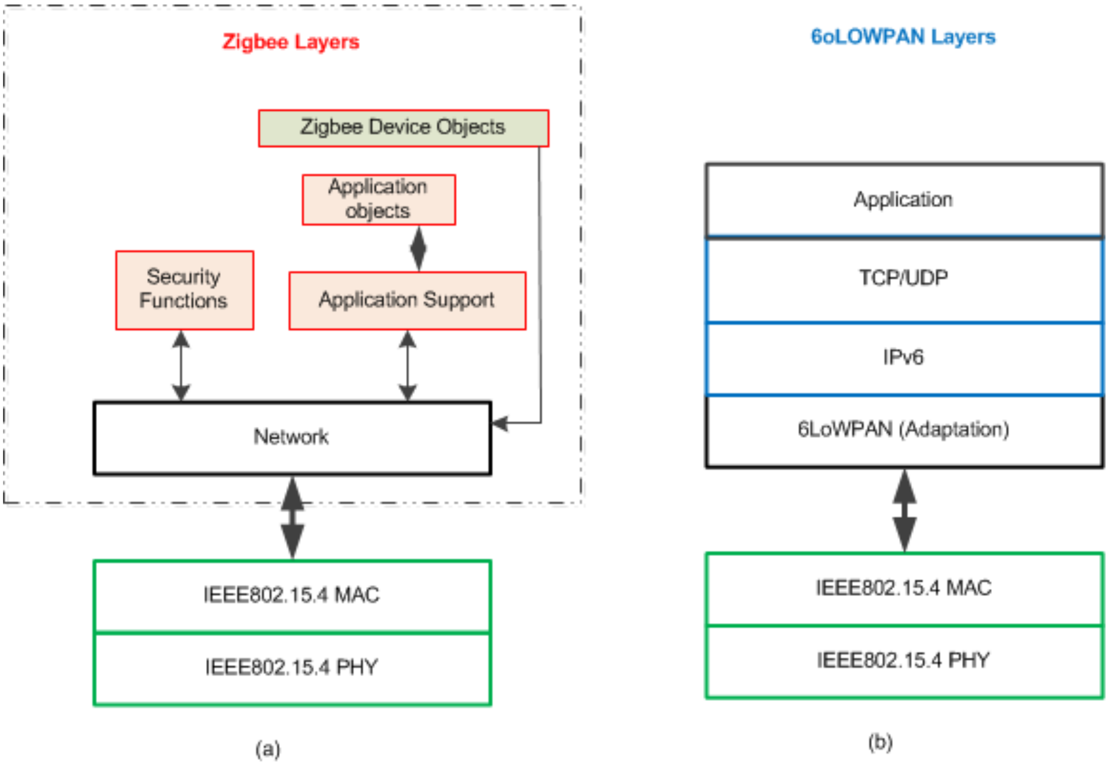
Network design for IoT systems requires significant multi-dimensional optimisation. Instead of going through different network design techniques, in the next section we present a low cost IoT network design techniques based on the IEEE 802.15.4 and IEEE 802.11 standards.

IV. Low Cost Heterogeneous Network Design for IoT Applications

In recent times many low cost wireless networking standards have been developed mainly to support low data rate short-range networking applications, primarily for sensor networking applications. Most of the IoT applications can be seen either as basic or as enhanced sensor network type applications. The IEEE 802.15.4 standard that has developed the Physical layer and MAC (Medium Access Control) layers for the short range radios has now been adopted by many other organisations such as Zigbee, IETF, HART communication foundation, IEC and others, to further develop the protocol stack for different system developments.

Figures 3a and 3b show the Zigbee and 6LoPWAN protocol stacks developed on top of the basic IEEE 802.15.4 protocol stack. Figure 3 shows that Zigbee and 6LoWPAN standards have introduced different higher layer functionalities on top of the basic 802.15.4 radios. Zigbee layers introduce networking, security and application layer functionalities whereas the 6LoWPAN protocol provides end to end IP (Internet Protocol) connectivity using higher layer protocols. The IEEE 802.15.4 standard is evolving to support various applications and operating environments. Initially the standard only supported the 2.4 GHz ISM (Instrumentation Scientific Medical) unlicensed band for the radio but recently the standard is also supporting 700/800/900 MHz band which reduces the transmission loss paving the way for lowering the transmission power, hence increasing the battery lifetime of a node/device. The IEEE 802.15.4 MAC layer use a simple random access protocol known as the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) which is similar to the MAC protocol used by the IEEE 802.11 based wireless standard.

Use of the CSMA/CA protocol reduces the network device complexities and node energy requirements if a network is properly designed. WirelessHART and ISA100.11a use the IEEE 802.15.4 physical layer but MAC layers have been modified for these standards. Based on features, cost and functionalities, the IEEE 802.15.4 based standards are ideal for IoT networking applications, particularly in the area network. Also, this standard can be combined with the IEEE 802.11 based medium to high data rate WLAN standard to implement both area and access network designs. Key features of the IEEE 802.15.4 and IEEE 802.11 standards are listed in Table 2.



(a) : Zigbee protocol stack, (b): 6LoWPAN protocol stack.

Figure 3: Zigbee and 6LoWPAN protocol stacks built on top of the IEEE 802.15.4 layers.

Table2: Some of the key features of the IEEE 802.15.4 and IEEE 802.11 standards

Parameters	**IEEE 802.15.4**	**IEEE 802.11**
Operating frequencies	700/800/900 MHz, 2.4 GHz	2.4/5 GHz, 0.9/60 GHz in 2016
Data rates	20, 40 and 250 kbits/sec	2 Mbits to 1 Gbits/sec
MAC protocol	CSMA/CA	CSMA/CA
Transmission format	Beacon & non-beacon based	Beacon & non-beacon based
Transmission power	Up to 10 mW	Typically up to 250 mW
Transmission range	10-50 metres	Up to 300 metres
Receiver sensitivity	-85 dBm @ 2.4 GHz -92 dBm @ 800/900 MHz	-89 dBm @ 6Mbits/sec -73 dBm @ 54 Mbits/sec

In Figure 4 we propose a low cost based heterogeneous IoT city network architecture using the IEEE 802.15.4 and 802.11 standards. The area network consists of several sensor clusters, sensor nodes, traffic control systems and building IoT systems connected via relay nodes to a dual radio routers. The sensor clusters could be distributed in a city area where low power sensor nodes could be gathering various data. This area network could support device-to-device communications as well as the client/server applications via the access and the core network. Device-to-device applications can easily be supported when using the 6LoWPAN standard because each device is IP addressable. Nodes within the area network could communicate with other devices either by using cluster head nodes or by using relay nodes. A large area network could be segmented in sub-networks each served by an area router.

The design introduces a dual radio router to support network heterogeneity. The dual radio router on one side will exchange information with the 802.15.4 devices which have shorter transmission range. On other side the dual radio router will connect to mesh routers within the access network. The mesh routers could be located further away from the dual radio router. Hence we propose to use an 802.15.4 and 802.11 standard based on the dual radio router. In our laboratory we have developed the dual radio router architecture by resolving the co-existence problem which is described briefly later.

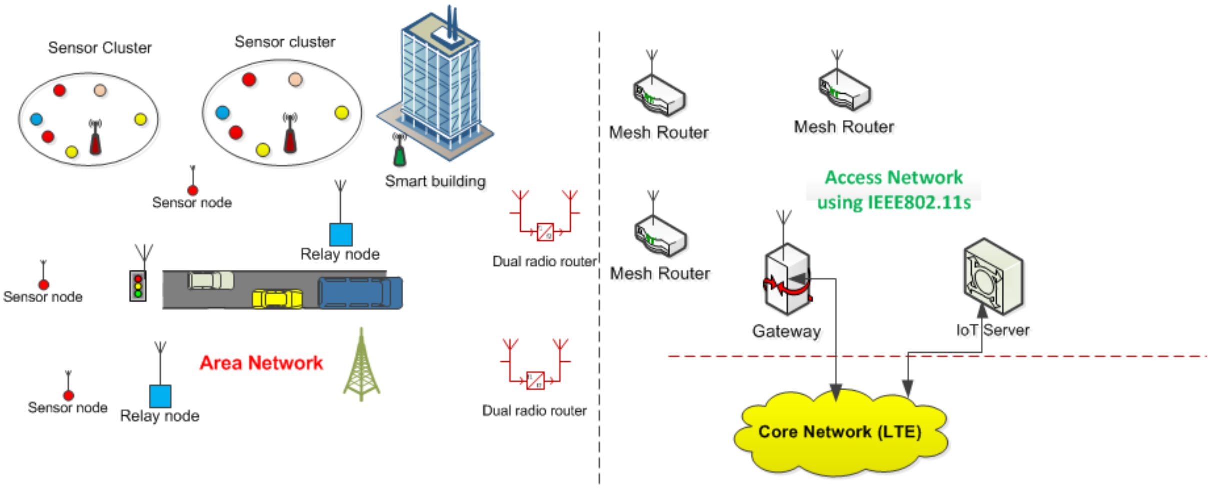


Figure 4: A heterogeneous low cost city IoT network using IEEE 802.11, IEEE 802.15.4 and LTE standards.

For a low cost IoT network we propose to use an IEEE 802.11s standard based mesh network on the access network side. The access network could connect several area networks and provide connectivity between area-to-area networks or between areas to the core network. The access network may also connect enhanced IoT devices. For a city network the core network could either be served by the 4G LTE network or it may be possible to use 3G/3.5G standards. In the core network it may be possible to use the broadband network infrastructure if an appropriate termination is available.

Short-range radio-based area network design introduces two major challenges: they are mainly deployment challenges. One of the challenges is the share of transmission spectrum by the IEEE 802.15.4 and IEEE 802.11 standards. This problem is referred as the co-existence problem and currently researchers are trying to solve the problem with minimum complexities. The other challenge is the energy supply to sensor and relay nodes which are typically battery powered. Both of the above problems are being studied at the University of Newcastle telecommunications networks research group.

To solve the first problem we have developed a new packet area scheduling technique using a control signalling system known as the ***Blank Burst (BB)*** (Chen et al 2014). Due to the limitations of the paper size the algorithm is not described here; the algorithm has been developed using the dual radio router protocol stack which is shown in Figure 5. This figure shows the area network interface on the left side and the access network interface on the right hand of the protocol stack. We have implemented two new layers on top of the IEEE 802.11 protocol to implement the area packet scheduler using BB control signalling. The protocol stack allows packet to flow between IEEE 802.15.4 and IEEE 802.11 networks.

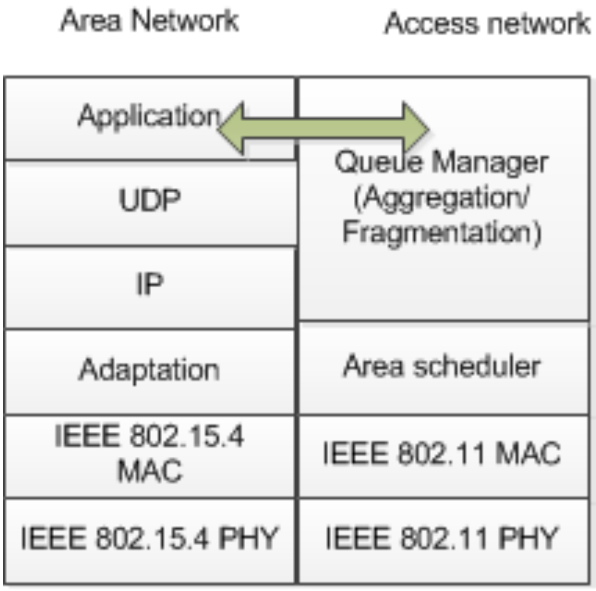


Figure 5: Dual radio router protocol stack.

V. Simulation And Test Bed Measurement Results

Figure 6 shows the performance of an area network involving 30 sensor nodes within two clusters with one relay node and a dual radio router. An OPNET based simulation model was developed to study the performance of the area network. The figure shows the packet success rates (PSR) for three different transmission scenarios. In the first scenario (blue line) only the sensor nodes are transmitting packets where only device to device communications exist. The figure shows the PSR value for different offered loads.

In the second scenario the offered traffic is received by the dual radio router and then forwarded to the access network by using the access network interface of the router. In this case both interfaces of the dual radio router are operating at 2.4 GHz. Figure 6 shows the PSR in scenario 2 (orange line) drops due to collisions between the IEEE 802.15.4 and IEEE 802.11 devices. In order to solve the problem we introduce the BB signalling technique which is represented by the Scenario 3 simulation results (grey line). Results show that the introduction of the BB control signalling technique completely eliminates the inter-network packet collisions yielding the same PSR as the scenario 1 when the IEEE 802.11 radio was silent. Our packet scheduler enables the low cost area network to operate at very high efficiency.

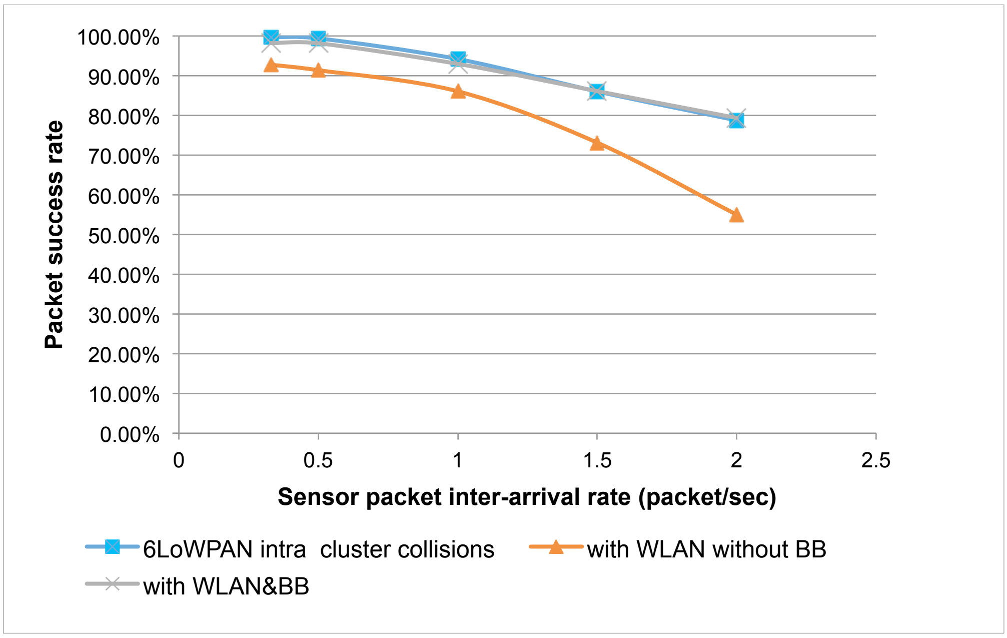


Figure 6: Packet success rate in the IEEE 802.11/IEEE 802.15.4 heterogeneous area network.

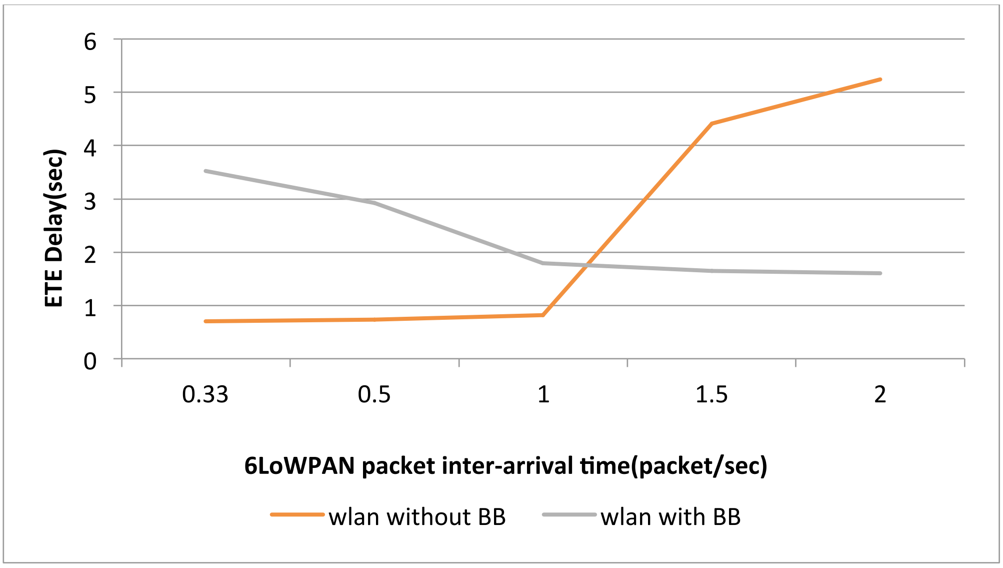


Figure 7: End-to-end delay area to access network packet transmission.

Next we examine the end-to-end delay of IoT packets transmitted from sensor nodes to the access network using the dual radio routers. Figure 7 shows the end-to-end delay for simulation scenarios 2 and 3. In scenario 2, all the received packets are directly related to the access network thus introducing minimum delay. However, the delay increases with increasing traffic due to inter-network collisions. In scenario 3, sensor data is aggregated at the dual radio router and then forwarded to the access network to reduce the signalling overhead and delay. Figure 7 shows that for low offered load the delay is higher than the scenario 2, which is due to higher aggregation delay. The aggregation delay decreases with the traffic load. At the higher traffic load scenario 3 shows lower end to end delay due to elimination of inter-network packet collisions. Both results show that the performance of the heterogeneous access network is enhanced when the developed dual radio router is used in combination with the BB signalling technique. It is worthwhile to mention here that new IEEE 802.11 devices will also appear in the 900 MHz spectrum; hence in future the coexistence problem will exist in other frequency bands.

The next design and deployment challenge is energy availability for the sensor and router nodes in the area and also in access networks. To solve the energy issue we have developed solar powered IoT nodes and routers based on the IEEE 802.15.4 radio operating in the 900 MHz band. Figure 8 shows the developed solar IoT node which is currently used in a campus network test bed. This is a proof-of-concept design which we have developed as a part of an energy scavenging sensor network design project.

The foundation for this proof of concept node design utilises the Texas Instruments (TI) CC430F5137RF900 development board which is a small PCB (Printed Circuit Board) solution designed by TI to allow rapid prototyping and testing of sub GHz wireless senor network projects. The node utilises the CC430 IC which combines the TI MSP430 microcontroller with a CC1101 transceiver into a single chip. The development board provides accessible I/O and is typically powered by two AAA batteries. Utilising the TI Code Composer Studio IDE a custom mesh network was implemented and programmed on to the custom sensor nodes.

To then develop this microcontroller into a deployable wireless sensor node a stackable two-layer PCB design was formulated. The first layer interfaces the CC430 I/O ports and power connections onto the custom PCB which comprises a 2 x AAA battery holder, solar charging circuitry and 8 digital and 8 ADC (Analog-to-Digital Converter) capable IO ports. The IO ports are broken out into a header allowing for rapid prototyping with sensors as developmental needs change. The initial design utilised 3V temperature and humidity sensors switched by the digital IO and read by the ADC ports. A second small PCB interconnects on top of this first layer which contains the solar panels. This creates a small form factor complete sensor node device with dimensions 90x60x25 mm (excluding external casing). The design provides a self-sustaining yet flexible wireless sensor node device capable of quick sensor installation and adjustment.

The power supply design is a simple 6V 16mA 40x50 mm solar panel connected in parallel to the batteries and microcontroller with a current-blocking protective diode. Voltage regulation is maintained by the battery voltage and CC430 on-board regulator. The panels were sized to ensure a sufficiently small charge rate would be achieved at maximum sunlight so as not to damage the batteries over time, but also selected to allow an effective recharge rate each day, as the graphs demonstrate, for reasonable packet transmission rates.

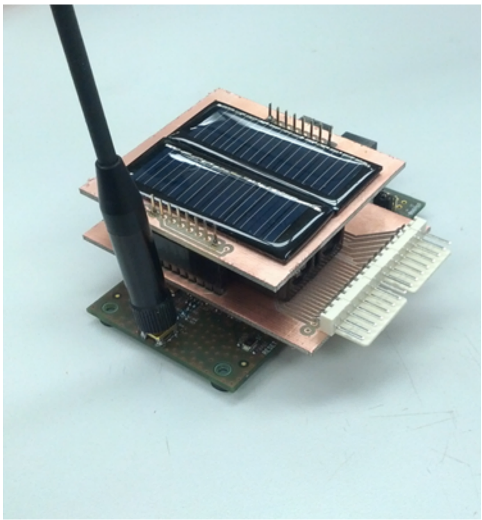


Figure 8: Proof of concept solar IoT node.

The design was finalised with a 3D printed external casing. This allows for adjustments made in the design to allow for ventilation or sensor access depending on the specific sensor solution required. The flexible solar panel stackable design means that the solar panels can be mounted within the casing (necessitating a window to light the panels). Alternatively, and more simply, the panels can be located on the exterior of the casing with wiring fed back to the second layer PCB.

The developed IoT node was tested for the durability of the energy scavenging power supply. The IoT node was placed on a side window where direct sun light was available for about 4-5 hours/day and programmed to transmit packets to another node located about 20 metres away. The node was using 0 dBm transmission power. Figure 9 shows the node voltage profile which is supplied by two AAA batteries. The battery voltage was monitored for nine days, three days for each packet transmission rate.

Results show that the IoT nodes can operate in an uninterrupted manner when powered by solar panels even inside a room. The min/max value of the battery voltage depends on the weather. When measurements were carried out for the highest packet rate the days were perfectly sunny, whereas other days were cloudy or partially cloudy. Minimum operating voltage of this sensor node is 1.8 volts. The measurement shows that these low-power sensor nodes can operate for a very long period without changing batteries. Currently we are measuring the battery voltage by equipping several nodes with different active and passive sensors

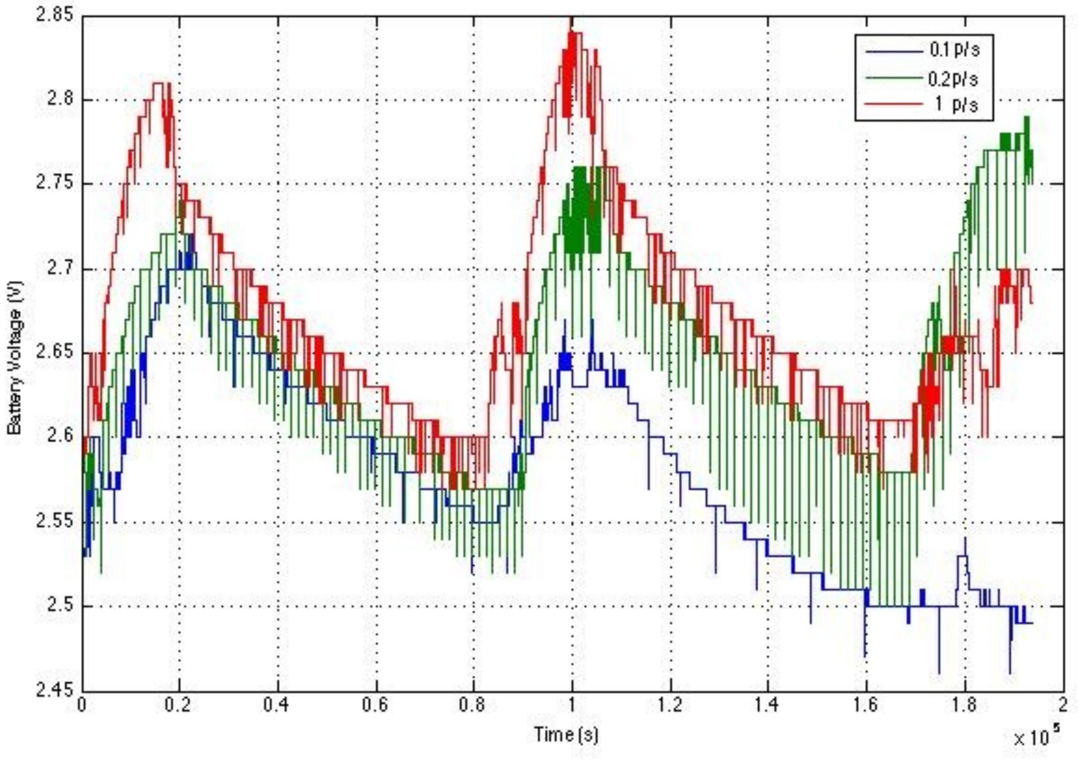


Figure 9: Battery voltage charge/discharge profile for different packet transmission rates measured over three days.

VI. Conclusions

This paper presented a comprehensive review of the IoT applications and communication network design techniques. The paper reviewed different communication technologies suitable for IoT applications. The review showed that both wireless and wired networks could be used to develop future IoT systems; however, due to the nature of the system, wireless technologies will dominate the networking area. We presented a low-cost wide-area network design architecture which can be developed for both city and rural area applications using low-cost network devices. The proposed energy-scavenging-based heterogeneous network has very low CAPEX (Capital Expenses) compared to a cellular network based system. IoT nodes and networks can be developed at a low cost when embedded wireless technologies are used. Embedded wireless technologies will be scalable and easily upgradable as they are based on international standards.

The OPEX (Operational Expenses) cost of the proposed network is virtually zero because the greater part of the area and access networks will developed on embedded wireless devices where many devices will scavenge their energy from natural sources, thus the operating energy cost will be minimum. Some OPEX cost could occur when 3G/4G networks or broadband connectivity could be used in the core network or to support a distributed access network. IoT is an evolving area; many new technologies including embedded wireless technologies will emerge which may further reduce the cost of deployments in future.

Acknowledgements

The authors would like to thank the Australian Research Council and Ausgrid for supporting part of the project.

References

Akyildiz, I. F; Jornet, J. M. 2010. “The Internet of Nano-Things”, *IEEE Wireless Communications,* December 2010, pp. 58-63.

Atzori, L; Iera, A; Morabito, G. 2010. “The Internet of Things: A Survey”, *Computer Networks*, 54(2010), pp2787-2805.

Balasubramaniam, S; Kangasharju, J. 2013. “Realizing Internet of Nano Things: Challenges, Solutions and Applications”, *IEEE Computer*, February 2013, pp. 62-68.

Chen, D; Khan, J.Y; Brown, J. 2014. ‘An Area Packet Scheduler to Mitigate the Coexistence Issue in a WPAN/WLAN Based Heterogeneous Network’ submitted for review *IEEE WCNC 2014,* New Orleans, USA, 9-12 March, 2104.

Edson, A; Marques, L; dos Passos, D; Macedo, R; Dias, K; Nogueira, M. 2014. ‘Interoperability issues on heterogeneous wireless communication for smart cities’, *Computer Communications*, early access article, http://dx.doi.org/10.1016/j.comcom.2014.07.005

Euisin, L; Eun-Kyu, L; Gerala, M; Oh, S. Y. 2014, ‘Vehicular Cloud Networking: Architecture & Design Principles’, *IEEE Communication Magazine*, February 2014, 148-155.

Forbes. 2013. Forbes Magazine 1 July 2013. "How many things are currently connected to the internet of Things (IoT)?" Available at: http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/

Gartner. 2014. Media release. "Gartner says a Thirty-Fold increase in internet-connected physical devices by 2020 will significantly alter how the Supply Chain operates" March 24, 2014. Available at: http://www.gartner.com/newsroom/id/2688717

Iniewski, K. 2010. *Convergence of Mobile & Stationary Next-Generation Networks*, John Wiley & Sons.

Jin, J; Gubbi, J; Marusic, S; Palaniswami, M. 2014. "An information framework of creating Smart City through Internet of Things", *IEEE Journal of Internet of Things*, DOI: 1109/JIOT.2013.2296516,

Kim, J; Lee, J; Kim, J; Yun, J. 2014. "M2M Service Platforms: Survey, Issues and Enabling Technologies", *IEEE Communications Surveys & Tutorials*, vol: 16, no:1, First quarter, 2014, pp. 61-76.

M2M Satellite. 2013. "M2M Connectivity". Available at: http://www.m2mconnectivity.com.au/technologies/satellite

Miorandi, D; Sicari, S; De Pellegrini, F; Chlamtac, I. 2012. "Internet of things: Vision, applications and research challenges", *Ad hoc Networks*, 10 (2012), pp. 1497-1516.

Mobile World. 2014. Mobile World Live 23 April 2014. "Huawei predicts 100B connected terminals by 2025". Available at: http://www.mobileworldlive.com/evolving-ict-market-create-infinite-opportunities-huawei

Ardis, Kristopher. 2013. "What's to come: the IoT's role in smart grid evolution". *Smart Grid News*. Dec 3, 2013. Available at: http://www.smartgridnews.com/artman/publish/End_Use_Smart_Homes/What-s-to-come-the-IoT-s-role-in-smart-grid-evolution-6200.html#.VDb_6_mSzh4

Sterling, L; Tareter, K. 2009. *Intelligent Lifestyle Applications*, MIT Press, 1st edition, 2009, 281-326.

Wu, X; Mincic, R; Al-Stouhi; Misener, J; Bai, S; Chan, W-H. 2014. 'Car Talks to Phones: A DSRC Based Vehicle – Pedestrian Safety System', *Proc. Of the IEEE VTC Fall*, 14-17 September, Vancouver, 2014.

Xu, L. D; He, W; Li, S. 2014. "Internet of Things in Industries: A Survey", *IEEE Trans. On Industrial Informatics*, DOI:10.1109/TII.2014.2300753, early access article available from IEEE Explore, 2014, early access article available for IEEE Explore, 2014.

Yuce M; Khan, J. Y. (editors). 2011. *Wireless Body Area Networks: Technology, Implementation, and Applications,* Pan Stanford Publishing, 2011.

Zaslavsky; A. 2013. "Internet of Things and Ubiquitous Sensing" *Computing Now*, September 2013,