International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2018): 5.426

Energy Consumption in Internet of Things (IOT)

Ayman Ahmad Omar Omar

ayman_omar [at]yahoo.com
Amman-Jordan, Arab Academy For Banking & Financial Sciences – AABFS

1. Introduction

An Internet of Things (IoT) architecture consists of a wide range of Internet-connected devices or things. The IoT is a broad term referring to applications as diverse as Internet-connected vehicles, consumer electronics and smart phones. IoT refers not only to personal computers and mobile phones connected through the Internet, but also to the wireless interconnection of all of the billions of 'things' and devices through the internet or local area networks that is done to increase efficient utilization [1, 2], as shown in (Figure 1). Internet of Things (IoT) is a network that enables new forms of communication between people and things and between things themselves. Each of the things or objects in IoT communicates with the others and plays a defined role [3]. Wireless nodes equipped with sensors are among the things and devices on the IoT. Wireless sensor nodes connected to a network collect information about the environment surrounding the sensor node. Many types of sensors are used by wireless sensor nodes, including those for measuring temperature, humidity, illumination, motion, pressure, stress, distortion, position, flow rate, and gas. The sensor is the most important component in the (IOT), So to increase the number, the accuracy of collected data we need to increase the number of sensor nodes [2].

Figure 1: Internet of Things [4]

A major limitation of wireless nodes is finite battery capacity—nodes will operate for a finite duration, only as long as the battery lasts. Finite node lifetime implies finite lifetime of the applications or additional cost and complexity to regularly change batteries. Nodes could possibly use large batteries for longer lifetimes, but will have to deal with increased size, weight and cost. Nodes may also choose to use low-power hardware like a low-power processor and radio, at the cost of lesser computation ability and lower transmission ranges [3].

In networks for IoT, nodes are distributed in a certain region for specific purpose and gather the required information, for example, the information about the temperature, motion, and physical changes. The nodes forward the gathered information to the intermediate nodes because of the limited transmission range of the node. Therefore, the intermediate nodes use the unintended energy for the packet forwarding of the source node, which induces high energy consumption of the nodes and thus accelerates network partitioning. Therefore, the energy efficiency of the nodes is the key factor that affects the network performance in distributed networks for IoT [5].

The Internet of Things (IOT) offers many sophisticated and ubiquitous applications for different devices. The energy demand of IoT applications is increased, while IoT devices continue to grow in both numbers and requirements. Therefore, IOT solutions must have the ability to efficiently utilize energy and handle the associated challenges. Energy management is considered as a key paradigm for the realization of complex energy systems in IOT [6]. A lot of work has been done in the field of Wireless Sensor Networks (WSN) in recent years. Efforts to make efficient, low cost, scalable and easily deployable WSN have been on going. In order to reduce cost and improve life of a sensor node, it is necessary to optimize battery usage and power consumption [7]. We need to find methods and techniques for reduce the energy consumption without affecting the user's satisfaction [8].

Several solution techniques and methods have been proposed to maximize the lifetime of battery-powered sensor nodes. Some of these include energy-aware MAC protocols, power aware storage, routing and data dissemination protocols, duty-cycling strategies, adaptive sensing rate, tiered system architectures and redundant placement of nodes. While all the above techniques optimize and adapt energy usage to maximize the lifetime of a sensor node, the lifetime remains bounded and finite. The above techniques help to increase the application lifetime and/or the time interval between battery replacements. With a finite energy source, seldom can all the performance parameters be optimized simultaneously, e.g., higher battery capacity implies increased cost, low duty-cycle implies decreased sensing reliability, higher transmission range implies higher power requirement and lower transmission range implies transmission paths with more number of hops resulting in energy usage at more number of nodes [3]. An alternative technique that has been applied to address the problem of finite node lifetime is the use of energy harvesting. Energy harvesting refers to harnessing energy from the environment or other energy sources (body heat, foot strike, finger strokes) and converting it to electrical energy. The harnessed electrical energy powers the sensor nodes. If the harvested energy source is large and periodically/continuously available, a sensor node can be powered permanently. In addition, based on the periodicity and magnitude of harvestable energy, system parameters of a node can be tuned to increase node and network performance. [3, 9].

2. IOT Elements

In this section we will discuss the basic elements in the to deliver the functionality of the IOT as shown in (Figure 2).

2.1 Identification

Identification is crucial for the IoT to name and match services with their demand. Many identification methods are available for the IoT such as electronic product codes (EPC) and ubiquitous codes (uCode). Furthermore, addressing the IoT objects is critical to differentiate between object ID and its address. Object ID refers to its name such as ―"T1" for a particular temperature sensor and object‘s address refers to its address within a communications network. In addition, addressing methods of IoT objects include IPv6 and IPv4. 6LoWPAN provides a compression mechanism over IPv6 an header that makes IPv6 addressing appropriate for low power wireless networks. Distinguishing between object‘s identification and address is necessary. Since identification methods are not globally unique, so addressing assists to uniquely identify objects. Identification methods are used to provide a clear identity for each object within the network [10].

2.2Sensing

The IoT sensing means collecting data from related objects within the network and sending it back to a data warehouse, database, or cloud. The collected data is analyzed to take specific actions based on required services. The IoT sensors can be smart sensors, actuators or wearable sensing devices. Single Board Computers (SBCs) integrated with sensors and built-in TCP/IP and security functionalities are typically used to realize IoT products. Such devices typically connect to a central management portal to provide the required data by customers [3, 10].

Figure 2: The IOT elements [10]

2.3 Communication

The IoT communication technologies connect heterogeneous objects together to deliver specific smart services. Typically, the IoT nodes should operate using low power in the presence of lossy and noisy communication links. Examples of communication protocols used for the IoT are as the following:

1- Radio-Frequency Identification (RFID): Uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader [11].The RFID tag represents a simple chip or label attached to provide object‘s identity. The RFID reader transmits a query signal to the tag and receives reflected signal from the tag, which in turn is passed to the database. The database connects to a processing center to identify objects based on the reflected signals within a (10 cm to 200 m) range. RFID tags can be active, passive or semi-passive/active. Active tags are powered by battery while passive ones do not need battery. Semi-passive/active tags use board power when needed [10].

2- The Near Filed Communication (NFC) Protocol : Works at high frequency band at 13.56 MHz and supports data rate up to 424 kbps. The applicable range is up to 10 cm where communication between active readers and passive tags or two active readers can occur [10, 12].

3- The Ultra-Wide Bandwidth (UWB): Communication technology is designed to support communications within a low range coverage area using low energy and high bandwidth whose applications to connect sensors have been increased recently [10].

4- WiFi Based on IEEE 802.11: That uses radio waves to exchange data amongst things within 100 m range. WiFi allows smart devices to communicate and exchange information without using a router in some ad hoc configurations [10, 13].

5- Bluetooth: Presents a communication technology that is used to exchange data between devices over short distances using short-wavelength radio to minimize power consumption. Recently, the Bluetooth special interest group (SIG) produced Bluetooth 4.1 that provides Bluetooth Low Energy as well as high-speed and IP connectivity to support IoT [10, 14].

6- The IEEE 802.15.4 standard: Specifies both a physical layer and a medium access control for low power wireless networks targeting reliable and scalable communications [10, 15].

7- Long-Term Evolution (LTE): Is originally a standard wireless communication for high-speed data transfer between mobile phones based on GSM/UMTS network technologies. It can cover fast-travelling devices and provide multicasting and broadcasting services [[10, 16]

8- LTE Advanced (TE-A): Is an improved version of LTE including bandwidth extension which supports up to 100 MHz, downlink and uplink spatial multiplexing, extended coverage, higher throughput and lower latencies [10, 17].

2.4 Computation

Processing units (e.g., microcontrollers, microprocessors, SOCs, FPGAs) and software applications represent the "brain" and the computational ability of the IoT. Various hardware platforms were developed to run IoT applications such as Arduino, UDOO, Friendly ARM, Intel Galileo, Raspberry PI, Gadgeteer, BeagleBone, Cubieboard, Z1, WiSense, Mulle, and T-Mote Sky. Moreover, many software platforms are utilized to provide IoT functionalities. Among these platforms, Operating Systems (RTOS) are vital since they run for the whole activation time of a device. There are several Real-Time Operating Systems (RTOS) that are good candidates for the development of RTOS-based IoT applications. For instance, the Contiki RTOS has been used widely in IoT scenarios. These platforms provide facilities for smart objects to send their data to the cloud, for big data to be processed in real-time, and eventually for end-users to benefit from the knowledge extracted from the collected big data. There are a lot of free and commercial cloud platforms and frameworks available to host IoT services [10, 18]. (Table 1) shows comparison between common operating system used in IOT environment.

Table 1: Comparison between operating system used in IOT Environment [10]

Operating System	Language Support	Minimum Memory (KB)	Event-based Programming	Multi-threading	Dynamic Memory
TinyOS	nesC	1	Yes	Partial	Yes
Contiki	C	2	Yes	Yes	Yes
LiteOS	C	4	Yes	Yes	Yes
RiotOS	C/C++	1.5	No	Yes	Yes
Android	Java	-	Yes	Yes	Yes

2.5 Services

IOT services can be categorized into four classes as the following [10, 19]:

1- Identity-related services: Are the most basic and important services that are used in other types of services. Every application that needs to bring real world objects to the virtual world has to identify those objects.

2- Information Aggregation Services: Collect and summarize raw sensory measurements that need to be processed and reported to the IoT application (e.g., Smart healthcare and smart grids).

3- Collaborative-Aware Services: Act on top of Information Aggregation Services and use the obtained data to make decision and react accordingly.

4- Ubiquitous Services: Provide Collaborative-Aware Services anytime they are needed to anyone who needs them anywhere (e.g., smart home, smart buildings, intelligent transportation systems (ITS), and industrial automation).

2.6 Semantic

Semantic in the IoT refers to the ability to extract knowledge by different devices to provide the required services. Knowledge extraction includes discovering and using resources and modeling information. Also, it includes recognizing and analyzing data to make sense of the right decision to provide the exact service. Thus, semantic represents the brain of the IoT by sending demands to the right resource. This requirement is supported by Semantic Web technologies such as the Resource Description Framework (RDF) and the Web Ontology Language (OWL) Efficient XML Interchange (EXI), EXI is important in the context of the IoT because it is designed to optimize XML applications for resource-constrained environments. Furthermore, it reduces bandwidth needs without affecting related resources such as battery life, code size, energy consumed for processing, and memory size. EXI converts XML messages to binary to reduce the needed bandwidth and minimize the required storage size. [10, 20].

3. Wireless Sensor Networks

Wireless Sensor Network (WSN) (or Wireless Sensor and Actor Network (WSAN)) is a network of sensor nodes spatially distributed in a region to monitor real-world physical parameters and report the sensed values to a central controller. WSAN adds the capability to take actions based on the sensed and collected values. WSNs are rapidly becoming ubiquitous in the world of Environmental Monitoring, Healthcare monitoring, Smart Cities and Home Automation. Building Smart Cities and Smart Homes requires large scale data collection. A smart home is effectively an autonomous home automation system [1]. Actions like setting the thermostat based on factors like weather and user preference, turning lights and fans on/off without human intervention, tracking consumption of consumable products like gas cylinders and a number of other tasks. Making daily life easier, more convenient and minimizing human intervention in mundane tasks are some of the main objectives behind home automation. However automating these processes requires acquiring data from a distributed array of sensors. WSN provides a possible solution to this problem. WSN provides an innovative and robust solution to problems in multiple spheres of life [7, 20].

A lot of research has been done in the field of Wireless Sensor Networks (WSN) in recent years. Efforts to make efficient, low cost, scalable and easily deployable WSN and power consumption and optimize battery usage have been ongoing.

3.1Sensor Architecture

Most of the wireless sensor networks (WSNs) consist of a set autonomous sensor nodes. These nodes consist of sensor arrays, System-on-Chip (SoC), wireless communication interfaces and power supply and distribution units. The wireless communication aspect of a WSN allows each node to operate autonomously. As illustrates in (Figure 3).

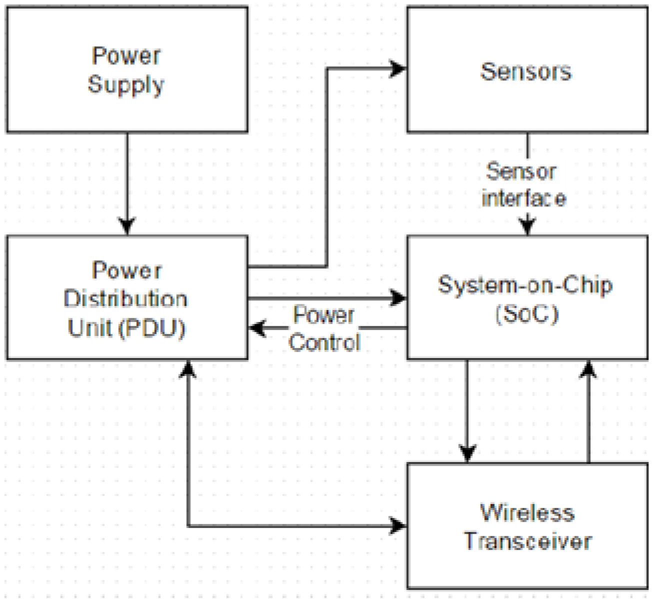

Figure 3: Architecture of WSN [7]

- **Sensor:** Is an electronic component, module, or subsystem whose purpose is to detect events or changes in its environment and send the information to other electronics, frequently a computer processor.
- **System On Chip (SOC):** Is an integrated circuit that integrates all components of a computer or other electronic system. Also, SoC integrates a microcontroller or microprocessor with advanced peripherals like graphics processing unit (GPU), Wi-Fi module, or one or more coprocessors. Similar to how a microcontroller integrates a microprocessor with peripheral circuits and memory, an SoC can be seen as integrating a microcontroller with even more advanced peripherals [21].
- **Wireless Transceiver:** Does a device comprise both a transmitter and receivers that are combined and share common circuitry or a single housing. When no circuitry is common between transmit and receive functions, the device is a transmitter-receiver. In WSNs transceivers often lack unique identifiers. The operational states are transmitted, receive, idle, and sleep. Current generation transceivers have built-in state machines that perform some operations automatically. Most transceivers operating in idle mode have a power consumption almost equal to the power consumed in receive mode. Thus, it is better to completely shut down the transceiver rather than leave it in the idle mode when it is not transmitting or receiving. A significant amount of power is consumed when switching from sleep mode to transmit mode in order to transmit a packet [22].
- **Power Supply:** Since the wireless sensor node is often paced in a hard-to-reach location, changing the battery regularly can be costly and inconvenient. An important aspect in the development of a wireless sensor node is ensuring that there is always adequate energy available to power the system. The sensor node consumes power for sensing, communicating and data processing. More energy is required for data communication than any other process. The energy cost of transmitting 1 Kb a distance of 100 metres (330 ft) is approximately the same as that used for the execution of 3 million instructions by a 100 million instructions per second/W processor. Power is stored either in batteries or capacitors. Batteries, both rechargeable and non-rechargeable, are the main source of power supply for sensor nodes. They are also classified according to electrochemical material used for the electrodes such as NiCd (nickel-cadmium), NiZn (nickel-zinc), NiMH (nickel-metal hydride), and lithium-ion. Current sensors are able to renew their energy from solar sources, temperature differences, or vibration. Two power saving policies used are Dynamic Power Management (DPM) and Dynamic Voltage Scaling (DVS). DPM conserves power by shutting down parts of the sensor node which are not currently used or active. A DVS scheme varies the power levels within the sensor node depending on the non-deterministic workload. By varying the voltage along with the frequency, it is possible to obtain quadratic reduction in power consumption [22].
- **Power Distribution Unit:** is a device fitted with multiple outputs designed to distribute electric power

3.2Topology

The nodes are usually configured in a typical star topology (each node connected directly to a central hub called a sink node), or more typically a multi-hop mesh network. As the following:

-**The star topology**: Each node is connected directly to the central hub. The main advantage of this topology is that the network is not affected by node failure as long as the hub is active. Star topology centralizes control, as only the sink node is aware of the status of all the nodes. For a single node to transmit data, other nodes do not need to be active. The disadvantage is apparent as size of network increases. The hub needs connect to larger number of devices which increases power consumption [7].As shown in (Figure 4).

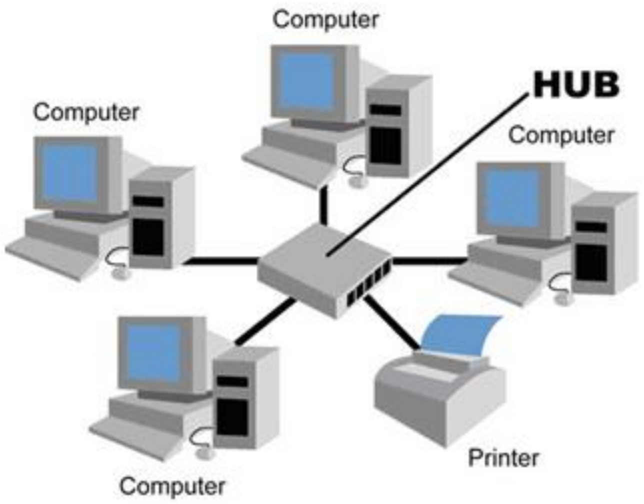

Figure 4: Star topology [23]

-The multi-hop mesh network: Each sensor node links to its nearest neighbors. Data is communicated to a server through the mesh by flooding and routing algorithms. Mesh networks are more robust as compared to star topologies as it is more resistant to node failure. Data is pushed to a central hub by routing the packet through multiple nodes. Transmission power of each node can thus be lower, even if size of network is large. However there is a drawback. For a node located at the edges of the mesh, to transmit a packet to an opposite edge of the mesh, the routing path will pass through multiple intermediate hops. Each hop consumes power in each of the nodes it passes through. Hence as size of the network (number of nodes as well as spatial region covered) increases, the average power consumption of the entire network goes up [7].As shown in (Figure 5).

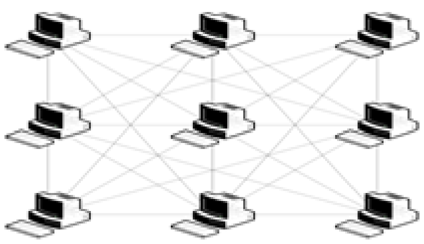

Figure 5: Mesh topology [24]

1.3 Wireless Technology

Wireless communication is a high power consumption block of any WSN. Since each node is autonomous and distributed in spatially diverse regions, minimizing power consumption of each node is an important aspect of any sensor node. Continuous power supply may not be available, which necessitates that a node must draw power from a battery pack or similar temporary power supply. Energy is one of the scarcest resources for any sensor node. If the energy consumption is too high, it will require frequent replacement of power cells. Typical WSN implementations use some form of WPAN like Zigbee or more traditional RF modules like NRF24L01Pand CC2500. And we will discuss some of them briefly.

NRF24L01P: Basic wireless communications can be achieved using any readily available RF transmitters. The small, low costNRF24L01P can be used in WSN; it wasn't designed to be power efficient. It also lacks any hardware based routing or networking algorithms. This means any routing and network formation has to done on a software level. NRF24L01P is capable of covering in 5 distinct modes [7]:

1) **Power Down Mode:** Radio is disabled. Only registers and SPI interface are kept active to accept new configurations. His offers minimum power consumption.
2) **Standby-I mode**: This mode is to ensure shorter start up time than. Power down mode at the cost of slightly higher power consumption.
3) **Standby-II mode:** This mode is primarily when data is to be transmitted at short notice. Additional clock buffers are activated. If data arrives in the Tx buffer, it gets transmitted after a minimal settling delay.
4) **Rx mode:** In this mode the NRF24L01P is actively listening for packets. The power consumption depends on the Air data rate being used. It increases with increase in air data rate.
5) **Tx mode:** This mode is when the NRF24L01P is actively transmitting data. Depending on the state of the TX buffer, the module switches between standby-II mode and TX mode. It has the highest power consumption of any mode. The power consumption depends heavily on the transmit power being used.

- **Zigbee:** One of the most popular choices for wireless communication in WSNs is the implementation of the IEEE 802.15.4 standard popularly known as Zigbee. Zigbee is a high-level communication protocol which operates on a mesh topology. It is a self-organizing network, where each Zigbee device only needs to be assigned a role. Zigbee is a low cost system which is very well suited for WSN. Zigbee also supports low power sleep modes alongside active power consuming modes [7].

1.4 Power Saving Techniques

Since power consumption has to be minimized, many WSN architectures communicate with very low duty cycles (often used to reduce the energy consumption caused by idle listening in Wireless Sensor Networks (WSNs)). The sensor node is kept in a low power state, with the sensors and peripherals switched off and the controller and communication interfaces in a low-power, sleep-like state. The node becomes active for a short duration periodically, where it wakes up, senses the value, relays this value over the network and then returns back to the sleep state. While this approach does minimize power consumption, it suffers from a drawback. Applications requiring real-time data monitoring cannot use this approach. Real-time monitoring will require the duty cycle of the sensor node to be very high, which increases power consumption and decreases battery life. Another measure to reduce power consumption, especially in larger sensor networks is to use a mesh topology. Mesh networks are generally preferred, since it makes the size and power of the wireless antenna smaller. This reduces cost of the node as well as the power consumption. However real-time data collection again introduces an issue. As network size and sensor node distribution density increases, average power consumption of all nodes rises. The chances of packet collision during transmission also increases, which introduces additional cost of retransmission [7].

1.5 Accessing the Data

When the data is communicated to the sink node, it needs to be processed and action needs to be taken on it. This requires that the data be accessible. Many WSN systems need to be remotely accessed to modify the configuration and read sensed values. A need for integrating the WSN with a system to provide easy access to the data is vital in order to maximize the usefulness of the data [7].

From previous discussion we can conclude the following problems in WSNs:

- The wireless communication technology used in the sensor nodes need to consume as little power as possible.
- The network topology chosen should minimize transmission power requirements while also providing robust network which is not sensitive to node failures.
- Nodes should avoid real-time monitoring unless essential to reduce overall power consumption.
- Node data should not be accessible only locally from a central sink node. A more reliable and robust method of accessing the network is needed.

Power consumption it is obvious, as we mentioned before is one of the most important challenge in the WSNs, we need to find methods and techniques for power consumption and power management to solve this challenge.

4. Energy Management In IOT

Energy demand around the world is increasing day by day. To fulfill this demand the existing generation is facing a lot of challenges. It is estimated that total energy demand at the end of 2020 will increase by 75% as compared to energy demand in 2000 [25].In this section, we present a brief overview of energy management and challenges in IOT system. We classify the energy management inIOT into two main types: energy-efficient techniques and energy harvesting operations.

4.1 Energy Efficiency Techniques

Energy efficiency is one of the important performance parameters of IOT system and its related network. IOT application and devices have even further strict requirements for network lifetime and delays. With increasing the applications in IOT, energy efficient techniques also evolving for low-power devices. There are some energy-efficient techniques that can either reduce energy consumption or optimize resource utilization. We can classify as following:

4.1.1 Lightweight Protocols

Lightweight means that a protocol causes less overhead. IoT systems have to use various protocols for communication. There are several existing protocols in the literature such as Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queue Protocol (AMQP), 6lowPAN, and Universal Plug and Play (UPnP) IoT. MQTT and CoAP are the most popular protocols. MQTT is a lightweight protocol that collects data from IoT devices and transmits to the servers. CoAP is designed for constrained devices and networks for web transfer. Each of these protocols is designed for specific scenarios and applications in which it performs well. In addition, protocol conversion is an important building block for IoT, which may require that the IoT devices be from different manufacturers or using different protocols [6].

- COAP and MQTT Protocol:

Two of the most promising for small devices are MQTT and CoAP in IOT. Both MQTT and CoAP:

- Are open standards.
- Are better suited to constrained environments than HTTP.
- Provide mechanisms for asynchronous communication.
- Run on IP.

MQTT gives flexibility in communication patterns and acts purely as a pipe for binary data. CoAP is designed for interoperability with the web.

MQTT Protocol:

Is a publish/subscribe messaging protocol designed for lightweight M2M communications. It was originally developed by IBM and is now an open standard. MQTT has a client/server model, where every sensor is a client and connects to a server, known as a broker, over TCP [26].

CoAP Protocol:

Is the Constrained Application Protocol from the CoRE (Constrained Resource Environments). CoAp is a document transfer protocol. Unlike HTTP, CoAP is designed for the needs of constrained devices.

4.1.2 Predictive Models For Energy Consumption

Predictive models for energy consumption in IoT are indeed of vital importance. They refer to the wide range of applications in IOT systems including predictive models for traffic and travel, predictive models for controlling temperature and humidity, and so on. Various prediction models such as neural networks and Markov decision processes can be incorporated here. Exploiting the predictive models will not only reduce the significant energy consumption but also lead to many societal benefits [6]. In [28] The B-Model experiment used the FIESTA platform to gather large volumes of IoT observations, which are then used to validate advanced Machine Learning algorithms for the prediction of energy consumption in office buildings and data centers. To feed the prediction algorithms with multi-domain data, this experiment collects heterogeneous data, such as historical energy consumption, cooling temperature, outdoor weather and building's occupancy and feed the prediction algorithms.

4.1.3 Cloud-based Approach

Cloud computing has reshaped the computing and storage services, which can be used to provide energy-efficient solutions for IoT. More precisely, the cloud-based approach helps in managing the massive data center flexibility and in a more energy-efficient manner [6].IoT involves billions of connected devices mainly communicating through wireless networks, their power consumption is a major concern and limitation for the widespread of IoT. An IoT device does not consume a lot of power by itself, typically from few milli Watts to few Watts. Yet, the increasing number of devices produces a scale effect and causes also a non-negligible impact on Cloud infrastructures that provide the computing power required by IoT devices to offer services. To cope with the traffic increase caused by IoT devices, Cloud computing infrastructures start to explore the newly proposed distributed architectures, and in particular edge Cloud architectures where small data centers are located at the edge of the Cloud, typically in Internet Service Providers' (ISP) edge infrastructures. While the current state of the art offers numerous studies on energy models for IoT devices and Cloud infrastructures, to the best of our knowledge, none of them provides the overall picture. It is thus hard to estimate the energy consumption induced by the increase of IoT devices on Cloud infrastructures for instance. The issue resides in having an end-to-end energy estimation of all the involved devices and infrastructures, including network devices from ISP and Cloud servers. Such results could also serve to identify which part consumes the most, and should then focus the energy-efficient efforts [29].

4.1.4 Low-Power Transceiver

Since the IoT devices applications operate on limited batteries, low-power design architecture or operation framework is of superior importance for addressing the energy management in IoT Mostly, the existing application protocols for IoT devices are not in accordance with the energy efficiency perspective. More specifically, The radio duty cycle for IoT devices is an important factor in energy efficiency, and researchers are exploring methods of reducing the radio duty cycle of IoT devices and subsequently to achieve the energy-efficient architecture [6].

4.1.5 Duty Cycling Techniques

Duty cycling is the fraction of one period in which a signal or system is active Duty cycle is commonly expressed as a percentage or a ratio. A period is the time it takes for a signal to complete an on-and-off cycle. As a formula, a duty cycle (%) may be expressed as shown in (Figure 5). With duty cycling, the energy conservation and increased network lifetime are achieved by alternating the operational mode of the IoT devices or nodes between active and dormant state. They use the ability of an IoT device to operate in various modes to reduce the power being consumed. Examples of such duty cycling can involve powering down the IoT device, putting it in sleep mode where the radio is still active, or putting the IoT device in a deep sleep mode where the radio is turned off and is activate at predefined intervals to listen from the neighbor IoT devices. The drawback of duty cycling is that it could reduce the area being monitored opportunistically offloading the sensor data to smart devices [26].

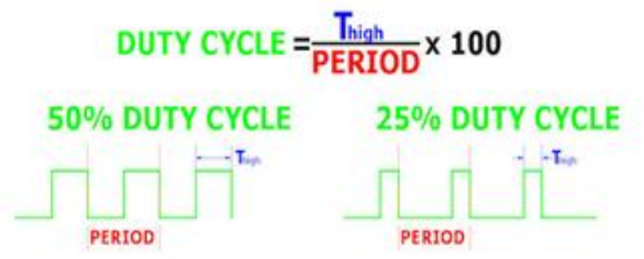

Figure 5: Duty Cycling

Where:
T_{high}: The pulse width.
Period Total period of the signal

4.1.6 Efficient Filtering Techniques

Efficient filtering and sensor data fusion techniques reduce the amount of data that is being transmitted across the network. Since the amount of data being transmitted by the radio of the IoT device is reduced, the radio itself has to be powered for a shorter duration of time than what it would have been normally. This leads to reduced power consumption at the IoT devices. While such sensor data filtering and fusion techniques are extremely efficient and successful at reducing the power being consumed at the IoT devices, they also have drawbacks. Such techniques are not effective when regulatory requirements impose finer granularity of data being reported to satisfy the SLAs [26].

4.1.7 Mobile Ferry Based Techniques

Mobile ferry based techniques when the IoT device that can move across the IoT network. This mobile ferry travels around the network visiting the IoT devices in it to receive the sensor data collected by them. Once it has collected the data from the entire network, it returns to the BS to offload the data before embarking on the travel again. Such techniques require the IoT devices to have a large buffer to store the data till the arrival of the mobile ferry which is costly. While using a mobile ferry works well for delay tolerant network [26].All the above techniques optimize and adapt energy usage to maximize the lifetime of a sensor node, the lifetime remains bounded and finite. The above techniques help expand the application lifetime and/or the time interval between battery replacements but do not prevent energy related inhibitions. With a finite energy source, seldom can all the performance parameters be optimized simultaneously, e.g., higher battery capacity implies increased cost, low duty cycle implies decreased sensing reliability, higher transmission range implies higher power requirement and lower transmission range implies transmission paths with more number of hops resulting in energy usage at more number of nodes.

4.2 Energy Harvesting

There is a major limitation in WSN nodes which is finite battery capacity—nodes will operate for a finite duration, only as long as the battery lasts. As we mentioned before finite node lifetime implies finite lifetime of the applications or additional cost and complexity to regularly change batteries. Nodes could possibly use large batteries for longer lifetimes, but will have to deal with increased size, weight and cost. Nodes may also choose to use low-power hardware like a low-power processor and radio, at the cost of lesser computation ability and lower transmission ranges. Several techniques have been proposed to maximize the lifetime of the battery-powered sensor node. Harvesting is an alternative technique that has been applied to address the problem of finite node lifetime. Energy harvesting refers to harnessing energy from the environment or other energy sources (body heat, foot strike, finger strokes) and converting it to electrical energy. The harnessed electrical energy powers the sensor nodes. If the harvested energy source is large and periodically / continuously available, a sensor node can be powered permanently. Further, based on the periodicity and magnitude of harvestable energy, system parameters of a node can be tuned to increase node and network performance. Since a node is energy-limited only till the next harvesting opportunity (recharge cycle), it can optimize its energy usage to maximize performance during that interval. For example, a node can increase its sampling frequency or its duty-cycle to increase sensing reliability, or increase transmission power to decrease length of routing paths [3]. In section we will discuss briefly harvesting sources, harvesting architecture, storage technologies, harvesting Techniques and energy harvesting challenges.

4.2.1 Harvesting Architecture

Energy harvesting architecture can be divided into architectures as the following:

4.2.1.1 Harvest - Use Architecture

Energy is harvested just in time for use (no storage capability). As shown in (Figure 6) the harvesting system directly powers the sensor node and as a result, for the node to be operational, the power output of the harvesting system has to be continuously above the minimum operating point. If sufficient energy is not available, the node will be disabled. power point will cause the sensor node to oscillate in ON and OFF states. A Harvest-Use system can be built to use mechanical energy sources like pushing keys/buttons, walking, pedaling [3].

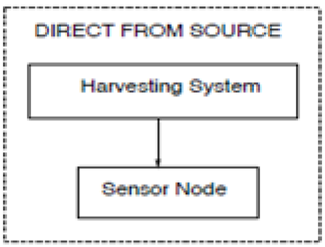

Figure 6: Harvest-Use Architecture [3]

4.2.1.2 Harvest –Store-Use Architecture

The Harvest-Store-Use architecture energy is harvested whenever possible and stored for future use (storage capability). As shown in (Figure 7) the architecture consists of a storage component that stores harvested energy and also powers the sensor node. Energy storage is useful when the harvested energy available is more than its current usage. Alternatively, energy can also be stored in storage until enough has been collected for system operation. Energy is stored to be used later when either harvesting opportunity does not exist or energy usage of the sensor node has to be increased to improve capability and performance parameters. The storage component itself may be single-stage or double stage. Secondary storage is a backup storage for situations when the Primary storage is exhausted. As an example, a Harvest-Store-Use system can use uncontrolled but predictable energy sources like solar energy. During the daytime, energy is used for work and also stored for later use. During night, the stored energy is conservatively used to power the sensor node [3].

.

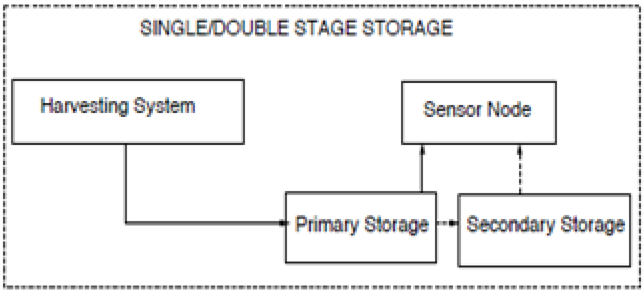

Figure 7: Harvest –Store -Use Architecture [3]

References

[1] Azmoodeh, Amin, et al. "Detecting crypto-ransomware in IoT networks based on energy consumption footprint." Journal of Ambient Intelligence and Humanized Computing (2017): 1-12.
[2] Shin, Minchul, and Inwhee Joe. "Energy management algorithm for solar-powered energy harvesting wireless sensor node for Internet of Things." Iet Communications 10.12 (2016): 1508-1521.
[3] Sudevalayam, Sujesha, and Purushottam Kulkarni. "Energy harvesting sensor nodes: Survey and implications." IEEE Communications Surveys & Tutorials 13.3 (2011): 443-461.
[4] https://justcreative.com/2018/11/19/internet-of-things-explained/ 1/4/2019.
[5] Park, Sang-Hyun, Seungryong Cho, and Jung-Ryun Lee. "Energy-efficient probabilistic routing algorithm for internet of things." Journal of Applied Mathematics 2014 (2014)
[6] Ejaz, Waleed, et al. "Efficient energy management for the internet of things in smart cities." IEEE Communications Magazine 55.1 (2017): 84-91.
[7] Nair, Karan, et al. "Optimizing power consumption in IoT based wireless sensor networks using Bluetooth Low Energy." 2015 International Conference on

Green Computing and Internet of Things (ICGCIoT). IEEE, 2015.
[8] Khanouche, Mohamed Essaid, et al. "Energy-centered and QoS-aware services selection for Internet of Things." IEEE Transactions on Automation Science and Engineering 13.3 (2016): 1256-1269.
[9] Ye, Wei, John Heidemann, and Deborah Estrin. "An energy-efficient MAC protocol for wireless sensor networks." Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Vol. 3. IEEE, 2002.
[10] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015): 2347-2376.
[11] https://en.wikipedia.org/wiki/Radio-requency_identification.30/3/2019.
[12] Want, Roy. "Near field communication." IEEE Pervasive Computing 3 (2011): 4-7.
[13] Ferro, Erina, and Francesco Potorti. "Bluetooth and Wi-Fi wireless protocols: a survey and a comparison." IEEE Wireless Communications 12.1 (2005): 12-26.
[14] Elkhodr, Mahmoud, Seyed Shahrestani, and Hon Cheung. "Emerging wireless technologies in the internet of things: a comparative study." arXiv preprint arXiv:1611.00861 (2016).
[15] IEEE Standard,"IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Std 802. 15. 4-2011, 2011.
[16] G. V. Crosby and F. Vafa,"Wireless sensor networks and LTE-A network convergence," in Local Computer Networks (LCN), 2013 IEEE 38th Conference On, 2013, pp. 731-734..
[17] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe and T. Thomas," LTE-advanced: next-generation wireless broadband technology [Invited Paper]," Wireless Communications, IEEE, vol. 17, pp. 10-22, 2010.
[18] A. Dunkels, B. Gronvall and T. Voigt,"Contiki - a lightweight and flexible operating system for tiny networked sensors," in Local Computer Networks, 2004. 29th Annual IEEE International Conference On, 2004, pp. 455-462.
[19] X. Xiaojiang, W. Jianli and L. Mingdong,"Services and key technologies of the internet of things," ZTE Communications, vol. 2, pp. 011, 2010.
[20] P. Barnaghi, W. Wang, C. Henson and K. Taylor," Semantics for the Internet of Things: early progress and back to the future," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 8, pp. 1-21, 2012.
[21] https://en.wikipedia.org/wiki/System_on_a_chipl. 30/3/2019
[22] https://en.wikipedia.org/wiki/Transceiver.29/3/2019.
[23] http://computernetworkingtopics.weebly.com/star-topology.html. 12/3/2019.
[24] https://en.wikipedia.org/wiki/File:True_Mesh_Diagram.svg.2/4/20019.
[25] Kazmi, Saqib, et al. "Towards optimization of met heuristic algorithms for IoT enabled smart homes targeting balanced demand and supply of energy." IEEE Access (2017).
[26] https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php. 30/3/2019.
[27] Dhondge, Kaustubh, Rajeev Shorey, and Jeffrey Tew. "Hola: Heuristic and opportunistic link selection algorithm for energy efficiency in industrial internet of things (iiot) systems." 2016 8th international conference on communication systems and networks (COMSNETS). IEEE, 2016.
[28] http://fiesta-iot.eu/index.php/fiesta-experiments/b-model/ 2/4/2019.
[29] Kamalinejad, Pouya, et al. "Wireless energy harvesting for the Internet of Things." IEEE Communications Magazine 53.6 (2015): 102-108.).
[30] Hassan, Muhammad, and Amine Bermak. "Solar harvested energy prediction algorithm for wireless sensors." 2012 4th Asia Symposium on Quality Electronic Design (ASQED). IEEE, 2012.
[31] Vullers, Rudd JM, et al. "Energy harvesting for autonomous wireless sensor networks." IEEE Solid-State Circuits Magazine 2.2 (2010): 29-38