MSc thesis

Master's Programme in Computer Science

The Secure and Energy Efficient Data Routing in the IoT based Network

Nepali, Santosh

June 10, 2020

FACULTY OF SCIENCE

UNIVERSITY OF HELSINKI

Supervisor(s)

Prof. Jussi Kangasharju

Examiner(s)

Dr. Walter Wong

Contact information

P. O. Box 68 (Pietari Kalmin katu 5)
00014 University of Helsinki,Finland

Email address: info@cs.helsinki.fi
URL: http://www.cs.helsinki.fi/

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty Faculty of Science	Koulutusohjelma — Utbildningsprogram — Study programme Master's Programme in Computer Science

Tekijä — Författare — Author

Nepali, Santosh

Työn nimi — Arbetets titel — Title

The Secure and Energy Efficient Data Routing in the IoT based Network

Ohjaajat — Handledare — Supervisors

Prof. Jussi Kangasharju

Työn laji — Arbetets art — Level MSc thesis	Aika — Datum — Month and year June 10, 2020	Sivumäärä — Sidoantal — Number of pages 64 pages, 65 appendice pages

Tiivistelmä — Referat — Abstract

The business applications such as weather forecasting, traffic management, weather forecasting, traffic management, etc., are enormously adopting Internet of Things(IoT). While scaling of these applications are fast, the device/sensor capabilities, particularly in terms of battery life and energy efficiency is limited. Despite of intensive research conducted to address these shortcomings, Wireless IoT Sensor Network(WIoTSN) still cannot assure 100% efficient network life. Therefore, the core objective of the thesis is to provide an overview of energy efficiency of proactive(OLSR) and reactive(DSR and AODV) data routing protocols by scaling the size of network, i.e. number of sensor nodes, data packet size, data transmission rate and speed of mobile sink node. It also reviews the importance of security in WIoTSN.

The two approaches, such as literature review and simulation testing, are used to achieve the objective of the thesis. The literature review provides information about reactive and proactive protocols and their mechanism for route discovery. Similarly, the network simulator tool NS3 is used for running simulation to evaluate the performance of selected routing protocols for energy efficiency.

The thesis results showed the effect of scaling the parameters selected for experimental purpose on the energy efficiency of proactive and reactive data routing protocols. The simulation results prove that the reactive protocol DSR outperforms another reactive protocol AODV and proactive protocol OLSR in energy efficiency. From the security perspective, the thesis also emphasizes its need in IoT and suggest to minimize wasteful resources in WIoTSN and use them by restructuring the network for secure energy-efficient data routing protocols.

ACM Computing Classification System (CCS)
General and reference → Document types → Surveys and overviews
Applied computing → Document management and text processing → Document management → Text editing

Avainsanat — Nyckelord — Keywords

WIoTSN, Energy Efficiency, Security, Proactive, Reactive, Routing

Säilytyspaikka — Förvaringsställe — Where deposited

Helsinki University Library

Muita tietoja — övriga uppgifter — Additional information

Networking and Services study track

Contents

1 Introduction

The rapid urbanization is straining the existing resources of urban living. Every human being enjoys living an urban lifestyle. Therefore, it is expected more of the world's population is in cities in recent years. Consequently, the demand for facilities and services also increase with the growth of towns and the people living in these cities. The technology comes to the rescue of ever-growing demand. Internet of Things(IoT) is such technology which improves various aspects of urban life. The World Economic Forum's [28] also focusing on the digital economy and social system to ensure digital future inclusive, trustworthy and sustainable. It is expected that IoT [69] will encompass around 75 billion units connected by 2025. Similarly, the IoT's economic contribution will be approximately $11.1 trillion [28], which is 14% of today's global Gross Domestic Product(GDP) by 2025.

Internet of Things(IoT) [13] is a network of heterogeneous communicating devices which are exchanging data without human intervention to provide smart services to end-users. During recent years, the field of IoT has been witnessing under significant research and developments. Smart metering, smart home appliances, intelligent road traffic management, smart security and smart weather forecasting system are use case examples of IoT. The network of IoT is more complex and broad in scale, which is composed of objects like Radio Frequency Identification(RFID) tags, sensing devices and mobile phones. These objects are used to obtain data from the physical parameters of the environment, and also known as sensor nodes, have low computational power and battery life. Sometimes sensor nodes may use the solar system to get energy.

The studies show [10] that the routing is a crucial part for IoT applications. Different routing protocols have been using to define the path or route between sender and receiver. According to the Encyclopedia [65] "routing protocol" is defined as follow:

> ***"A formula used by routers to determine the appropriate path onto which data should be forwarded. The routing protocol also specifies how routers report changes and share information with the other routers in the network that they can reach. A routing protocol allows the network to dynamically adjust to changing conditions; otherwise, all routing decisions have to be predetermined and remain static."***

According to the above definition, the routing protocol decides the way to forward packets to other sensor nodes. Based on route discovery, there are proactive, reactive and hybrid routing protocols. In proactive routing protocols, as soon as sensor nodes start, they exchange control messages periodically to update the routes information in the network. These protocols are also known as table-driven protocols. These protocols share its routing information among all sensor nodes in the network. On the other hand, the reactive protocols define routes whenever needed. Therefore, these protocols are known as table-less or on-demand routing protocols. Thus, these protocols require more time to find the path. Similarly, a hybrid routing protocol unites the capabilities of reactive and proactive protocols to achieve better results while routing. Adhoc On-demand Distance Vector(AODV), Dynamic Source Routing (DSR) are examples of reactive routing protocols. Similarly, Optimized Link State Routing (OLSR) is an example of a proactive routing protocol, and a hybrid routing protocol is the Zone Routing Protocol(ZRP).

Wireless IoT sensor Network, as mentioned above, nodes work in energy supplied from the battery with limited power for a limited time and also have limited storage and processing capabilities. Typically, nodes are deployed in the region where human access is almost not possible. Thus, replacing the battery is not possible. Therefore, among different kinds of problems, power consumption [21] is a significant obstacle for wireless IoT sensor network. The studies show [10] that the routing is a crucial part for IoT applications for power consumption. But, it is a difficult task for researchers to design robust energy-efficient routing protocols for generalized IoT applications. Many researchers developed different protocols, but the energy issue remains. It is because efficient power consumption or energy-efficient routing protocol is an open field of research, and researchers are still working on it. The system needs more and more energy-efficient routing protocols for the increase of network life and performance of the IoT applications.

In light of the motivations, as mentioned earlier, this thesis aims to find out the operational difference of proactive and reactive protocols in terms of power efficiency while routing data between sensor nodes.

1.1 Problem Statement

As mentioned in the introduction, sensor nodes in an IoT generate data at a high and rapid speed; energy is spent in both transmission and reception of the message. For a successful message transmission, the amount of energy used depends on several factors, such as distance between sensor nodes and sink nodes, length of the message to be delivered, operational energy cost incurred by transmitter and receiver hardware etc. The purpose of this thesis is to study the energy efficiency of proactive and reactive routing protocols, especially AODV, DSR and OLSR routing protocols. These protocols have different characteristics for wireless routing. The main problem is to select the correct and energy-efficient routing protocol. Therefore, this thesis addresses the following challenges:

"Which routing protocols(reactive and proactive) support in energy efficiency?"

The ***"routing protocols"*** refers to the existing implementation of the proactive protocol such as OLSR and reactive protocols such as AODV and DSR.

The word ***"support"*** refers to the performance of sensor nodes for the utilization of energy.

Similarly, ***"energy efficiency"*** refers to appropriate power consumption by nodes to find route for packet communication.

In order to answer the research question, the following steps will be investigated:

- Research of literature to identify energy efficiency of proactive and reactive routing protocols.
- Simulation using Network Simulator 3(NS3)for OLSR(proactive protocol) and AODV and DSR(reactive protocol) protocols scaling following parameters to check their average energy consumption:
  - Number of nodes
  - Data Packet size
  - Data transmission rate
  - Sink speed

1.2 Organization of the Thesis

The rest of the thesis is structured as follows. Chapter 2 begins with a brief introduction to IoT with its current market status. Similarly, the security threats and its measures in WIoTSN are also discussed. In the chapter, special attention is given to the energy efficiency in data routing.

Chapter 3 introduces different types of communication model in the IoT network along with kinds of IoT network. It also includes differences between ad-hoc wireless network, wireless sensor network and IoT with some introduction. This chapter primarily focuses on route discovery methods of a proactive protocol(OLSR) and reactive protocols(AODV and DSR).

Chapter 4 starts with the introduction of different open source and proprietary network simulation tools. Among the available network simulation tools in the market, one is chosen, i.e. NS3. It also describes the experimental setup and parameters selected for simulating to study the energy efficiency of OLSR, DSR and AODV routing protocols.

Chapter 5 describes the results of simulation on the energy efficiency of OLSR, DSR and AODV routing protocols. Here the energy efficiency of above routing protocols is analyzed and evaluated by scaling the network size, data packet size, data transmission rate and speed of mobile sink nodes. This chapter also highlights the importance of security in WIoTSN.

Chapter 6 concludes the research of the thesis by highlighting some critical keynotes.

2 Background

This chapter provides an overview of the related theoretical and practical concepts which are relevant to the presentation of this thesis. A discussion of similar previous work is also carried out to show state-of-the-art solutions. This thesis is well placed with the development of energy-efficient routing protocol for wireless IoT sensor nodes in IoT applications and its performance evaluation.

2.1 Internet of Things(IoT)

The history of the Internet of Things(IoT) has not been so long. However, the vision of machines communicating each other exists from the early 1800s. During the 1830s to 1840s, telegraph(the first landline) was developed as machines communication. The first voice transmitting device "wireless telegraphy" on 3rd June 1900, providing another necessary component for developing the IoT. The beginning of computer development by 1950s and the Internet started as part of Defense Advanced Research Projects Agency(DARPA) in 1962, which is later evolved into the Advanced Research Projects Agency Network(ARPANET) added significant path towards IoT. The support for public use of ARPANET from the commercial service provider in 1980s helps to develop new Internet service. It is believed new Internet service is milestones for IoT development. In Early 1993, installation of Global Positioning Satellites by Department of Defence encouraged private sectors to place satellites for commercial purpose in orbit. It is because satellites and landlines are the primary communications medium for much of the IoT [11]. The Internet Protocol Version 6(IPV6) addresses play a crucial role in developing a functional IoT. The Computer History Museum expert Steve Leibson states [11]:

"The address space expansion means that we could assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths."

It means we are not going to run out of internet addresses supporting millions and billions of IoT devices. The Internet of Things, as a concept was officially named only in 1999 by Kevin Ashton during his work at ProcterGamble(P&G) as he was working in supply chain optimization [29]. But, the first example of an Internet of Things is from the early 1980s as a coke dispenser linked via the Internet to check availability of coca-cola, at the Carnegie Melon University. Even though Kevin grabbed the attention of his executives at PG, the term Internet of Things(IoT) was still unfamiliar among the people. In 2005, the concept of the Internet of Things(IoT) was reported for the first time by International Telecommunication Union (ITU) stating future society will be a “ubiquitous network society” where many smart devices can be connected to the Internet [32][6]. The concept of IoT caught the attention of people in 2010 when information leaked that Google’s StreetView service not only stored pictures but also saved the data of people’s WiFi network. The following activities have outgrown “Internet of Things” and their other related concepts [29]:

- In 2010, China published its five-year plan with strategic development of IoT.
- In 2011, famous market research company Gartner listed IoT as “hype-cycle for emerging technologies”.
- In 2012, Europe’s most prominent Internet Conference “LeWeb” defined “IoT” as their central theme.
- In 2012, the popular technology-focused magazines like Forbes, Fast Company and Wired started to use IoT to describe their methods.
- In January 2014, Google announced to buy Nest for $3.2 billion to operate as Google Nest for a smart home.
- In 2014, Consumer Electronic Show(CES) was held in Las Vegas under theme IoT.

Recently, the researchers from University of Massachusetts(UMass), Amherst [36][12], have developed an IoT device called *FluSense,* that uses machine learning model to track the presence of influenza-like illness. It uses data of coughing sound and crowd size sampled in a large group in real-time. *FluSense* can be expanded as a health surveillance tool to forecast seasonal flu or other viral respiratory outbreaks such as Corona Virus Disease 2019(COVID-19) pandemic. This IoT model helps to save lives by directly informing public health centres, imposing potential travel restrictions to stop spreading of virus and also allowing proper allocation of medical supplies during a flu epidemic.

2.1.1 Definition

The term Internet of Things(IoT) known to everyone, but it is hard to find a single universally accepted definition. It is believed that diversified groups used a different meaning to promote their view about IoT. For example, consider the following definitions.

In 2015, the journal “Architectural Considerations in Smart Object Networking” published by Internet Architecture Board(IAB) [54] had following description:

“The term ”Internet of Things”(IoT) denotes a trend where a large number of embedded devices employ communication services offered by Internet protocols. Many of these devices, often called ”smart objects”, are not directly operated by humans but exist as components in buildings or vehicles, or are spread out in the environment.”

The term “smart object networking” is commonly used to represent the Internet of Things by the Internet Engineering Task Force(IETF) [3], which has significant constraints such as limited resource, memory, power, bandwidth etc. According to the article [22] published by the International Telecommunication Union(ITU), the concept of interconnectivity has been discussed but does not specify IoT to the Internet. But later, the paper published in the Institute of Electrical and Electronics Engineers(IEEE) communication magazine [42], defines the connectivity of IoT to the cloud services.

All of these definitions describe a scenario of network connectivity and computing capabilities of a self-configured object, devices, sensors which are not ordinarily considered to be the computer. Those devices are capable of generating, exchanging and consuming data with minimal human intervention. It is also considered IoT as the connectivity of similar as well as heterogeneous devices. The Internet of Things enables tools(things) to interact and coordinate with each other, thereby reducing human intervention in basic everyday tasks.

To get a better understanding of IoT, consider the scenario of a smart home. As soon as the alarm rings to wake up if it sends a signal to the coffee maker and the toaster, which automatically starts doing their jobs without any human intervention. This application area is saving time, significantly reducing human effort and improving the quality of life, is known as the **Internet of Things**. A network of heterogeneous or homogeneous devices/applications has its own set of challenges. Moreover, the communication among the devices as well as with related services is expected to happen anytime, anywhere for anybody, anything with any service following any network path as explained in figure 2.1, in a wireless, ad-hoc way. The services become decentralised and complex. Consequently, the security barriers in the Internet of Things become much thinner.

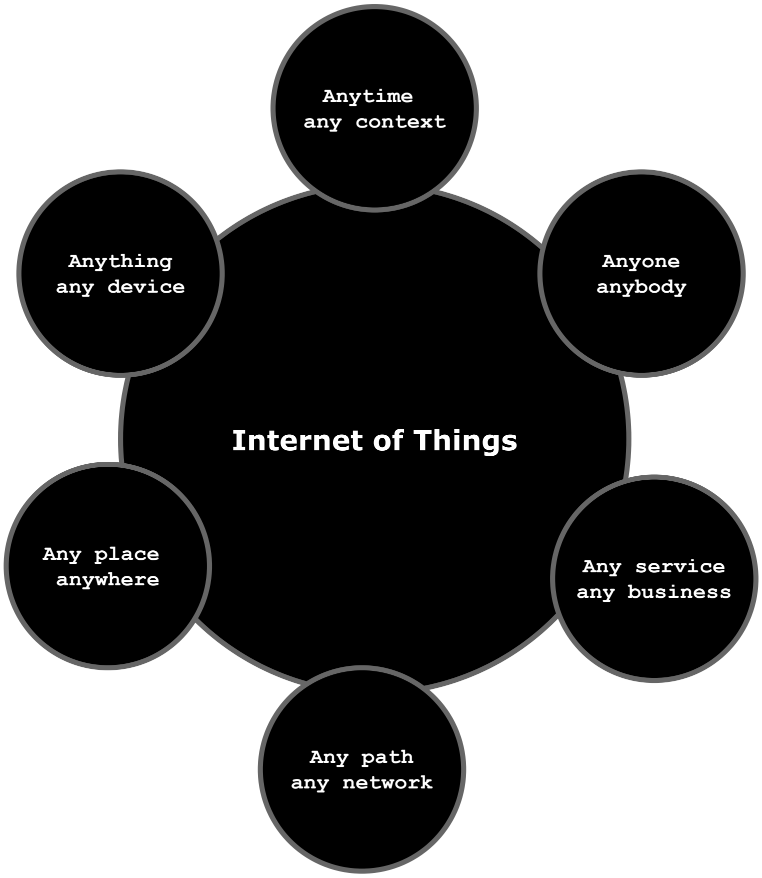

Figure 2.1: Definition of IoT, figure redrawn from [41]

The IoT is not a single technology; it is a concept in which most new things are connected and enabled. For example, street lights being networked and things like embedded sensors, image recognition functionality, augmented reality, near field communication, is integrated into situational decision support, asset management and new services. These bring many business opportunities and add to the complexity of IoT [41]. Due to the complexity of IoT, it is still considered IoT field in its early stage.

Therefore, the Lexico dictionary powered by dictionary.com and Oxford university [61] offers a concise definition invoking the Internet as a significant element of the IoT as following:

"The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data."

2.1.2 Features of IoT System

To build a clear mental picture of IoT, which has been defined, it is fruitful to list the features of IoT. The characteristics of IoT, according to [33][17] are:

- ***Interconnection of Things:*** It is the first feature which is derived from the name itself. It is the system that deals with a link between "things". Here the word "things" refers to physical objects or devices which are useful for a user or any application.

- ***Connection of Things to the internet:*** It is another essential feature of IoT. Here self-organizing devices(Things) are connected to the internet, but it is not the system of Intranet of Things or Extranet of Things.

- ***Uniquely Identifiable Things:*** To build communication between IoT devices, each device are supposed to retain unique identification, which is defined by their addresses.

- ***Ubiquity:*** According to ITU's definition for IoT [22], ubiquity is the primary feature. It indicates a network of IoT system is available anywhere and anytime. But anywhere does not mean "globally" instead, it refers to the concept of where it is needed. Similarly, anytime does not mean "always" instead, it relates to the idea of when it is required.

- ***Sensing and Actuation capability:*** Sensors and actuators are used in IoT system. They give sensing and actuation operation, adding smartness to the "Things" or "devices".

- ***Interoperable Communication Capability:*** IoT system uses standard communication protocol which allows the sensors or actuators to be interoperable.

- ***Self-configurability:*** It is a significant feature of the IoT system. The actions of neighbour and service discovery, network organization and resource provisioning fall under self configurability. Due to the heterogeneity of IoT devices such as sensors, actuators, mobile phones, network elements connected to the internet need to manage themselves in terms of software and hardware configurations and the utilization of their resources. Here resources utilization refers to energy used, communication method, bandwidth used, medium access etc.

- ***Programmability:*** Devices or Things of the IoT system support programmability. Here programmability means a user can configure the IoT system as per the wish without changing physical features. Therefore, quick and easy changes in the IoT system is possible.

2.1.3 Advantages and Disadvantages of IoT

The applications of IoT are used in various field, and it dominates multiple areas. However, there are many challenging issues in the context of the use of IoT. As mentioned in [67], the following are advantages and disadvantages of IoT.

Advantages:

- ***Access Information:*** Smart sensory devices are connected to facilitate communication between them. They provide the facility to access information from any location without being physically present in real-time.
- ***Communication:*** It is possible to make faster and efficient communication between interconnected sensor devices.
- ***Cost-Effective:*** As mentioned in the above point, the faster and efficient communication between networked sensor devices makes the daily task easy along with saving time and money.
- ***Automation:*** Automation is the primary advantage of IoT. Automation task increases efficiency and quality of service, avoiding human error.

Disadvantages:

- ***Security and Confidentiality:*** It is one of the biggest challenges in the IoT. Every device is communicating via the Internet. The confidentiality and security of the data transmitted are at high risk and has chances of being hacked by hackers.
- ***Complexity:*** The IoT is a giant network encompassing various devices under it. The single minute loophole in the hardware or software can affect the entire system resulting in catastrophic consequences. Therefore, it is the most complicated aspect of IoT.

- ***Lesser Jobs:*** The need for human labour declined sharply due to the automation of every task. The uses of IoT devices are drastically increasing, as shown in figure 2.2 and the voice of "**future IoT**" has been raising. There will be a visible decline in hiring professionals.

- ***Technological Dependability:*** There is no doubt technology is dominating the human lifestyle and witnessing a significant shift in its implementation in our daily lives. Thus, this reflects a human's dependability on technology and affecting necessary human social interaction skills. People enjoy virtual interactions than real-life ones resulting from lower self-esteem and raising depression patients.

2.1.4 Architecture of IoT

The Internet of Things(IoT) involves a growing number of smart interconnected devices and sensors.

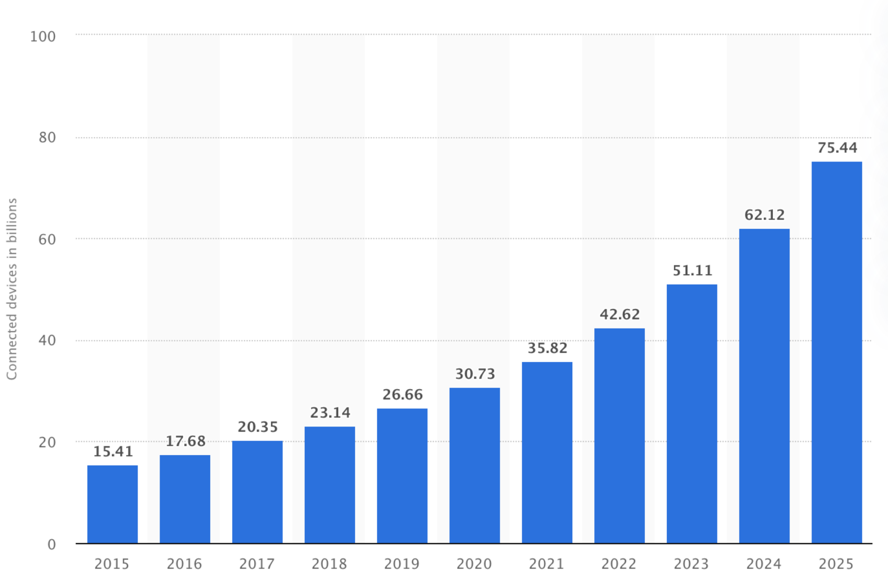

Figure 2.2: Total Number of Active Device Connections Worldwide, figure from [69]

As shown in figure 2.2, the projection of numbers of active device connection grows from 15.41 billion to 75.44 billion between 2015 to 2025, respectively [69]. Based on this prediction, the complexity of the IoT system also increases when the number of active device connection grows. Despite its complexity, communication, as well as its related services, should be available anytime and anywhere when and where they are needed respectively. Thus, to manage the complexity IoT architecture is necessary. In this context as shown in figure 2.3, the term architecture is defined as a structure of the network's physical components and their operational principles and procedures based on their functional organization and configuration and also data formats used in operation [57].

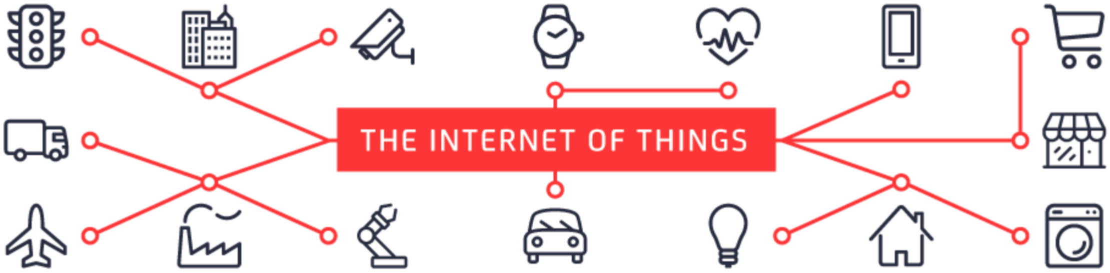

Figure 2.3: Basic Architecture of IoT, figure redrawn from source [57]

However, every IoT system is different, but its foundation for each IoT architecture as well as its primary data processing flow is roughly the same. There is no single view on the architecture of IoT which are universally accepted as researchers purpose different architectures. According to [59], the building block of IoT architecture is devices/things, IoT data acquisition systems and gateway, edge devices and data centres. Here, devices or things are objects which are connected to the internet where their embedded sensors and actuators can sense the environment. IoT data acquisition systems and gateway receive raw data through embedded sensors and actuators of things. This block is also responsible for converting raw data into digital streams, filter and preprocess for further analysis. Edge devices are the third layer of IoT architecture where enhanced analysis is performed, and visualization and machine learning system are also introduced. After that, data is transferred to either cloud-based or local-based data centre for depth analysis to actionable insights.

According to the authors from [57] and [46], they have discussed three layers and five layers architectures, which are considered too basic layer concept of IoT architecture and same architecture concept has been followed throughout the thesis.

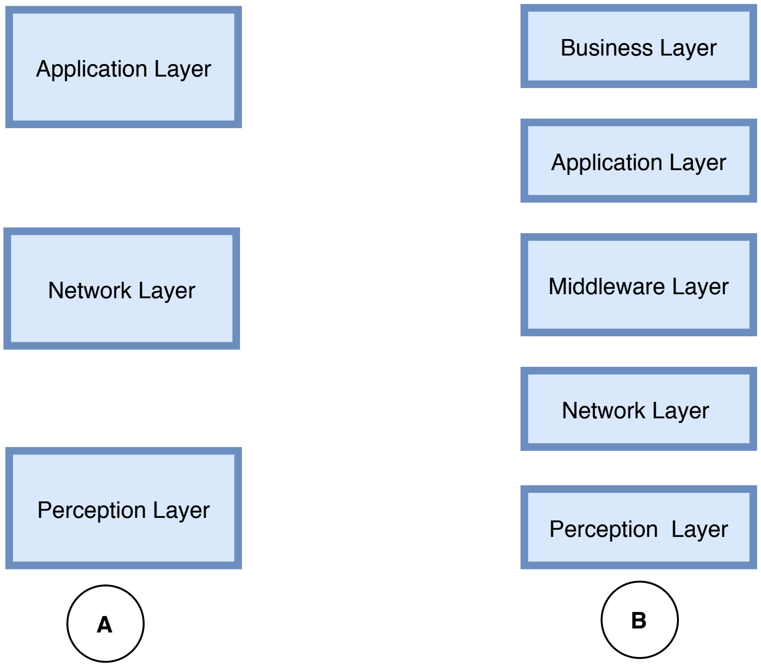

Figure 2.4: IoT Architecture (A): three layers & (B): five layers, figure redrawn from [46] and [57]

The IoT architecture, as shown in figure 2.4, has the following features:

- ***Perception Layer:*** Perception layer is also known as the physical layer, which consists of embedded sensors and actuators which are used for gathering information from the environment. This layer is also responsible for maintaining device identification and forwarding collected data to the network layer for its secure communication.

- ***Network Layer:*** Network layer is also known as a transport layer that maintains confidentiality of data received from the perception layer and securely forward to upper layer toward the central data processing system. It uses third-generation(3G), fourth-generation(4G), wireless fidelity(WiFi), Wireless Interoperability for Microwave Access(WiMax), Radio-frequency identification(RFID) etc. depending upon nature of sensors.

- ***Middleware Layer:*** When IoT device is connected and starts to send and receive data, then they generated a various type of services. This primary task of this layer is to manage service and to store layer information in the database or cloud. It is also responsible for retrieving, processing, computing information and making a decision based on calculated results automatically. This layer is also known as processing layer which employs database, cloud computing and big data processing modules.

- ***Application Layer:*** It receives the information processed by the middleware layer and responsible for application management. It delivers application-specific service to the user. Smart postal, smart health, smart car etc. are examples of IoT application.
- ***Business Layer:*** Business layer manages the whole IoT system such as application, business and profit models and privacy of users. It helps managers in making business decisions.

As stated in the previous section, IoT architecture may vary from solution to solution. Still, its core building block provides fundamental features to make sustainable IoT ecosystem such as scalability, availability, maintainability and functionality [59]. Although three-layers architecture defines the main idea of IoT, it is not sufficient for detail and more beautiful research aspects of IoT. Therefore, as mentioned in [46], five layers of architecture are prevalent.

2.1.5 Taxonomy

The taxonomy is based on the architectural elements of IoT presented in subsection 2.1.4. Figure 2.5 highlights the primary research topics in IoT technologies.

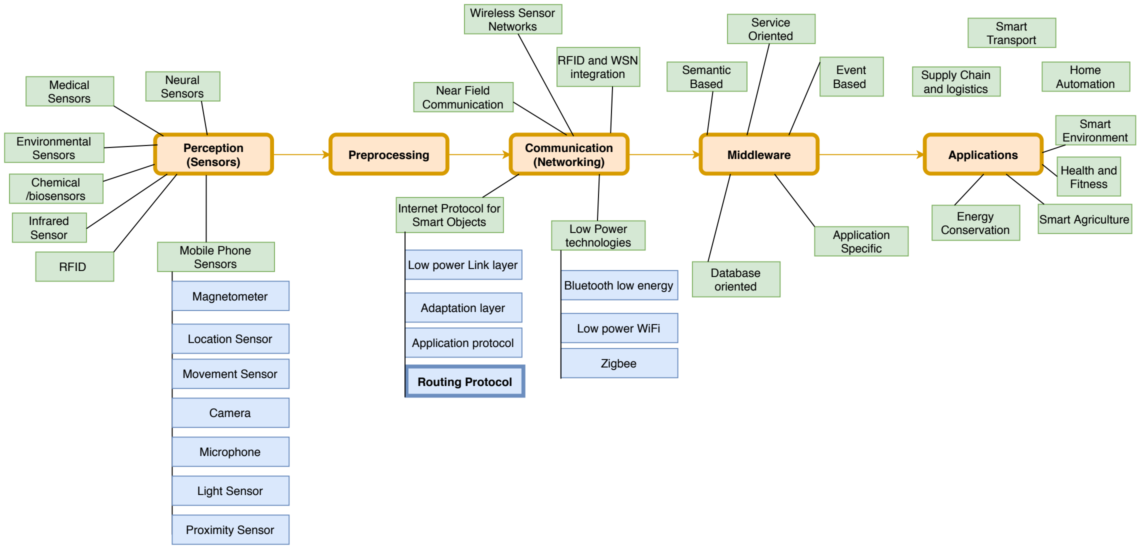

Figure 2.5: Taxonomy of research in IoT technologies, figure redrawn from [46]

The presentation layer is the first architectural component of IoT that collects data using sensors, which are the most critical drivers of the IoT [53]. This layer uses diversified sensors based on the nature of the application. Among them, the most generic sensor available today is smartphones. The smartphone itself has multiple embedded sensors [23] such as location sensor, movement sensor, camera etc. In this layer, there are other sensors used for measuring pressure, humidity, temperature, presence of smoke and gases, neural signals etc. Since it is not the scope of this thesis, the detailed analysis of the presentation layer is not the interest of research.

Preprocessing unit typically deals with the amount of temporary storage, limited processing capacity and security issues. Therefore, they can be a research topic under the preprocessing group. Section 2.2 covers security issues.

Subsequently, another architectural component is communication or networking. The entities of IoT follow a standard protocol based on the nature of their applications. The commonly used technologies for short-range low power communication [46] protocols are Radio Frequency Identification(RFID)and Near Field Communication(NFC) [63]. Similarly, for medium-range technologies like Bluetooth, WiFi, Zigbee etc. are used. Special protocols and mechanisms are needed for IoT communication since they have limited processing, storage and energy capacity. The communication issues such as routing protocol and its energy efficiency that has been highlighted in figure 2.5 are discussed in chapters 3 and 5. Since it is the main scope of this thesis and these chapters highlight the energy efficiency of routing protocols in wireless sensor IoT network.

There are two kinds of software components in IoT architecture such as middleware and application. The middleware hides details of the hardware by creating abstraction for the programmer enhancing interoperability of smart objects. Similarly, the uses of IoT such as home automation, smart grids, smart environment etc. are final output which is realised and experienced by service users. Since their detail study is not the scope of this thesis, middleware IoT architecture does not have a separate section, and however, the below subsection defines application area where IoT implementation and its market status are discussed.

2.1.6 IoT Implementation and its Market

IoT technology has proven milestone for multiple business organization, society by supporting them in digital transformation from traditional practices. As mention in introduction chapter 1, the prediction of the IoT market will contribute 14% of today's global GDP by 2025 [28]. The IoT technology market is multiplying due to adoption of Artificial

Intelligence(AI) and Machine Learning(ML).

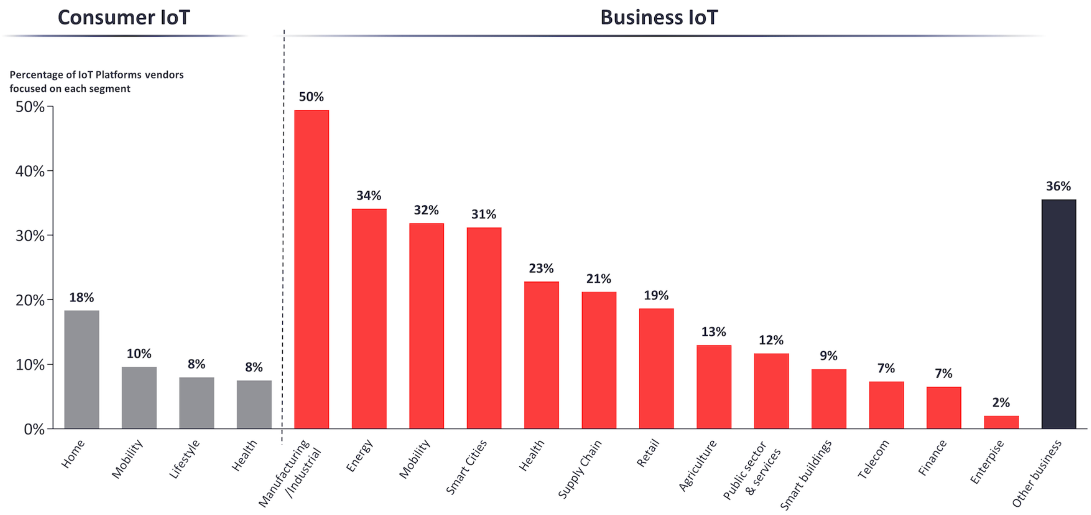

Figure 2.6: Number of Identified IoT Platform-By Industry(Dec 2019), figure from [27]

The market is broadly categorized into two, i.e. Personal use consumer of IoT and business use of IoT, as shown in figure 2.6. The personal use consumer uses IoT products for their benefits such as home security, mobility and lifestyle management, health etc. But, business IoT includes diversified fields such as manufacturing and industries, energy, mobility, smart cities, supply chain management, retail, agriculture management etc. The demand for IoT market is satisfied by IoT platform companies that may be small, medium or large. The IoT Analytics(leading market insight company for IoT), reports 620 active IoT platform companies on the open market [27] till 2019. According to figure 2.6, 50% of all IoT platform profiled companies focused on making smart industrial or manufacturing system [27]. Along with selling the IoT product, they also publish a report on the efficiency gained by the implementation of a smart manufacturing system for positive marketing. The application area of IoT platform in the manufacturing space includes condition monitoring and predictive maintenance, energy monitoring, quality control and comprehensive dashboards and visualizations.

Throughout 2019, the IoT Analytics [26] monitors major development in IoT technology to stabilize IoT markets which are in chronological order in figure 2.7.

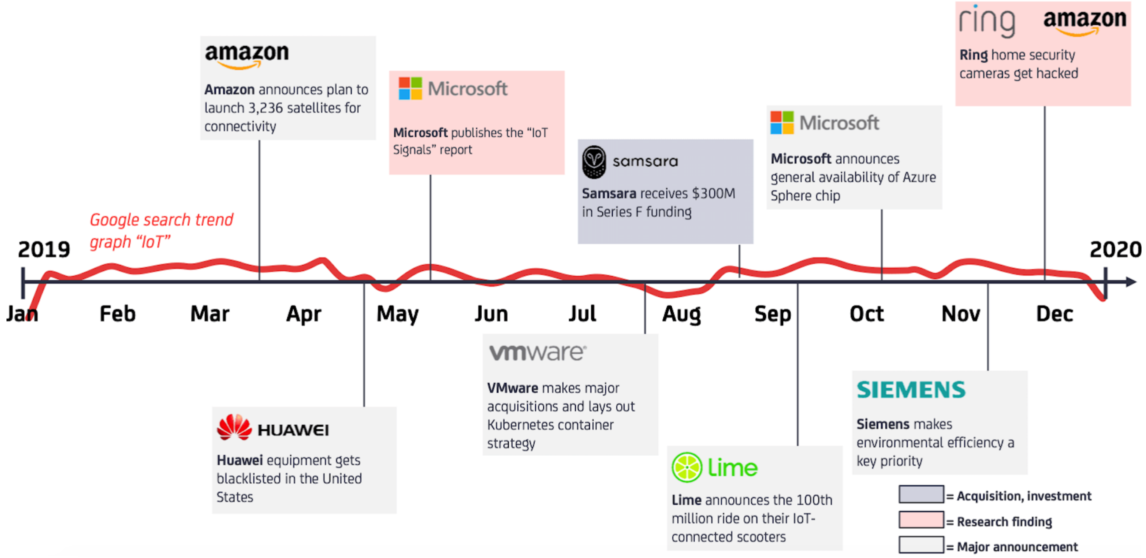
amazon
Amazon announces plan to launch 3,236 satellites for connectivity
Microsoft
Microsoft publishes the "IoT Signals" report
samsara
Samsara receives $300M in Series F funding
Microsoft
Microsoft announces general availability of Azure Sphere chip
ring amazon
Ring home security cameras get hacked
Google search trend graph "IoT"
2019
2020
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
HUAWEI
Huawei equipment gets blacklisted in the United States
vmware
VMware makes major acquisitions and lays out Kubernetes container strategy
Lime
Lime announces the 100th million ride on their IoT-connected scooters
SIEMENS
Siemens makes environmental efficiency a key priority
= Acquisition, investment
= Research finding
= Major announcement

Figure 2.7: The IoT year 2019 in review, figure from [26]

It is describing research finding, major announcement and acquisition and investment throughout the year. The several companies, such as Eutelsat and Amazon, are planning to launch nano-satellite for new IoT connectivity for ubiquitous connection. The most influencing report known as "IoT Signal" was published by Microsoft highlighting IoT current adoption and top use cases. Similarly, Samsara receives $300 million funds, who is famous for making IoT hardware and software. Light IoT-enabled vehicles such as smart scooters are getting widespread enhancing impressive growth of micro-mobility solution. The celebration of Lime, which is famous in 120 different countries, reaches 100 million rides connecting with IoT.

The overall activities in 2019 give bright symbols for 2020 in the IoT market, but it is wise to handle it properly.

2.2 Security

In October 2016, hackers found a vulnerability on a specific model of security camera and started to attack several social network websites, including twitter using around 300,000 IoT video recorders [60]. Similarly, the US-based company Wyze Labs, Inc., reported in December 2019 [26] of being hacked on its smart home security system affecting 2.4 million customers. Kaspersky Lab is a Moscow, Russia based multinational cybersecurity and antivirus provider company [26], reported of detecting one hundred million of IoT device hacks in 2019 and the ratio is increased by nine times from previous years. Since the internet is the underlying foundation of IoT, the issues of security exist on the internet also appear in IoT platform. The above given an example is just an example of an attack that might happen due to inadequate protection in IoT devices. Similar to the video camera, the IoT devices such as smart locks, smart vehicles, intelligent toys etc. which are connected to the internet poses IoT security challenges.

IoT is a beautiful technology and supporting humanity, but it is not yet technically matured. The entire IoT environment, including manufacturers to users, still have many security challenges to overcome because of the following causes, as mentioned in the [60]:

- ***Lack of Compliance on the part of IoT Manufacturers:*** A lot of new IoT devices are introduced without considering vulnerabilities. For example, most fitness trackers with Bluetooth connectivity remain visible after a successful pairing; smart refrigerator exposes Gmail login credentials etc. It is happening because of the lack of universal IoT security standards.

- ***Lack of User Knowledge and Awareness:*** The user's ignorance and lack of awareness of IoT functionality are the primary reason for security challenges. IoT is growing like a mushroom and user's lack of knowledge about it, keeping everyone on risk.

- ***IoT Security Problems in Device Update Management:*** The poor update management of IoT devices adds risk on its security. The use of outdated software or firmware does not protect the system from the latest vulnerabilities. During updating, the device backups copy is sent back to the data centres, i.e. the cloud. If they are transferred insecurely, there is a high chance of information hacking and sensitive information may be stolen.

- ***Lack of Physical Hardening:*** The IoT devices or sensors are spread in remote locations and operating autonomously without any human intervention. Therefore, there is a chance of physical tampered. It is the responsibility of manufacturers to design the IoT device physically secured. But it is a tough task for the manufacturer to build secured sensors and transmitters in a very low-cost device. Users are also responsible for their physical protection.

2.2.1 Security Threats in IoT

The three layers, as shown in figure 2.4(A), has its security challenges. According to the [57], the security challenges on presentation, network and application layers are:

- ***Presentation Layer:*** As figure 2.5 describes, the presentation layer consists of mostly sensors, RFID [70]. They are remotely installed in a diversified environment. They use wireless nature of signals for communication. Therefore, sensor nodes are at high risk of being intercepted by hackers and high chances of hardware components being tampered in this layer [31]. Hackers may add additional sensor nodes to the system to challenge the integrity of data causing Denial of Service(DoS) attack. The ultimate result of a DoS attack is to consume more energy of the sensor nodes and putting them into an inactive mode(sleep mode) for saving energy [32]. The additional security threats of this layer are leakage of confidential data, terminal virus, copying etc.

- ***Network Layer:*** While relaying the information received from the perception layer to information processing system through existing communication networks as mentioned in the architecture of IoT, it faces different kinds of security issues such as network content security, hacker intrusion and illegal authorization. The most crucial characteristic of IoT is **"openness"**, [4] which is considered to be one of the reasons for the identification authentication problem. The list of attacks that are considered as a security issue in this layer as described by [57]:

  - ***Sybil Attack:*** It is the kind of attack in which a reputation of the node is subverted by creating multiple identities.
  - ***Sinkhole Attack:*** Sinkhole attack is carried out either by hacking node and introducing compromised or fabricated node in the network. The intruder node or sinkhole node diverts the traffic towards itself from other nodes by presenting false information. Thus, intruder nodes easily manipulated the information of the nodes. Sinkhole attack results in more power consumption.
  - ***Sleep Deprivation Attack:*** Sleep deprivation attack is the attack where victim nodes keep awake, resulting use of more battery. It reduces the lifetime of the cell, causing the victim nodes to shut down.
  - ***Denial of Service Attack:*** In this attack, the IoT network is flooding with unnecessary traffic signals by hackers resulting in service unavailable every time.

  - ***Malicious Code Injection:*** In this attack, the hacker introduces the compromised node by inputting validation flaw in the system to inject malicious code. This results of shutting down the network or gaining full control of the network by an attacker.
  - ***Man-in-the-Middle Attack:*** In this attack, the attacker intercepts the communication between two nodes either by secretly eavesdropping or modifying the traffic signals to monitor and control the private conversation resulting in leakage of information, identity, much more.

- ***Application Layer:*** The reason for developing IoT system and its smart environment realizes at the application layer. The integrity, confidentiality and authenticity of data are essential features of uncompromised data [31], are achieved at a layer of IoT architecture. The authors of [24] addressed following as security threats at the application layer:

  - ***Injection:*** It is a widespread attack where attacker quickly injects malicious code in the application causing data loss, data corruption and providing bad results [34].
  - ***Sniffer/Loggers:*** The attacker introduces a sniffer application into the system which could gain important network information from the network traffic [34], stealing passwords, files and email text [24].
  - ***Session Hijacking:*** The attack discloses personal identities by using security loopholes in authentication and session management [24].
  - ***Distributed Denial of Service(DDoS):*** The working principle of DDoS is similar to DoS. However, multiple attackers become active at the same time [24].
  - ***Social Engineering:*** It is a severe threat for the application layer where the attacker attacks a victim lures into opening a malicious application or email or chats, through which credentials of the victim is gained [34].

2.2.2 Security Measures for IoT

The security solutions with respect the security threats in IoT are classified into three categories, i.e. security of the presentation layer, the protection of the network layer and security of application layer. The security solutions of IoT are summarizing in Figure 2.8.

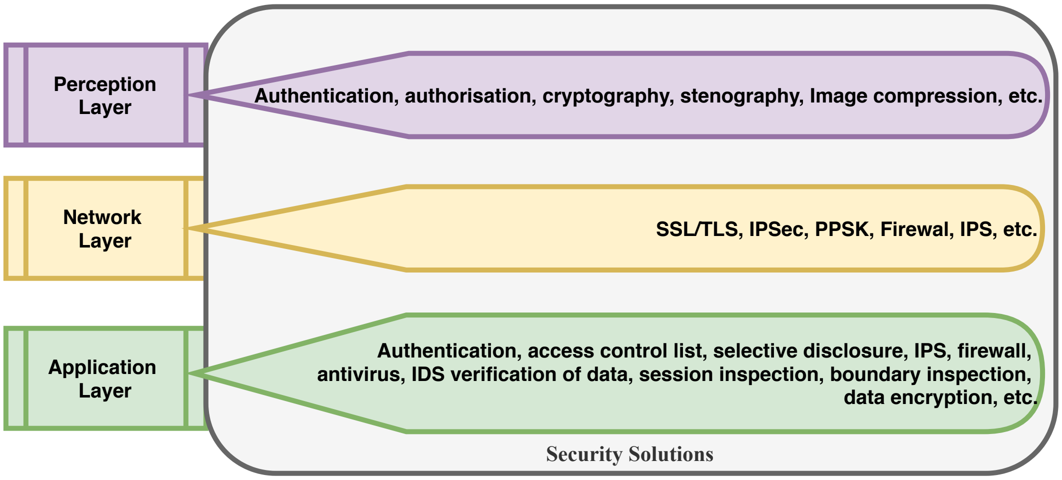
Perception Layer
Authentication, authorisation, cryptography, stenography, Image compression, etc.
Network Layer
SSL/TLS, IPSec, PPSK, Firewal, IPS, etc.
Application Layer
Authentication, access control list, selective disclosure, IPS, firewall, antivirus, IDS verification of data, session inspection, boundary inspection, data encryption, etc.
Security Solutions

Figure 2.8: Security Solutions on Layers of IoT

- ***Security for Perception Layer:*** The IoT devices such as sensors, RFID and other tools need to be adequately secured. The **intellectsoft** has identified poor physical security in the top 10 most significant IoT security issues [60]. Therefore, to obtain data or information produced by physical objects, i.e. IoT devices, it is essential to ensure the only authorised person can have access to sensitive data. The physical identity and access management policy need to be defined to provide secure access [1]. Similarly, following the same standard process authentication and authorisation requirement should be satisfied for IoT. The main issue of this layer is data collection. The security techniques such as multimedia compression, stenography, watermarking, time session, intellectual property can be implemented. Similarly, the use of cryptography method often ensures privacy of data [24].

- ***Security for Network Layer:*** The safety of the Network layer is broadly defined under two sub-heading, i.e. wireless and wired. The vital step for securing wireless is the development of the protocol for authentication and key management [18]. For example, to protect the network layer itself Internet Protocol Security(IPSec) protocol is used and to encrypt the link of network layer Secure Sockets Layer(SSL) and Transport Layer Security(TLS). They ensure confidentiality, authenticity and integrity in the layer [48]. For each sensor devices connected to the network are uniquely defined by using different keys via Private Pre-Shared Key(PPSK) [58] increase the security. The removal of default password, disabling guest login, following strong password policies, periodic changing of password [1] etc. makes the wireless network layer even more secure. Similarly, the IoT devices that used the wired channel can be secured using a firewall and Intrusion Prevention System(IPS). But designing of low research hungry firewall for IoT device is still an ongoing research topic [48].

- ***Security for Application Layer:*** The safety of application layer is crucial in IoT system because different kinds of application services are delivered to the intended users. Therefore, the use of encryption techniques, authorization, authentication, access control list, intrusion detection system, firewall, antivirus makes the system more secure. Data security is another crucial issue in this layer. Therefore, the following precautions help to improve data security [24]:
  - Session inspection to stop the attack of hijacking,
  - Using only a temporary cache to avoid malicious code injection attack,
  - Verification of data,
  - Testing antivirus software against service flaws and malicious code injection,
  - To prevent the leakage of privacy use boundary inspection, data encryption and resource access control.

Since IoT battery enabled, limited processing, storage capacity system, balancing between openness and security is challenging for both developers and security researchers. The smarter security system which includes managed threat detection, anomaly detection and predictive analysis need to evolved [57]. All the above-discussed issue of security is a research opportunity in IoT Security.

2.3 Energy Efficiency

The ubiquitous feature of IoT has changed the lifestyle of people. The booming growth of the IoT market and the increasing amount of investment by reputed companies show a positive sign for IoT technologies. While the use of these applications is enormously scaling, the device's capabilities such as processing, storage, bandwidth, battery life and its energy efficiency, are limited. Although battery cell is the primary source of energy in the IoT sensor network, they can also use scavenging devices or both as energy sources. When the energy level of the battery falls below a threshold value, the performance of sensors degrades along with decreasing network's operational lifetime. In most of the case, it is also difficult to replace the drained battery or even not possible to recharge them after their expiry in sensor nodes. It is because they are placed or spread in a remote location where human access is almost not possible. In the IoT network, sensor nodes consume energy during transmission and receiving of data packets [30]. Due to the limitation of network coverage of sensor nodes or devices in the IoT network, data packets are also forwarding via reliable multi-hop communication [51]. The process of selecting the path to send data packets from the source node to destination nodes is known as routing, which is operating under standard communication rules known as the protocol. Therefore, the routing protocol plays an essential role in the successful transmission of data packets from the source to the destination. The efficient utilization of the energy of sensor nodes by routing protocols increases the lifetime of the IoT network. It means less power consumption by IoT sensor nodes [51].

Moreover, the authors of [8] also highlight additional variables that affect the power consumption such as distance between the nodes, length of the data packet, cost for power amplification before transmission of the message, etc. The research on sleep scheduling technique for energy-efficient routing protocol in wireless IoT sensor networks. Similarly, in the [25], the researchers implemented clustering of sensor nodes methods using improved Low-energy Adaptive Clustering Hierarchy(LEACH) protocol to minimize the energy used by sensor nodes in wireless IoT Network. They claim the improved LEACH protocol increase the network lifetime by 127% because the consumption of energy is less during data transmission. We can say, network lifetime is inversely proportional to the energy consumption during data transmission.

Similarly, there are many journals, articles of researchers on efficient energy routing protocol in IoT paradigm; it is because energy is the powerhouse of IoT network and inefficient depletion of energy in sensor nodes hinders popularity of IoT. Thus, energy-efficient routing has been studied vigorously. Singh, Woo and Raghavendra in 1998 [52] highlights optimization methods for energy-efficient routing, which can improve the lifetime of the network. They are as follows:

- ***Minimizing energy consumption over a route:*** The primary purpose of such routing protocol is to find the path between source and destination nodes for data packets transmission with minimum route cost energy. The necessary distance vector routing protocols are designed for this purpose.

- ***Minimizing the routing overhead:*** The operations which are essential for routing purpose are a period message to check the status, route maintenance packets, packets for exploring topology, route request packets etc. But sometimes they become an overhead for routing purpose if they are excessive in the network, which should be minimized.

- ***Maximizing lifetime of the network:*** The routing protocol balances the battery resource of all the nodes to maximize the lifetime of the network. For this purpose, they use many advanced algorithms to deal the balancing metrics such as the location of nodes, amount of traffic handled by specific nodes etc.

Therefore, improving the efficiency of sensor nodes, reducing node energy consumption and extending network time is still the hot topic in wireless IoT network system.

2.4 Summary

This chapter has described the historical development of the IoT network and current activities that help to outgrown the IoT. It has highlighted the features of the IoT system, along with its merits and demerits. It has also included the layer concept as IoT architecture. This chapter has described security issues and its potential measures based on layer concept of IoT architecture. Finally, the chapter has been concluded by raising energy efficiency and its importance to increase the network lifetime.

3 IoT Network

The sensor nodes which is also known as a digital sensory organ in the IoT system. They use various combinations of connections between nodes such as line, ring mesh, fully connected, tree, bus etc. Out of them, the mesh network is most beneficial in wireless connectivity of nodes as it does not have any hierarchy; individual nodes can connect to any number of nodes within the transmission zone area. But according to the [44], wireless IoT networking system needs to fulfill following basic standards:

- *IoT network should have the capacity to connect a large number of different elements*
- *IoT network should be high reliable*
- *IoT network should real-time packets transmission*
- *IoT network should minimise delay*
- *IoT network should be able to protect data flows*
- *IoT network should support monitoring and traffic management at the device level*
- *IoT network should be cost-effective for a large number of connected sensor nodes*

3.1 IoT Communication Model

The communication model describes the operational perspective of IoT devices. The architectural documents published by Internal Architecture Board(IAB) in 2015 [42], defines four communication models of smart devices as described by figure 3.1, which are as follows:

- ***Device-to-Device Communication model:*** In this type of communication model, as expressed in figure 3.1(A), two or more smart objects communication directly without intermediaries to share the information in real-time. They use existing standard communication protocol for successful data packets exchange. This type of communication model is using in the small automation application, such as a home automation system. Typically, this communication model has small data packets and a relatively low data rate.

- ***Device-to-Cloud Communication model:*** In this type of communication model, IoT smart objects established a direct connection to the Cloud applications, as shown in figure 3.1(B). After a successful linkage between IoT devices and the data storage system(cloud), they exchange data and control message traffics. They use either traditional wired Ethernet or WiFi connection to establish a link between device and Internet Protocol(IP) network, which ultimately connects with a central data storage system.

- ***Device-to-Gateway Communication model:*** This communication model is also known as device-to-application-layer gateway(ALG)model, where ALG services on the local gateway device act as an intermediary between smart devices and central data storage system(cloud). Here gateway is more potent than sensors and provides security, protocol translation task. Gateway has two significant functions, i.e. collect data from sensors and route to the central data storage system(cloud) via the internet. This communication model is expressed in figure 3.1(C).

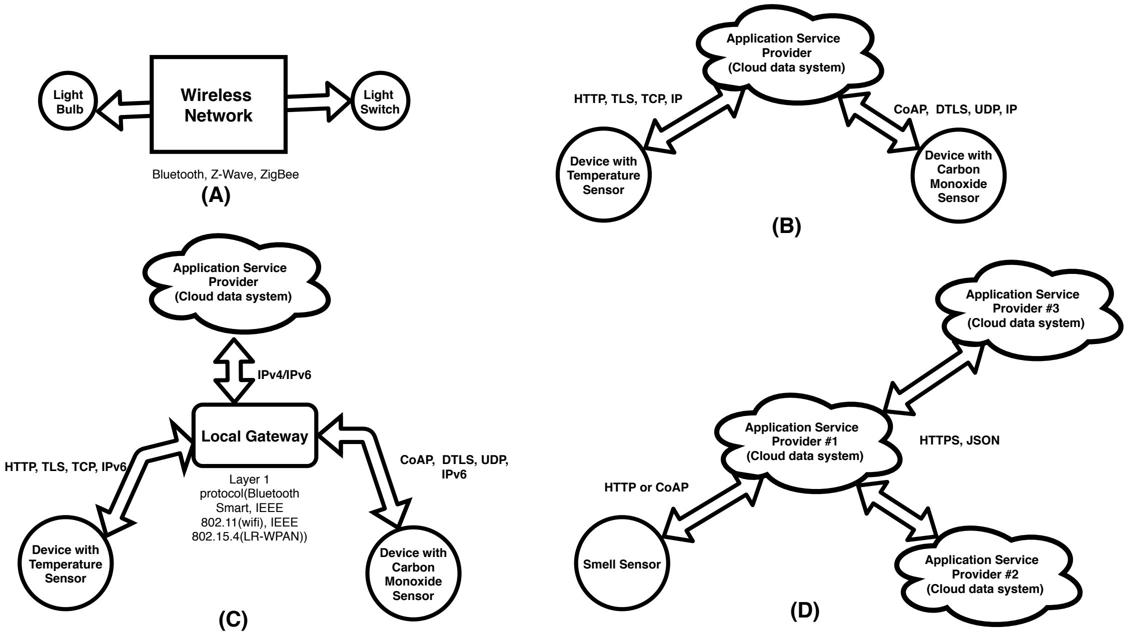
Light Bulb
Wireless Network
Light Switch
Bluetooth, Z-Wave, ZigBee
(A)
Application Service Provider (Cloud data system)
HTTP, TLS, TCP, IP
CoAP, DTLS, UDP, IP
Device with Temperature Sensor
Device with Carbon Monoxide Sensor
(B)
Application Service Provider (Cloud data system)
IPv4/IPv6
Local Gateway
HTTP, TLS, TCP, IPv6
CoAP, DTLS, UDP, IPv6
Layer 1 protocol(Bluetooth Smart, IEEE 802.11(wifi), IEEE 802.15.4(LR-WPAN))
Device with Temperature Sensor
Device with Carbon Monoxide Sensor
(C)
Application Service Provider #3 (Cloud data system)
Application Service Provider #1 (Cloud data system)
HTTPS, JSON
HTTP or CoAP
Smell Sensor
Application Service Provider #2 (Cloud data system)
(D)

Figure 3.1: Communication Models (A)=Device-to-Device, (B)=Device-to-Cloud, (C)= Device-to-Gateway and (D)=Back-End Data-Sharing, figure redrawn from [42]

- ***Back-End Data-Sharing Communication model:*** In this type of communication model, information is shared between the central data storage system or application service providers. This model facilitates users to merge data from different sources and analyse them. Here users may include individual or business enterprises. This model also helps in high availability, capacity and reliable disaster recovery [44]. This model is diagrammatically shown by figure 3.1(D).

3.2 Types of IoT Network

Figure 3.2 defines different types of IoT network. The diagrammatic representation of IoT networks is based on distance range coverage. Figure 3.2 below shows its increasing order from the centre.

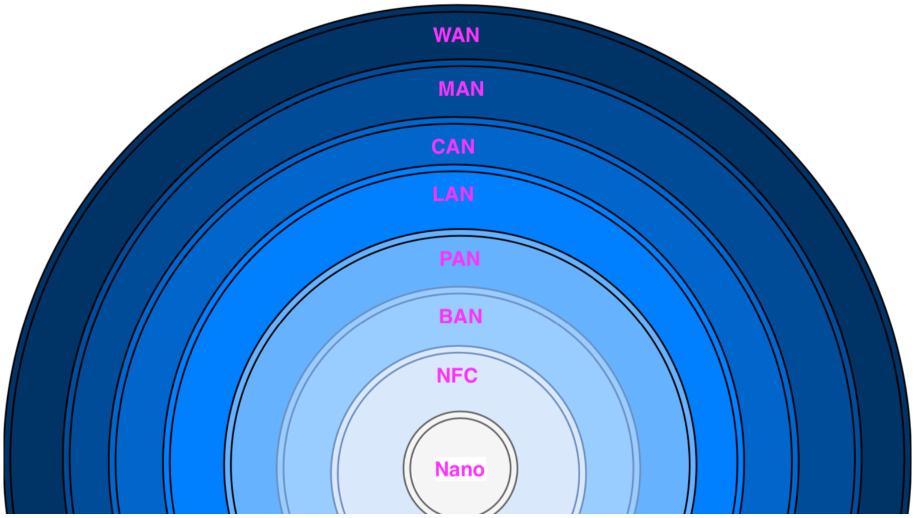

Figure 3.2: Types of IoT Network

- ***A Nano Network:*** The nanotechnology is the engineering of functional units or systems at the molecular scale [35]. Similarly, a nano network is a set of small devices of nanometers that are used to operate simple tasks such as sensing, processing, storing and actuation. This network is used for military application, biotechnology, biomedical industry, agriculture etc.

- ***A Near-Field Communication(NFC):*** NFC is a low-speed network which connects nano-devices at the distance of 4 centimetres [44]. It is typically employed in keycards, contactless payment etc.

- ***Body Area Network(BAN):*** It is the network that establishes a connection with wearable computing devices that can be worn in the body or near the body or implanted inside the human body.

- ***Personal Area Network(PAN):*** It is used to link devices usually span in one or two rooms covering approximately 10-20 feet radius [44].

- ***Local Area Network(LAN):*** It is also used to link IoT devices or sensors that are span over a single building [44].
- ***Campus/Corporate Area Network(CAN):*** This network is the collection of multiple LANs within a limited geographical area, i.e. enterprise or university.
- ***Metropolitan Area Network(MAN):*** It is a big network that uses microwave transmission technology covering particular metropolitan area [44].
- ***Wide Area Network(WAN):*** The IoT network that covers a large geographical area, which includes many small uses LAN and MAN is Wide Area Network [44].

3.3 Wireless Ad-hoc Network(WANet)

A Wireless Ad-hoc Network(WANet) is based on mesh network topology. In this network, nodes are organised to provide a pathway to propagate data from the source node to the destination node. The nodes or wireless devices are connected through a necessary point-to-point wireless connection. It means they do not require any central controlling unit and nodes itself are responsible for network operations such as routing, security, address and key management [43].

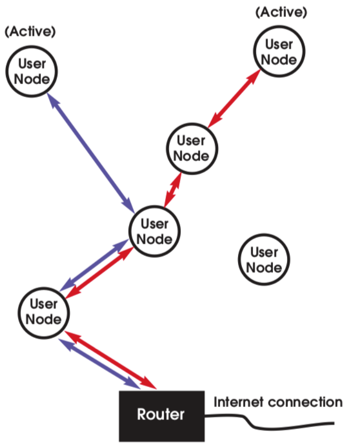

Figure 3.3: Basic structure of wireless Ad-hoc network, figure from [5]

They formed a network according to the need of using the resources on hand and configured accordingly to meet each user's demand. In this network, the entire collection of nodes form a giant connect in different ways, and each of them is aware of all the nodes within the range [5]. There are two forms of WANet; one is Static Ad-hoc Network(SANet), and other is called mobile ad-hoc Network(MANet). In SANet, the sensor nodes are fixed, whereas the sensor nodes keep on moving within the sensor field in MANet. Figure 3.3 provides a simple diagram defining the concept of Ad-hoc network. The number represents five nodes where four nodes are active, within the range and form a pathway towards the router. But one of them is not within the scope or not functioning, thus does not participate in building the path for packets communication. In the same figure, two nodes represent two paths highlighting multiple ways through several nodes to the router. If any intermediate active nodes become inactive or leave the network, the network automatically reconfigures and establishes new route itself.

According to Gary Breed [5], WANet has some advantages and some limitations too. The following are advantages and limitations of WANet:

Advantages of WANet

- *Nodes operate independently*
- *Nodes in WANet have self-configuring capabilities and act as routers*
- *Nodes in WANet have self-healing properties via continuous reconfiguration*
- *WANet is scalable as the addition of new nodes are easily accommodated*

Limitation of WANet

- *Every node should have the full performance capability*
- *System loading is affecting the throughput*
- *It needs sufficient number of nodes for reliability*
- *The large size of network may have excessive latency which affects some applications*

3.4 Wireless Sensor Network(WSN)

The enormous advancement in wireless communications and electronics have made it possible to develops nano size, low-cost, multi-functional sensor nodes to cover short distance communication. The sensor nodes consist of a sensing unit, data processing unit and transmission components. But all these units have limited capabilities.

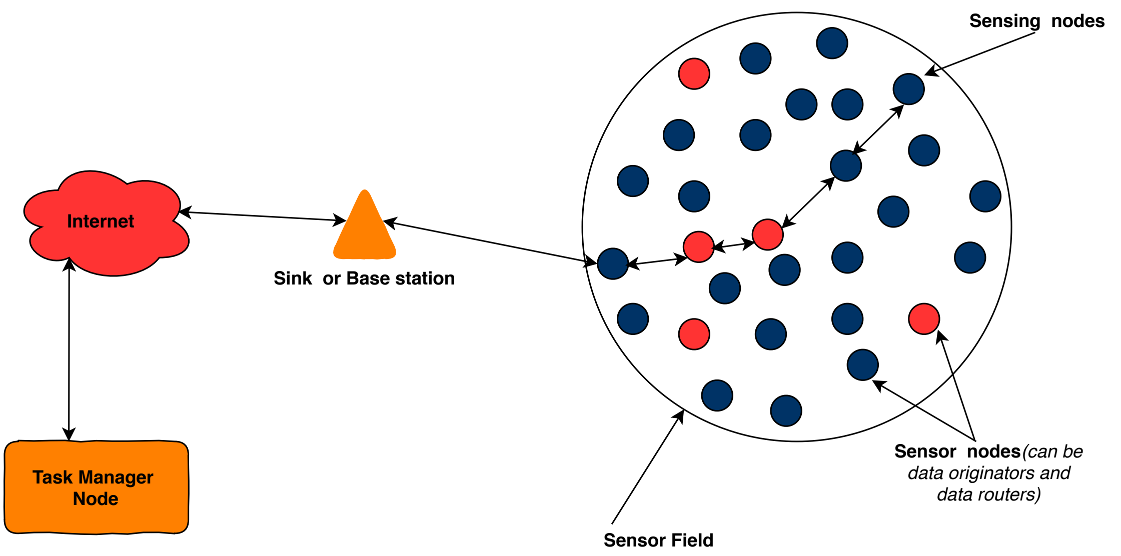

Figure 3.4: WSN Communication Architecture, figure redrawn from [50]

Wireless Sensor Network(WSN) is a collection of hundreds or thousands of sensor nodes which are capable of direct communication among themselves or directly to the base station or sink nodes, as shown in figure 3.4. Each sensor nodes scattered in the sensor field is capable of sensing data from the environment, i.e. data originators and routing data packets towards base station or sink node. Data are routed towards base station or sink node using multi-hop infrastructure-less architecture. Sink communicates with task manager node using the internet [50].

3.5 Difference Between WANet and WSN

A Wireless Sensor Network(WSN) is a Wireless Ad-hoc Network(WANet) consisting of distributed autonomous devices using sensors, but they are non-identical. There are many protocols and algorithm for WANet, but these techniques are suited for the application supported by WSN. Therefore, key differences between WANet and WSN [66] are tabulated below in table 3.1:

Features	Wireless Ad-hoc Network(WANet)	Wireless Sensor Network(WSN)
Medium Used	Radio waves is used as medium.	Infrared, Optical, Radio waves are used as medium.
Type	It is heterogeneous.	It is homogeneous.
Traffic triggering	It depends upon the application's need.	It is triggered by sensing events.
Traffic pattern	It uses point-to-point.	It uses any-to-any,one-to-many, many-to-one traffic patterns.
Network Support	It supports common services.	It supports specific application.
Interconnecting Device	It is wireless routers.	It uses application level gateway.
Number of nodes	It has limitation.	It has no limitation.
Factors Affecting Quality of Service(QoS)	Its QoS is affected by Latency and bandwidth.	Wake-up time and bandwidth affects its QoS.

Table 3.1: Comparison Between WANet and WSN, source from [66]

3.6 Internet of Things and Wireless Sensor Networks

Although there are apparent differences between IoT and Wireless Sensor Networks(WSN), there is still some confusion. A WSN is a spatially distributed network of autonomous sensors that behave as a digital skin, providing a virtual layer where information about the physical world is passed to the central computational system [33]. The WSN is developed using multiple sensor nodes which are coordinated to collect the data.

The scope of the IoT system is more substantial than WSN. When the WSN paradigm is connected to the internet, it becomes part of IoT. Therefore, WSN is one part of the IoT in which sensors used in the IoT system is networked to achieve the coordinated results. On the other hand, there is some application such as SCADA(Supervisory Control and Data Acquisition) System [2] that does not need the internet to monitor the status of the system in real-time. According to [2], the SCADA system needs four significant elements for its operation. They are wireless sensors(collecting data), conversion unit(receiving and interpreting data), master unit(managing different parts, organise data) and communication network(using specific industrial protocol).

Thus, Wireless Sensor Networks(WSN) may or may not integrate into the internet. But, the scope of this thesis is IoT, we will be dealing with the wireless sensor network connected with internet. Therefore, throughout the thesis, the term **Wireless IoT Sensor Network** is used, which is shorten as ***WIoTSN***.

3.7 Routing Protocol

According to the [62], a routing protocol is a process of selecting a reliable and energy-efficient path for the data packets to travel from source node to the destination node. But while choosing the route for data packets, it encounters several difficulties such as type of network, characteristics of the channel, performance metrics, energy level etc. The raw data sensed by the sensor from the existing environment in WIoTSN is typically forwarded to the base station or application gateway, which connects to the other network, i.e. the internet. Further, those collected data are analysed, and appropriate action is taken accordingly.

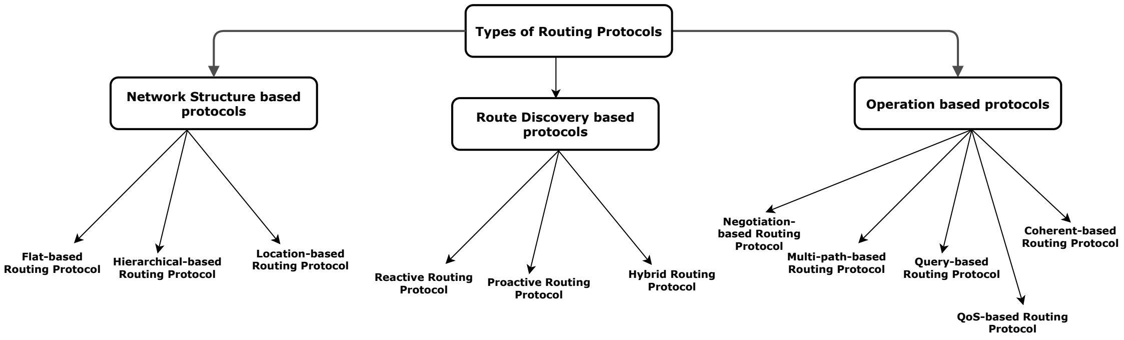
Types of Routing Protocols
Network Structure based protocols
Route Discovery based protocols
Operation based protocols
Flat-based Routing Protocol
Hierarchical-based Routing Protocol
Location-based Routing Protocol
Reactive Routing Protocol
Proactive Routing Protocol
Hybrid Routing Protocol
Negotiation-based Routing Protocol
Multi-path-based Routing Protocol
Query-based Routing Protocol
Coherent-based Routing Protocol
QoS-based Routing Protocol

Figure 3.5: Types of WIoTSN Routing protocols

When the network system is minimal, base station and sensor nodes can communicate directly known as single-hop communication. But single-hop communication is not possible when the network becomes large. In such a network, the multi-hop connection is required when the role of routing protocol is considered to be more significant. Several factors affect the performance of WIoTSN; among them, energy is considered to be the most important factor [8]. Energy-efficient routing protocol keeps the WIoTSN alive for a more extended period which is very crucial for constrained IoT sensor nodes. According to the [47], the routing protocol of WIoTSN has been classified based on network structure, route discovery and operation used by them. Their classification has been depicted in figure 3.5. The classification of routing protocol under network structure and operation are not under the scope of this thesis. Therefore, the below sections only address routing protocol of WIoTSN under route discovery.

3.8 Proactive routing Protocol

The Proactive routing protocol is also known as a table-driven routing protocol [47]. It is because proactive protocol maintains a routing table which keeps track of route or path nodes in a specific format from current sensor nodes to the destination nodes. This protocol transmits a control message periodically to update route information even if there is no data flow. Thus, the proactive protocol is not considered bandwidth-efficient [19]. One significant advantage of this protocol is, sensor nodes can quickly start the session as it has ready-made routing information. It also has a disadvantage since its sensor node holds too much information, particular failure of the link becomes an additional burden to reform the link, and it is slow too [47].

3.8.1 Optimized Link State Routing(OLSR)

Optimised Link State Routing(OLSR) stores and updates its routing table permanently. It is an optimisation version of pure link-state protocols which successfully reduces the size of controls packets along with the number of control packets transmission needed. To achieve this, OLSR has used Multi-Point Relay(MPR) selection algorithm, as mentioned in the RFC documents 3626 of OLSR [9]. According to the paper, MPR is a one-hop neighbour node from source node which has been choosing to broadcast the data packets. It does not mean all one-hop neighbour node is selected as MPR instead of those MPR nodes that have the maximum number of isolated nodes is selected as MPR, and its routing process is expressed in figure 3.6. Instead of pure flooding in pure link-state routing, OLSR uses source node MPR to forward the packet reducing the size of traffic control packets. MPRs helps to figure out the shortest path between source and destination. The network topology information is maintained periodically exchange link-state information.

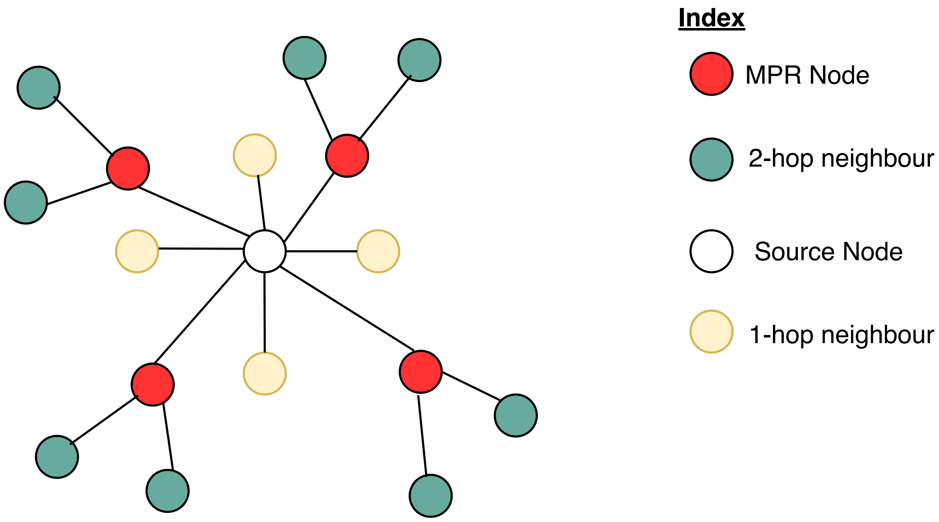

Figure 3.6: The mechanism of OLSR routing process , figure redrawn from [20]

3.9 Reactive Routing Protocol

The reactive routing protocol is table-less or on-demand routing protocol. They do not maintain a routing table of the whole topology; instead, the routes are built whenever it is needed. The advantages of this protocol are lower bandwidth for holding routing tables, more and productive energy efficiency and route maintenance [19]. It also has a disadvantage, it offers high latency in search of the network, and excessive flooding may lead to network clogging [55]. Dynamic Source Routing(DSR) and Ad-hoc On-demand Distance Vector(AODV) are examples of reactive routing protocols.

3.9.1 Dynamic Source Routing(DSR)

The use of source routing is a crucial distinguishing feature of DSR. It means the sender knows the complete hop-by-hop route towards the destination. The route information is stored in the route cache. In this routing protocol [49], every data packets that are required to transmit the source route in the packet header. DSR is beacon-less, and the node does not need to send a periodic message to inform about its presence. DSR performs two primary operations, i.e. route discovery and route maintenance. DSR uses three signals, namely Route Request(RREQs), Route Replies(RREPs) and Route Errors(RERRs). RREQs and RREPs are used to discover the route whereas RERRs are used for maintenance of the route.

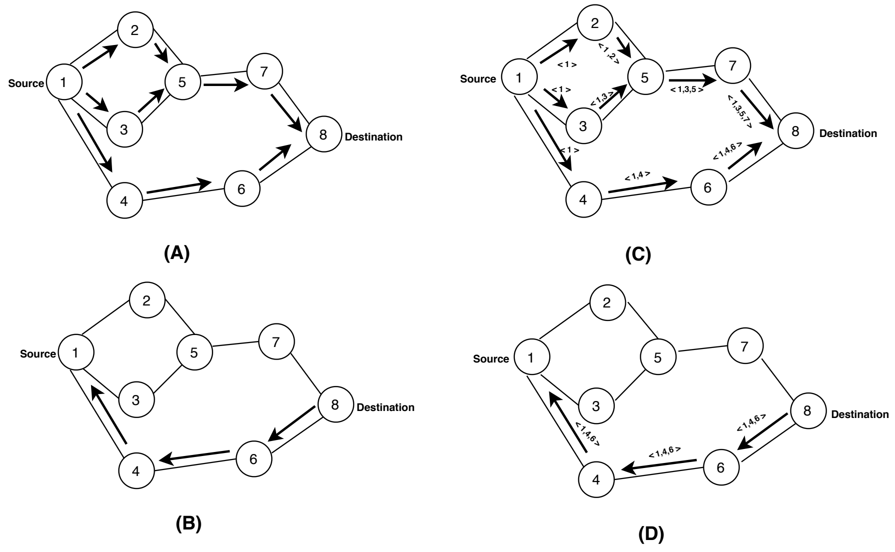

Figure 3.7: Route Discovery Mechanisms (A)= Propagation of Route Request(RREQ) packet of AODV (B)=Path Taken by Route Reply(RREP) packet of AODV (C)=Building Record Route during Route Discovery of DSR (D)= Propagation of Route Reply with Route Record of DSR, figures redrawn from [39][49]

The route discovery operation of DSR is expressed diagrammatically in figure 3.7(C) and 3.7(D). In DSR, the route discovery operation starts by flooding the data packets in the network with RREQ packets. The flooding process continues until data packets reach to the destination node and maintain route list which is caches in a route cache. After finding the destination node, RREps packets are routed back to the source with an optimal path. If the link is broken, then RERRs packet is sent to the source. In DSR, the route is maintained between those nodes only who need to communicate, which is reducing the overhead of route maintenance. Route caching can further reduce route discovery overhead. Whereas, the size of the packet header grows with the length of the route due to source routing [55].

3.9.2 Ad-hoc On-demand Distance Vector(AODV)

AODV routing protocol is reactive on request protocol which is engineered for the infrastructure-less network. AODV is a loop-free routing protocol. It uses Destination Sequence Numbers(DSN) to avoid the Bellman-Ford problem or counting to infinity problem. This routing protocol uses a sequence number to find the most favourable route [55]. AODV uses three messages, namely Route Request(RREQs), Route Replies(RREPs) and Route Errors(RERRs) as DSR does. RREQs and RREPs are used to discover the route whereas

RERRs are used for maintenance of the route. AODV selects the shortest path and loop-free path utilising a routing table to transmit data packets. If any problems come into the nominated path, then AODV establishes a new path for the rest of the communication [39]. AODV keeps on forwarding the periodic message to detect the link. The route discovery method is represented in figure 3.7(A) and 3.7(B). One primary advantage of AODV is, it uses uniform data packets though the length of route increases. It seems DSR and AODV are similar, but they are different in several aspects, which is defined in the following table 3.2:

Protocol Features	**DSR**	**AODV**
Table driven/Source Routing	Source Routing	Both Table-driven and Source Routing
Need of periodic message	Not needed	Yes needed
Route Discovery	It is on-demand.	It is also on-demand.
Route mechanism/maintenance	Complete route cached.	Route table with next hop
Network and Routing Overhead	it is low.	It is high.
Packet Size	It is non-uniform.	It is uniform.
Loop free	It is loop free protocol.	It is also loop free protocol.

Table 3.2: Comparison Between DSR and AODV, source from [49]

3.10 Summary

This chapter has illustrated the IoT network and its type with the communication model. A reader can easily differentiate between WANet, WSN and IoT after reading this chapter. It has described the data route discovery process of the proactive protocol(OLSR) and reactive protocol(AODV and DSR) with meaningful diagram.

4 Practical Implementation

This chapter addresses the methodology, scenario and different steps performed to highlight the central idea of the thesis, i.e. problem statements, which is in section 1.1. It defines how the rest of the work is conducted and gives clear explanation step-by-step of each section. The illustration detail of task performed of the thesis acts as guidelines for those people who want to pursue knowledge as well as explore more dimension of thesis work.

In the process of thesis work addressing the problem statement, the open-source Network Simulation tools for experimental purpose is chosen. The energy efficiency of reactive and proactive protocols have been analysed by changes parameters such as sensor nodes, sink speed, data rate and packet size. Its practical implementation is prime and core activities of the thesis to achieve this goal.

4.1 Network Simulation Tools

The process of designing, developing and evaluating new IoT products and protocols need appropriate testing and evaluation using a wide variety of research tool before it is deployed physically in the real environment. IoT simulator needs to offer some essential features such as high fidelity, support scalability, provide energy or computation energy and extensible to support custom requirements [7]. IoT simulators are categorised into three different types, i.e. full stack simulators, big data processing simulators and network simulators. Out of them, network simulators is the scope of this thesis. There are many popular network simulation tools; few of them are listed below:

- ***Cooja:*** Cooja is an associate simulator which is available with Contiki Operating system. Contiki operating system is used to program IoT sensor nodes. It supports popular application layer protocols such as Message Queue Telemetry Transport(MQTT) and Constrained Application Protocol(CoAP). It is not the only simulator, and rather it is the emulator which is capable of developing firmware level instructions in the wireless environment [37]. It uses the C programming language.
- ***Objective Modular Network Testbed in C++ (OMNeT++):*** It is one of

the most popular network simulators. It has been used in wireless sensor network extensively. Its framework is well established and supports external elements and thus used to create vehicular network simulator known as Veins and utilised to evaluate smart transportation system [7]. This simulator does not have built-in support of radio models and application-level protocols of IoT, thus needs to implement manually [56].

- ***Network Simulator-3(NS-3):*** It is the successor of NS-2. It is replicating perception layer of IoT in simulation, and this layer is described in layer architecture in figure 2.4. It supports C++ as OMNeT++ does, but it also supports radio models for IoT specific but does not support application-level protocols [14].
- ***QualNet:*** Along with some open-source simulator, there are some commercial tools, QualNet is one of them. Being a proprietory tool, it supports high fidelity for IoT-specific simulations. It has been extended to simulate various forms of cyber-attacks such as eavesdropping, radio jamming, virus attacks, DDoS, signal intelligence attack etc. [68].

Table 4.1 summarises the critical features of the above-listed network simulators.

Features	**Cooja**	**OMNeT++**	**NS-3**	**QualNet**
Scope	Network	Network	Network	Network
Type	Discrete-Event	Discrete-Event	Discrete-Event	Discrete-Event
Language	C/Java	C++	C++	C/C++
Mobility	Supported	Supported	Supported	Supported
Cyber Attack Simulation	Using Custom extensions	Using Custom extensions	Not Supported	Supported

Table 4.1: Comparison Between Network Simulators, source from [7]

4.2 Experimental Setup

Practical implementation is the core part of this thesis for testing purpose. A lot of information about reactive and proactive routing protocols, energy efficiency features of those protocols, their mechanism of finding the routes and available network simulators such as commercial or open-source have been collected using Google Scholar and IEEE websites. Thus, experimental testing is conducted in the following systematic ways:

- ***Choose one category of routing protocols, Network simulator tool:*** There are different types of routing protocol categorised based on network structure, operation and route discovery-based, as shown in figure 3.5. From the collected conference papers, journals for the guidance of thesis work, I have read many documents on energy efficiency based on above-listed categories of protocols for IoT network, wireless sensor network, Ad-Hoc network, MANet etc. I have selected for testing energy-efficient of routing protocol, i.e. proactive and reactive protocols based on route discovery. In the proactive protocol, I have chosen OLSR, and in the reactive protocol, DSR and AODV are selected for practical implementation. In the context of Network simulator, most researchers have used open-source network simulator rather than proprietary simulators. I have options of using Cooja, OMNeT++ and NS-3. At the beginning of the experimental setup, I tried to use Contiki Operating System for IoT network, which has Cooja simulator within it. But I realised the community of Cooja is not so active. I felt it is hard to implement further without update features and active community support and switched to NS-3. I found the community of NS-3 network simulator is very active and supports the latest features. They release new models and extension and bug fixes to previously released model about two or three times per year [64] that are crucial for the overall networking community and especially for IoT network, i.e. WIoTSN.

- ***Practical Implementation:*** For practical implementation, the hypervisor VirtualBox is used to install Ubuntu-18.04 where NS-3.30 network simulator is installed. This simulator supports C++ and also allow python bindings. But most of the resources are available in C++ programming language. Therefore, I have used C++ to code program for simulation. To resolve the coding issues and some implementation issues of energy efficiency of sensor nodes, I have used the resources and guidelines from the ns-3 user group in Google [16]. It is a community group where we can raise the issues faced during implementation and seek for help. The active member of the ns-3 user group in Google, Jack Higgins [15] and his research work is beneficial for my thesis implementation.

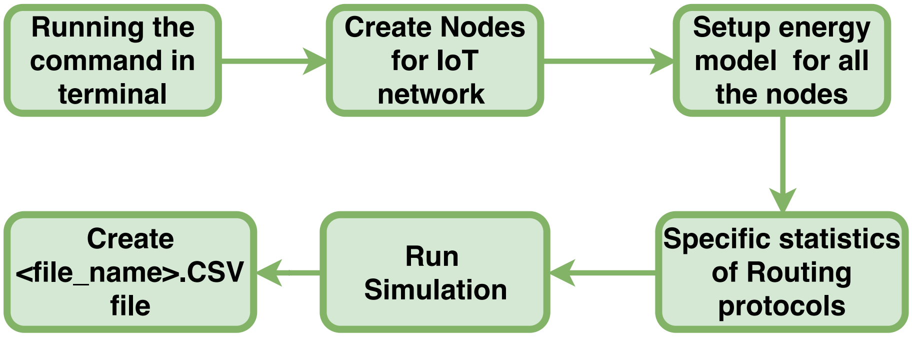
Running the command in terminal
Create Nodes for IoT network
Setup energy model for all the nodes
Specific statistics of Routing protocols
Run Simulation
Create <file_name>.CSV file

Figure 4.1: Simulation model

Figure 4.1 represents the simulation model of the thesis. When the command is executed to run the simulation program via Ubuntu terminal, sensor nodes are created along with the installation of the energy model and statistics of routing protocols which are according to the protocol selected. After completion of the simulation, results are saved into the file with extension comma-separated values(CSV).

In this thesis, I have used static sensor nodes. The mobility model used by NS-3 to make nodes static is known as ***Constant Position Mobility Model***. Similarly, an additional mobile sensor node is used, called base station node or sink node. The mobility model used for such nodes by NS-3 is ***Random Waypoint Mobility Model***. This sink node gets data packets from all static sensor nodes. During this operation, energy is consumed, and its efficiency analysis is the central task of thesis work. Therefore, there are two parts of the energy consumption model, which is supported by the NS-3 energy framework [64], namely energy source and device energy model. The energy source is the power supply for each node in the topology. A node can have single or multiple energy sources. Similarly, device energy model defines the energy consumption by a device on the nodes. Here each device can have various states such as transmit, receive, idle and sleep [45]. Each state consumes a certain amount of energy. The route discovery operation passes through above-listed states and thus consumes power. But the amount of energy consumed depends on the route discovery process followed by proactive and reactive protocols. The average energy consumption of static sensor nodes using selected proactive and reactive protocols are calculated under consideration of following parameters of simulation:

- **Changing number of nodes in a fixed sensor field**
- **Changing the speed of sink node in a fixed sensor field**
- **Changing the data rate of sensor nodes in a fixed sensor field**

- **Changing the size of data packets propagated by sensor nodes in a fixed sensor field**

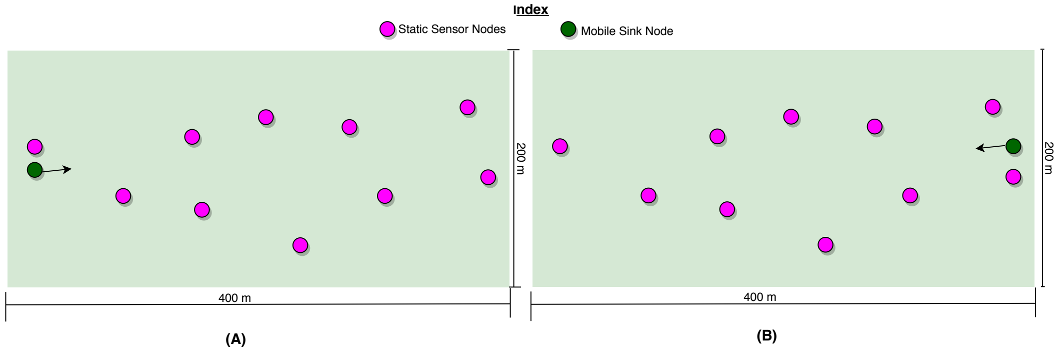

Figure 4.2: Topology of 1 Sink node & 10 Static sensor nodes, (A)=Sink node moving from Left to right direction, (B)=Sink node moving from right to left direction

Figure 4.2 shows a pictorial representation of the simulation topology setup. Here the sink node moves within the sensor field of area 200x400 square meter horizontally from the middle, as shown in figures 4.2(A) and 4.2(B). Sink node makes six complete rounds and simulation stops. Therefore, the sink node with speed 2 meters/second takes longer simulation time whereas 8 meters/second takes shorter simulation time. Thus, the simulation time for 2 meters/second needs 1200 seconds to cover six complete rounds, whereas 5 meters/second needs 480 seconds and 8 meters/second needs 300 seconds as listed in table 4.2.

During this movement, static sensor nodes, scattered within the sensor field, get data packets as sensing data from the environment and propagated to the mobile sink node via a route. The protocols OLSR, DSR and AODV, are described in sections 3.8 and 3.9 respectively, following their respective working principle and routes are discovered. As mentioned in section 3.1 in IoT communication model, the communication between static nodes and static nodes to the sink node follow device-to-device and device-to-gateway models, respectively. Table 4.2 contains a summary of the parameters used to carry out the simulations.

Parameters	**Parameter Values**
Simulation Tool	NS-3.30
Simulation Area	200x400 $meter^2$
Number of Nodes	10, 30, 50, 70, 90, 110, 130, 150, 170, 190
Channel	Wireless
Mobility Model	Constant Position Mobility model and Random Waypoint Mobility model
Propagation Loss model	Range Propagation Loss model
Propagation Delay model	Constant Speed Propagation Delay model
Data Packet Size(DPS)	1024 bytes and 2048 bytes
Transmission Rate(TR)	8232 bits per second and 32928 bits per second
Sink Node Speed(SNS)	2 meters per second, 5 meters per second and 8 meters per second
Initial Energy Source	3000 Joules
Simulation Time	1200 Seconds, 480 seconds and 300 seconds
Routing Protocol	OLSR, AODV and DSR

Table 4.2: Summary of Simulation Parameters

- ***Data Analysis:*** The analysis is based on results obtained from simulation. It also includes difficulty to do practical testing; the help received from other researchers, previous work followed etc. There are so many performance metrics to analyse routing protocols such as packet loss, average end-to-end delay, throughput, packet delivery ratio [40]. All of them are interlinked with each other. According to our simulation data, we are comparing the packet delivery ratio of WIoTSN of OLSR, DSR and AODV protocol. Packet Delivery Ratio(PDR) is the proportion of received packets by destination nodes(sink node) and packets transmitted by source nodes(sensor nodes). PDR is directly proportional to the performance of WIoTSN. But the primary evaluation of protocols is on efficient average energy consumption of sensor nodes of above selected proactive and reactive routing protocols under consideration of network size, size of data packets, data transmission rate and speed of sink nodes in WIoTSN. The analysis based on the speed of sink nodes only has multiple simulation time, as listed in table 4.2, since total simulation time is inversely proportional to the mobility speed of sensor nodes. But, the rest testing conditions uses constant simulation time, i.e. 480 seconds.

5 Simulation Results

This chapter includes analysis and discussion of simulation results of proactive and reactive protocols, especially OLSR, DSR and AODV routing protocols. The validation of the problem statements under selected criteria defined in section 1.1, follow network simulation results and inspect energy-efficient routing protocols. As it is mentioned in table 4.2, the simulation was ranging from 10 to 190 sensor nodes. During the simulation process, especially in the case of AODV protocol, it stops either in 110 or 130 nodes. Since its detail investigation might increase the length of the thesis period and does not meet the scope of the thesis, I did not perform any kind of additional testing. Therefore, in the case of AODV protocol, the graph is terminated approximately either in 110 or 130 sensor nodes. Thus, simulation results are available up to 110 or 130 nodes in AODV.

5.1 Routing

The performance of the routing protocol is directly related to the delivery of data packets. The successful delivery of data packets between sensor nodes and the sink node in the WIoTSN is not isolated features. The reasons for the dropping of data packets are expiring of packet Time-To-Live(TTL), route error, interface down, bad checksum, fragment timeout exceeded etc. As the sink node is mobile, which keeps on changing the location. The frequent changing of position suffers from packet loss. It has a high possibility of not getting a route for a new visiting network, causing rejection of all the traffics.

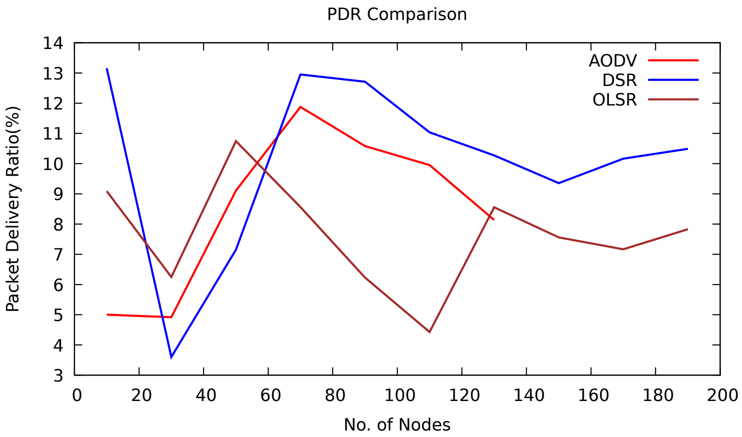

Figure 5.1: Comparison of Packet Delivery ratio of OLSR, DSR and AODV routing protocols

The figures 5.1, 5.2 and 5.3 plot the simulation results where the x-axis represents the size of WIoTSN and y-axis represents packet delivery ratio defined in percentage, with 5 meters per second speed of sink node, supporting maximum 190 static sensor nodes and 480 seconds simulation time. Referring to figure 5.1, the overall data defines poor performance in terms of packet delivery ratio, where out of 100% PDR is successful packets delivery is approximately lying between 3% to 14%.

It is also quite hard to identify the best routing protocol in the context of PDR. It is because of inconsistent performance with the increasing size of WIoTSN network. For the small size of WIoTSN, OLSR protocol is better than AODV and DSR. But when network size grows, the DSR protocol performs better than AODV and OLSR. AODV is a medium performer of both cases. It is not possible to plot the lines after 130 node size of WIoTSN in AODV protocol, and its reason is already explained in the above section.

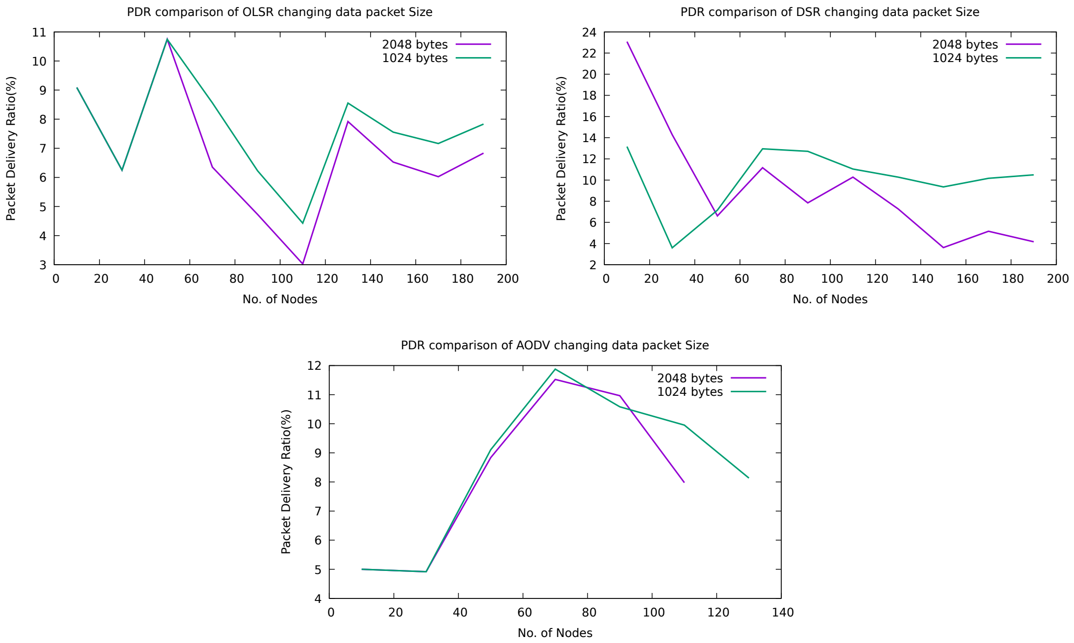

Figure 5.2: PDR Vs. Data Packet Size

The PDR is also affected by the change of data packet size in WIoTSN. According to the graphs of figure 5.2, the smaller size of data packet gives higher PDR, i.e. excellent performance than larger data packet size in most of the time. But the variation of data transfer rate gives mixed output among the tested protocols. According to the graphs of figure 5.3, PDR is higher with significant data transmission rate than lower in case of OLSR. It means excellent performance in packet delivery between sensor nodes and the sink node with a high transmission rate. But there is no significant change in the performance of packet delivery in case of AODV whereas DSR shows mixed performance in the same simulated environment.

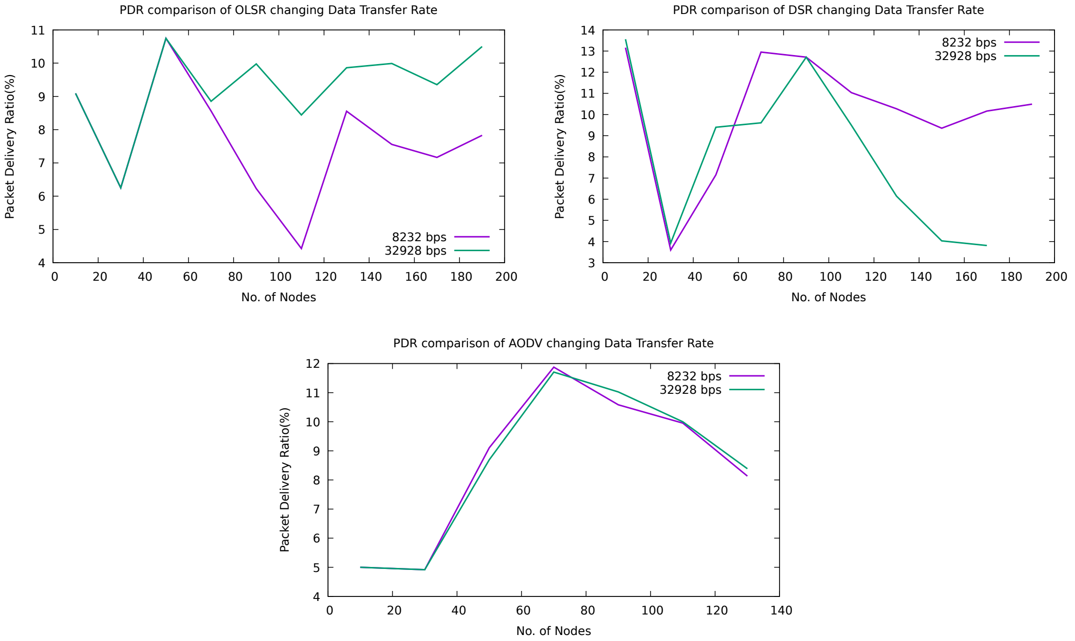

Figure 5.3: PDR Vs. Data Transmission Rate

5.2 Energy Efficiency

The energy-efficient routing protocol is selected based on the simulation results, which are graphically represented in the figures 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.11 and 5.13. The simulation results are analyzed using the following scenario such as scaling network size(no. of nodes), scaling packet size, scaling data transmission rate and scaling speed of mobile sink node for energy efficiency of AODV, OLSR and DSR.

- **Scenario 1: Average Energy Consumption on Scaling the Size of Network**

  In figure 5.4, figure 5.5 and figure 5.6, the x-axis represents the number of nodes, whereas y-axis represents the average amount of energy consumed. The y-axis values are approximately 397-401 joules average energy consumption. It is because they are the result of simulation with the same speed of mobile sink nodes, i.e. 5 meters per second(mps) and takes 480 seconds of simulation time. Whereas in figure 5.7, the average consumption of energy range represented in the y-axis is different. It is because this graph represents simulation result with 2 mps of mobile sink node of WIoTSN, which is resulting in longer simulation time, i.e. 1200 seconds. Similarly, the same logic is valid with the values represented in figure 5.8 in the y-axis. In this graph, mobile sink nodes have a speed of 8 mps resulting in less time to complete the simulation, i.e. 300 seconds.

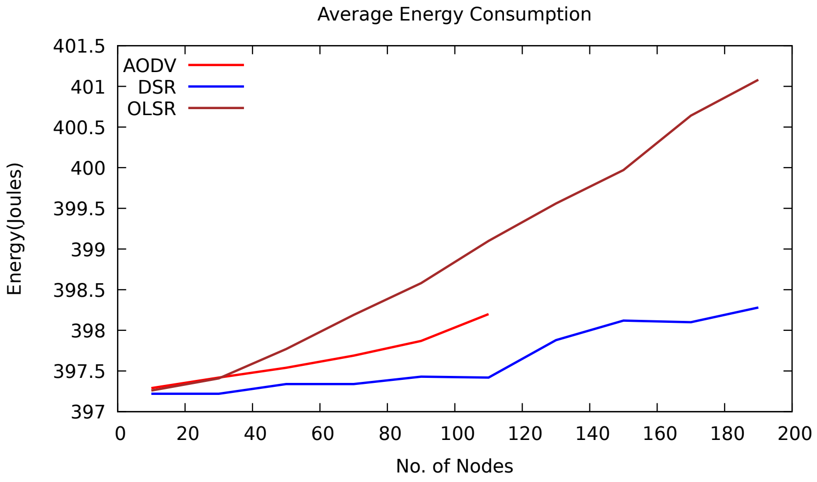

Figure 5.4: Average Energy Consumption of protocols(SNS=5mps, DPS=2048 bytes, TR=8232bps)

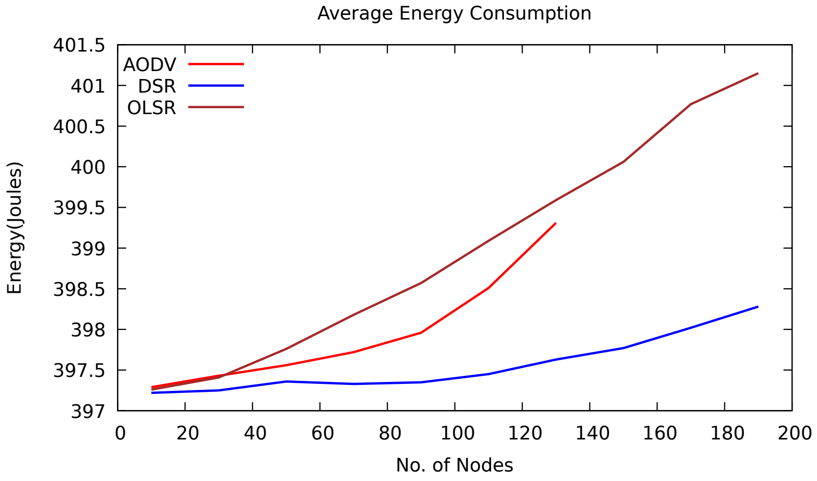

Figure 5.5: Average Energy Consumption of protocols(SNS=5mps, DPS=1024 bytes, TR=8232bps)

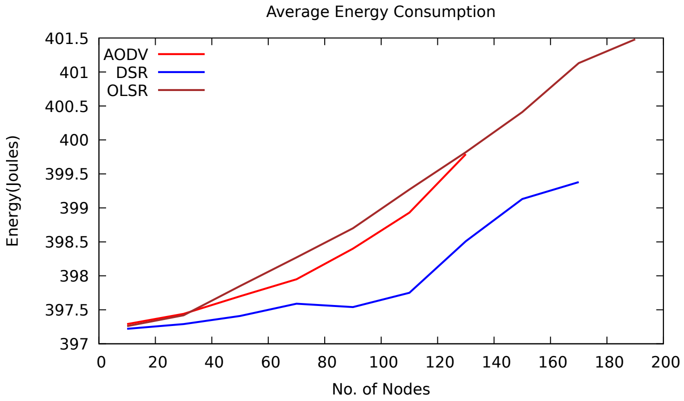

Figure 5.6: Average Energy Consumption of protocols(SNS=5mps, DPS=1024 bytes, TR=32928bps)

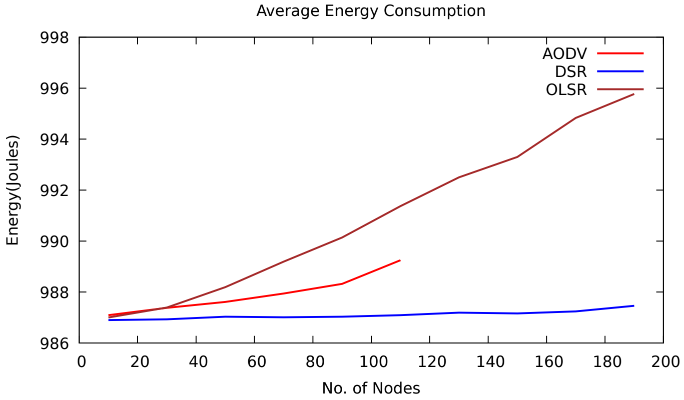

Figure 5.7: Average Energy Consumption of protocols(SNS=2mps, DPS=1024 bytes, TR=8232bps)

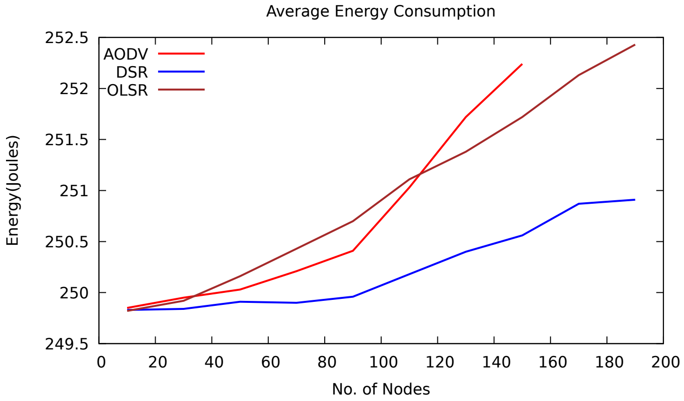

Figure 5.8: Average Energy Consumption of protocols(SNS=8mps, DPS=1024 bytes, TR=8232bps)

Similarly, lines legends for protocols AODV, DSR and OLSR are moving upward with increasing change in network size of WIoTSN and average energy consumption.

But all the lines of graphs do not stop at the same point, especially in case of line legend for AODV protocol. The reason behind this is already explained in chapter 5. Although simulation using network simulator NS3 has different experimental conditions concerning the size of the network, the average energy consumption increases with the increase of the size of nodes in the network, i.e. WIoTSN. The protocol DSR has the lowest level of average energy consumption than AODV and OLSR with an increase in network size in the corresponding simulation. But in the case of AODV and OLSR, the lines are approximately coinciding in the beginning, i.e. smaller network size and OLSR increase higher than AODV. Since successful simulation execution is not possible for AODV protocol, but the way line of legend AODV is moving upward, it is not wrong to predict, at a certain point representing network size, AODV bypasses OLSR and consumes more energy as this can be seen in figure 5.8. But reactive protocol DSR consumes the least power throughout the simulation period than AODV, and OLSR corresponds to the lowest trending lines in the graphs. Thus, DSR is an energy-efficient routing protocol with changing network size, i.e. number of sensor nodes in WIoTSN.

- **Scenario 2: Average Energy Consumption on Scaling the Data packet Size**

  Figure 5.9 shows the average energy consumption of three different routing protocols while changing the size of data packets with different network size keeping transmission rate and speed of mobile sensor nodes constant. In the graph, the lines of reactive protocol OLSR with both data packet size, i.e. 1024 bytes and 2048 bytes are increasing sharply than DSR and AODV. Similarly, in OLSR, lines representing both data packets are moving upward by overlapping each other until approximately 130 nodes of network size. It means there are no significant changes in average energy consumption upon the shift in data packet size. After an approximate point, i.e. 130 sensor nodes, the smaller data packet size is increasing higher than the large data packet size.

  Similarly, the lines of graph for both data packets size is mirroring the features of OLSR, but it is consuming less average energy than OLSR. In the case of DSR protocol, lines for 1024 bytes and 2048 bytes of data packets have been increasing slightly with an increase in the size of nodes of WIoTSN.

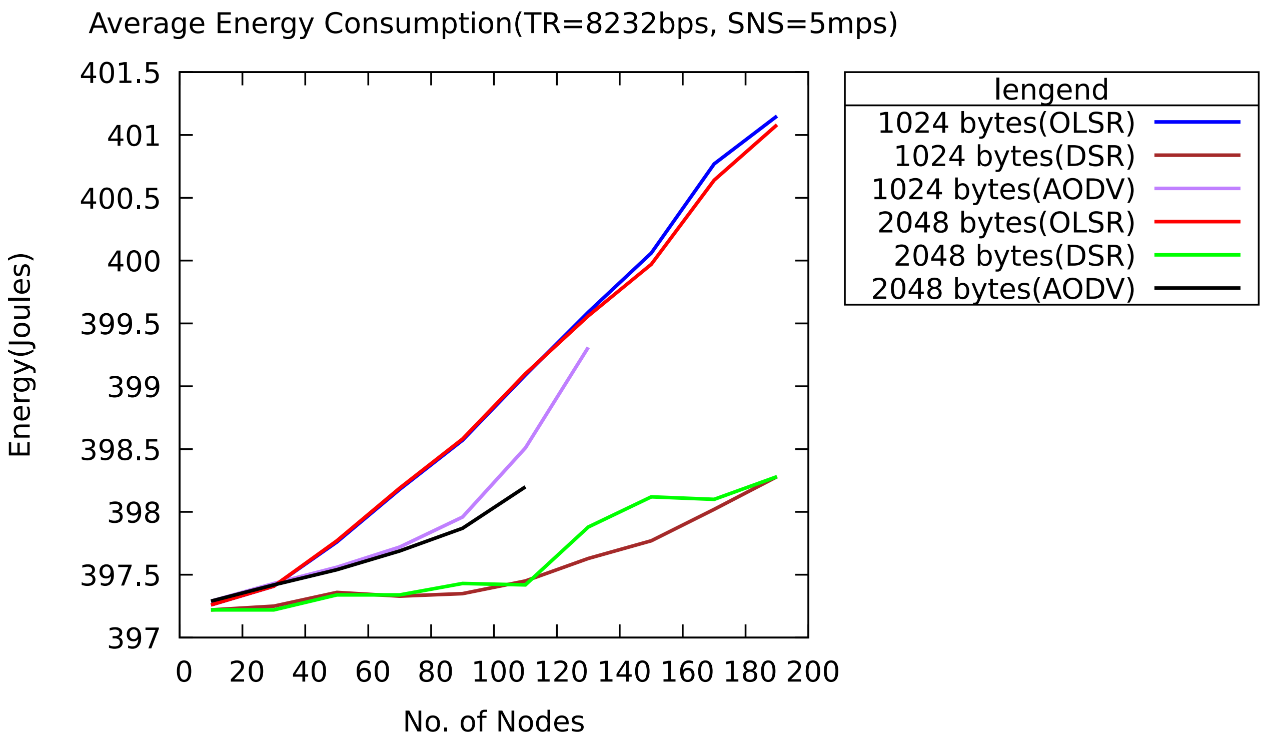

Figure 5.9: Average Energy Consumption Vs. Data Packet Size

Similar to OLSR and AODV, both lines seem to move upward overlapping each other in the beginning. Still, unlike to other two protocols, DSR with larger data packet size is higher than small data packets size. In comparison to OLSR and AODV, DSR seems to be more energy efficient with different data packets size as they are at the lowest level with changing network size.

To be more precise, the simulated results of all three protocols corresponding to 110 sensor nodes of WIoTSN are tabulated in the table 5.1.

Simulation Result for 110 Sensor nodes In Wireless IoT Sensor Network(WIoTSN)					
Protocol	Transmission Rate(TR)	Sink Node Speed(SNS)	Data Packet Size(DPS)	Average Remaining Energy(Joules)	Average Energy Consumption(Joules)
AODV	8232 bps	5 mps	1024 bytes	2601.49	398.51
			2048 bytes	2601.8	398.2
DSR	8232 bps	5 mps	1024 bytes	2602.55	397.45
			2048 bytes	2602.58	397.42
OLSR	8232 bps	5 mps	1024 bytes	2600.91	399.09
			2048 bytes	2600.9	399.1

Table 5.1: Average Energy Consumption Vs Data Packet Size

Figure 5.10 is a bar chart representation of the table where x-axis defines protocols used for simulation and y-axis defines average energy consumption by WIoTSN. At the selected network size, DSR with both data packet size has the lowest average energy consumption. In contrast, OLSR consumes highest and AODV is between DSR and OLSR average energy consumption range. Therefore, based on the above description DSR is energy efficient under changing the size of data packets scenario.

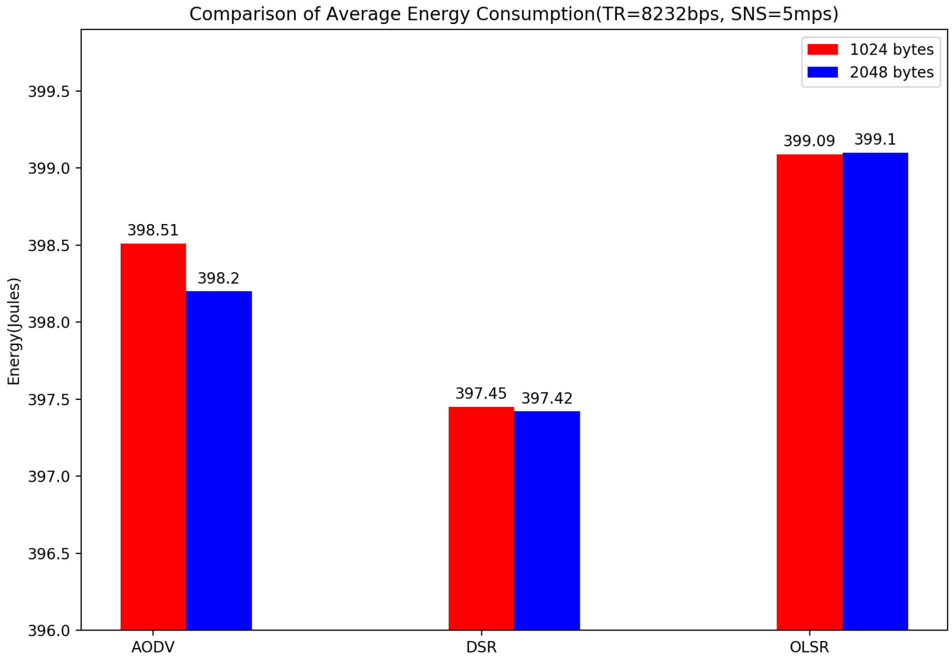

Figure 5.10: Average Energy Consumption Vs. Data Packet Size with 110 sensor nodes

- **Scenario 3: Average Energy Consumption on Scaling the Data transmission rate**

Figure 5.11 is a graphical representation of average energy consumption on different size of network with a change in data transmission rate, i.e. 8232 bps and 32928 bps of AODV, DSR and OLSR routing protocols. The simulation time for this task is 480 seconds with 1024 bytes data packet and 5 mps speed of mobile sensor nodes. As shown in the figure, the total average energy consumption by static sensor nodes of WIoTSN is lying approximately 397 joules to 401.5 joules. Similar to scenario 2, the average energy consumption of OLSR is higher than AODV and DSR routing protocols. The routing protocol DSR is at the lowest level of average energy consumption, whereas AODV lies between DSR and OLSR. The average use is directly proportional to the data transmission rate when comparing itself within the same routing protocol. Both lines representing high and low transmission rate are increasing sharply in OLSR, whereas increasing is slow rate in DSR routing protocols with a different number of nodes without overlapping.

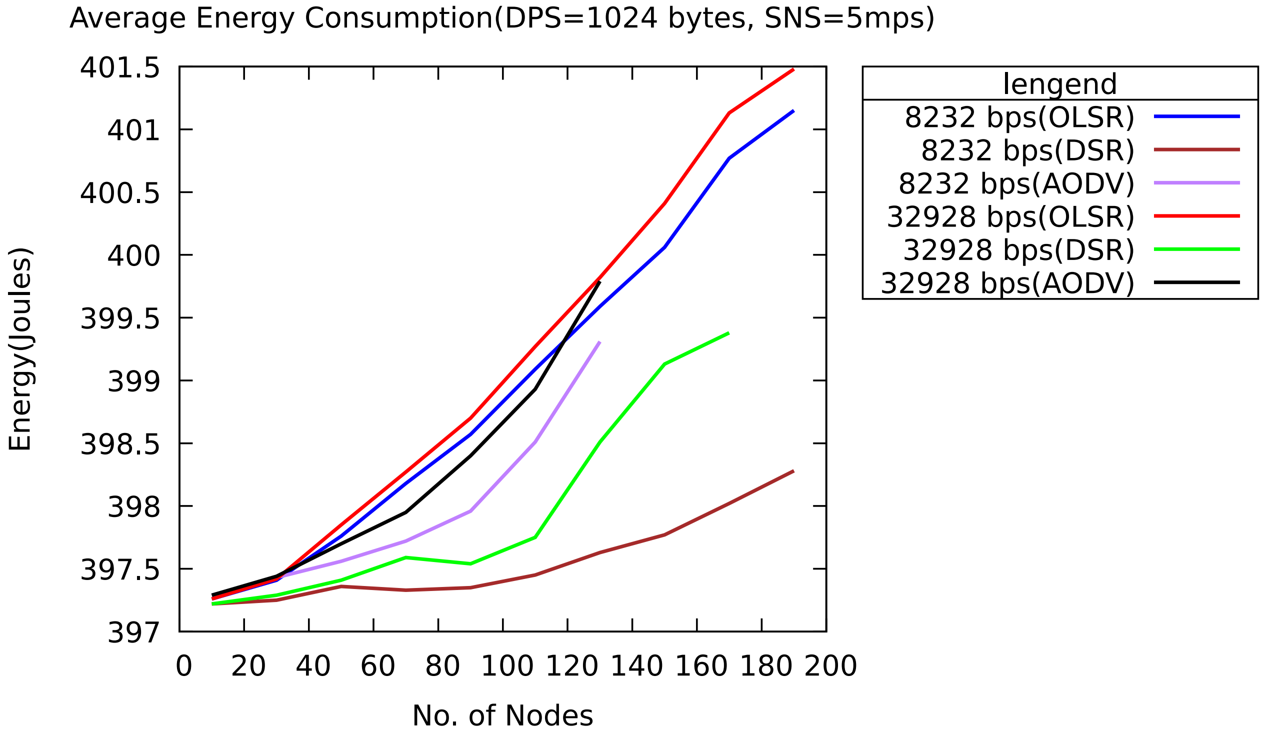

Figure 5.11: Average Energy Consumption Vs. Data Transmission Rate

The simulation results for 110 sensor nodes is taken as an example to inspect and generalize the effects on average energy consumption with a change in data transmission rate. Table 5.2 defines data for OLSR, AODV and DSR routing protocols and its diagrammatic representation is the figure 5.12 with average energy consumption in y-axis and list of used proactive and reactive routing protocols on the x-axis in the experiment.

Simulation Result for 110 Sensor nodes In Wireless IoT Sensor Network(WIoTSN)					
Protocol	Data Packet Size(DPS)	Sink Node Speed(SNS)	Transmission Rate(TR)	Average Remaining Energy(Joules)	Average Energy Consumption(Joules)
AODV	1024 bytes	5 mps	8232 bps	2601.49	398.51
			32928 bps	2601.07	398.93
DSR	1024 bytes	5 mps	8232 bps	2602.55	397.45
			32928 bps	2602.25	397.75
OLSR	1024 bytes	5 mps	8232 bps	2600.91	399.09
			32928 bps	2600.73	399.27

Table 5.2: Average Energy Consumption Vs Transmission Rate

The average energy consumption of AODV with higher transmission rate is maximum than the lower transmission rate. The result is also valid for DSR and OLSR routing protocols. In both of the scenario, the reactive routing protocol DSR has the most moderate average energy consumption. In contrast, OLSR has maximum, and AODV average energy consumption as its values lie between OLSR and DSR. Therefore, under scenario-3 also DSR is energy efficient reactive routing protocol.

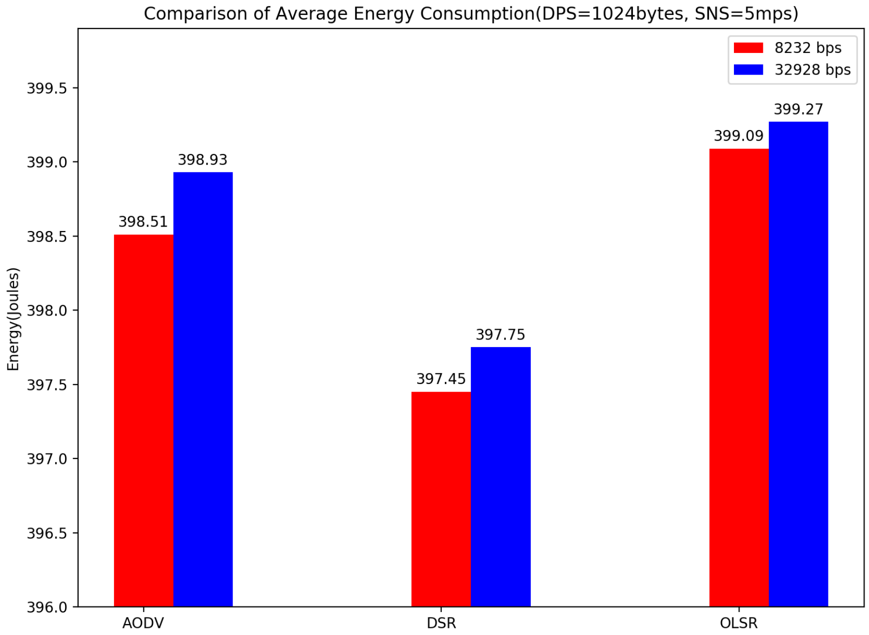

Figure 5.12: Average Energy Consumption Vs. Data Transmission rate with 110 sensor nodes

- **Scenario 4: Average Energy Consumption on Scaling the Speed of mobile sink Node**

  Table 5.3 shows the collection of simulation data for the mobile sink node for running with three different speed, i.e. 2 mps, 5 mps and 8 mps. Here transmission rate and data packet size are constant throughout the simulation, i.e. 8232 bps and 1024 bytes respectively.

Simulation Result for 110 Sensor nodes In Wireless IoT Sensor Network(WIoTSN)					
Protocol	Data Packet Size(DPS)	Transmission Rate(TR)	Sink Node Speed(SNS)	Average Remaining Energy(Joules)	Average Energy Consumption(Joules)
AODV	1024 bytes	8232 bps	2 mps	2010.75	989.25
			5 mps	2601.49	398.51
			8 mps	2748.97	251.03
DSR	1024 bytes	8232 bps	2 mps	2012.91	987.09
			5 mps	2602.55	397.45
			8 mps	2749.82	250.18
OLSR	1024 bytes	8232 bps	2 mps	2008.63	991.37
			5 mps	2600.91	399.09
			8 mps	2748.89	251.11

Table 5.3: Average Energy Consumption Vs Sink Sensor Speed

Figure 5.13 is a graphical representation of the above-tabulated data for AODV, DSR and OLSR. In the figure, similar to the above scenario, the x-axis shows a list of routing protocols based on reactive and proactive characteristics on route discovery method and the y-axis represents average energy consumption defined in joules. The bar chart presents a summary of energy efficiency on changing mobile sink speed. As described in figure 5.13, the total average energy used during simulation is higher when the mobile sink sensor node has a minimum speed and vice-versa. It is because average energy consumption is inversely proportional to the speed of nodes. The sensor nodes with higher speed take less to finish the task and thus consumes less energy. Whereas if it has lower speed takes more time to finish the job that requires more energy. During the experiment, the total time needed for completing the simulation is different while changing the variable of sink speed, keeping other variables such as transmission rate and data packet size constant.

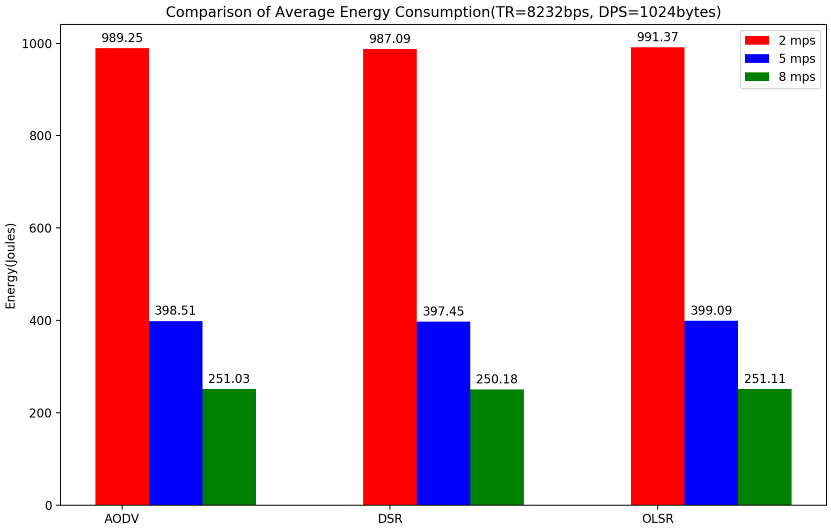

Figure 5.13: Average Energy Consumption Vs. Sink Speed with 110 sensor nodes

> Therefore, under all three conditions of speed(2 mps, 5 mps and 8 mps) of sink nodes, DSR consumes a minimum amount of average energy with respective simulation conditions. Similarly, proactive protocol OLSR requires the maximum amount of energy, and AODV needs more power than DSR but lesser than OLSR. Thus, DSR is an energy-efficient routing protocol than AODV and OLSR under this scenario.

Thus, the reactive routing protocol DSR is energy-efficient routing protocol than AODV and OLSR according to the results of simulation under above-defined scenarios, i.e. changing the number of sensor nodes, changing data packet size, changing data transmission rate and changing the speed of sink node in WIoTSN.

5.3 Security

As mention in section 2.2, there are so many security vulnerabilities still exist in IoT, and significant security threats are reported using IoT devices. If IoT devices are not secured technically, there is a high possibility of losing a considerable amount of potential customers in the IoT market. To retain those customers, it is essential to increase the security features of IoT. While mentioning the importance of security in IoT, which cannot be denied, being wireless nature of WIoTSN energy constraints also cannot be avoided. It is because energy efficiency is also essential to increase the network life in WIoTSN.

To resolve energy efficiency and security issues of WIoTSN, it is wise to choose the middle path so that secure energy-efficient WIoTSN is achieved. IoT scholars, researchers, have started their research towards safe energy-efficient of the routing protocol. Al-Sakib Khan Pathan and Choong Seon Hong [38] are one of them, who jointly propose a secure energy-efficient routing protocol around 2007. According to them, they identify wasteful energy consumption in WIoTSN and restructuring energy-efficient routing protocol with security. Their protocol was handling authenticity and confidentiality between sensor nodes and the base station in WIoTSN. Therefore, more intensive researches should be directed towards the way two researchers had started so that efficiency, along with security, can be achieved. This act of IoT scholar community brings more secure energy-efficient IoT devices and helps to mature the IoT market.

6 Conclusion

The goal of this thesis is to evaluate energy-efficient data routing along with the importance of security in WIoTSN. The importance of security issues on WIoTSN are highlighted in the thesis. Still, its practical experiment along with energy efficiency data routing is not conducted since the network simulator NS3 does not support security implementation. Therefore, the actual implementation of security issues is left for future work to the interested researchers. I think further research on secure energy-efficient data routing for IoT helps to stabilize the IoT market and increases more trust. To achieve the energy-efficient data routing objective, the problem statement is expressed under section 1.1, and two approaches are used, i.e. literature review and experimental simulation testing using Network simulator tools NS3.

The sub-question of problem statement called ”routing protocols” is addressed in chapter 3. In this chapter, communication models of IoT are introduced, and different types of proactive and reactive protocols are reviewed along with their features for route discovery. The discussion is based on the published paper, online blogs, websites etc. Similarly, the two sub-questions, i.e. ”supports” and ”energy efficiency” are addressed by simulation testing approach. In the simulation testing, the stable simulator NS3 is used with consistent Ubuntu using hypervisor. The reason for selecting NS3 is explained in chapter 4. This chapter also defines parameters for the simulation to check the energy-efficient data routing for IoT primarily reactive protocol(AODV and DSR) and proactive protocol(OLSR).

The scaling of sensor nodes(Scenario-1), packets size(Scenario-2), data transmission rate(Scenario-3) and sink speed(scenario-4) for the selected reactive and proactive routing protocols are defined in section 5.2, and the results represent the sub-question of problem statement specifying the word “energy efficiency”. The figures in the thesis from 5.4 to 5.13 represents results of above-listed scenarios of simulation test. According to the graphical representation of simulation results, the reactive protocol DSR is less hunger for energy than the other two protocols, i.e. AODV and OLSR.

In conclusion, the reactive routing protocol DSR supports energy efficiency and increase network lifetime. But it is wise to design a protocol that promotes secure energy-efficient data routing for WIoTSN since the security of IoT devices ensures IoT users that their system is well protected.

Bibliography

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. “Internet of Things security: A survey”. In: *Journal of Network and Computer Applications* 88 (2017), pp. 10–28.

[2] C. Alcaraz, P. Najera, J. Lopez, and R. Roman. “Wireless sensor networks and the internet of things: Do we need a complete integration?” In: *1st International Workshop on the Security of the Internet of Things (SecIoT’10)*. 2010.

[3] J. Arkko, D. Thaler, and D. McPherson. “IETF RC 7452: architectural considerations in smart object networking”. In: *IETF, Fremont, US* (2015).

[4] M. A. Bhabad and S. T. Bagade. “Internet of things: architecture, security issues and countermeasures”. In: *International Journal of Computer Applications* 125.14 (2015).

[5] G. Breed. “Wireless ad hoc networks: basic concepts”. In: *High frequency electronics* 1 (2007), pp. 44–47.

[6] L.-H. Chang, T.-H. Lee, S.-J. Chen, and C.-Y. Liao. “Energy-efficient oriented routing algorithm in wireless sensor networks”. In: *2013 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE. 2013, pp. 3813–3818.

[7] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally. “Internet of things (iot): Research, simulators, and testbeds”. In: *IEEE Internet of Things Journal* 5.3 (2017), pp. 1637–1647.

[8] A. Chhabra, V. Vashishth, A. Khanna, D. K. Sharma, and J. Singh. “An energy efficient routing protocol for wireless internet-of-things sensor networks”. In: *arXiv preprint arXiv:1808.01039* (2018).

[9] T. Clausen and P. Jacquet. *RFC3626: Optimized link state routing protocol (OLSR)*. 2003.

[10] V. A. Dhtore, A. R. Verma, and S. B. Thigale. “Energy Efficient Routing Protocol for IOT Based Application”. In: *Techno-Societal 2018*. Springer, 2020, pp. 197–204.

[11] K. D. Foote. *A Brief History of the Internet of Things*. https://www.dataversity.net/brief-history-internet-things. Accessed: 2020-3-12.

[12] J. Gold. *COVID-19 vs. Raspberry Pi: Researchers bring IoT technology to disease detection*. https://www.networkworld.com/article/3534101/covid-19-vs-raspberry-pi-researchers-bring-iot-technology-to-disease-detection.html. Accessed: 2020-3-16.

[13] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions". In: *Future generation computer systems* 29.7 (2013), pp. 1645–1660.

[14] T. R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Kopena. "Network simulations with the ns-3 simulator". In: *SIGCOMM demonstration* 14.14 (2008), p. 527.

[15] https://groups.google.com. *Aodv example with energy*. https://groups.google.com/forum/#!topic/ns-3-users/r96qVKEOVzQ. Accessed: 2020-4-24.

[16] https://groups.google.com. *The ns-3 Network Simulator*. https://groups.google.com/forum/#!forum/ns-3-users. Accessed: 2020-4-24.

[17] I. I. Initiative et al. "Towards a definition of the Internet of Things (IoT)". In: *Revision-1, on-line: http://iot.ieee.org/images/files/pdf/IEEE-IoT-Towards-Definition-Internet-of-Things-Revision1-27MAY15.pdf. Accessed* 27.2017 (2015), pp. 479–501.

[18] A. J. Jara, L. Ladid, and A. F. Gómez-Skarmeta. "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities." In: *JoWua* 4.3 (2013), pp. 97–118.

[19] G. Jayakumar and G. Ganapathy. "Performance comparison of mobile ad-hoc network routing protocol". In: *International Journal of Computer Science and Network Security (IJCSNS)* 7.11 (2007), pp. 77–84.

[20] M. A. Jubair, S. A. Mostafa, R. C. Muniyandi, H. Mahdin, A. Mustapha, M. H. Hassan, M. A. Mahmoud, Y. A. Al-Jawhar, A. S. Al-Khaleefa, and A. J. Mahmood. "Bat Optimized Link State Routing Protocol for Energy-Aware Mobile Ad-Hoc Networks". In: *Symmetry* 11.11 (2019), p. 1409.

[21] J. N. Al-Karaki and A. E. Kamal. "Routing techniques in wireless sensor networks: a survey". In: *IEEE wireless communications* 11.6 (2004), pp. 6–28.

[22] T. Kurakova. "Overview of the Internet of things". In: *Proceedings of the Internet of things and its enablers (INTHITEN)* (2013), pp. 82–94.

[23] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell. “A survey of mobile phone sensing”. In: *IEEE Communications magazine* 48.9 (2010), pp. 140–150.

[24] E. Leloglu. “A review of security concerns in Internet of Things”. In: *Journal of Computer and Communications* 5.1 (2016), pp. 121–136.

[25] H. Liang, S. Yang, L. Li, and J. Gao. “Research on routing optimization of WSNs based on improved LEACH protocol”. In: *EURASIP Journal on Wireless Communications and Networking* 2019.1 (2019), p. 194.

[26] K. L. Lueth. *IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year*. https://iot-analytics.com/iot-2019-in-review/. Accessed: 2020-3-13.

[27] K. L. Lueth. *IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally*. https://iot-analytics.com/iot-platform-companies-landscape-2020/. Accessed: 2020-04-09.

[28] K. L. Lueth. *The Effect of the Internet of Things on Sustainability*. https://iot-analytics.com/effect-iot-sustainability/. Accessed: 2020-04-09.

[29] K. L. Lueth. *Why the Internet of Things is called Internet of Things: Definition, history, disambiguation*. https://iot-analytics.com/internet-of-things-definition/. Accessed: 2020-3-13.

[30] Z. Magubane, P. Tarwireyi, and M. O. Adigun. “Evaluating the Energy Efficiency of IoT Routing Protocols”. In: *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. IEEE. 2019, pp. 1–7.

[31] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. “Internet of things (IoT) security: Current status, challenges and prospective measures”. In: *2015 10th International Conference for Internet Technology and Secured Transactions(ICITST)*. IEEE. 2015, pp. 336–341.

[32] M. A. Mahmud, A. Abdelgawad, and K. Yelamarthi. “Energy efficient routing for Internet of Things (IoT) applications”. In: *2017 IEEE international conference on electro information technology (EIT)*. IEEE. 2017, pp. 442–446.

[33] R. Minerva, A. Biru, and D. Rotondi. “Towards a definition of the Internet of Things (IoT)”. In: *IEEE Internet Initiative* 1.1 (2015), pp. 1–86.

[34] F. Muhammad, W. Anjum, and K. S. Mazhar. “A critical analysis on the security concerns of internet of things (IoT)”. In: *International Journal of Computer Applications (0975 8887)* 111.7 (2015).

[35] A. Nayyar, V. Puri, and D.-N. Le. "Internet of nano things (IoNT): Next evolutionary step in nanotechnology". In: *Nanoscience and Nanotechnology* 7.1 (2017), pp. 4–8.

[36] G. E. B. News. *AI and Edge Computing Combine in Portable Platform for Flu and Potentially Coronavirus Pandemic Forecasting*. https://www.genengnews.com/news/ai-and-edge-computing-combine-in-portable-platform-for-flu-and-potentially-coronavirus-forecasting/. Accessed: 2020-03-23.

[37] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt. "Cross-level sensor network simulation with cooja". In: *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*. IEEE. 2006, pp. 641–648.

[38] A.-S. K. Pathan and C. S. Hong. "A secure energy-efficient routing protocol for WSN". In: *International symposium on parallel and distributed processing and applications*. Springer. 2007, pp. 407–418.

[39] C. Perkins, E. Belding-Royer, and S. Das. *RFC3561: Ad hoc on-demand distance vector (AODV) routing*. 2003.

[40] T. Praveena, M. S. Parthasarathi, and K. Hariharan. "PERFORMANCE ANALYSIS OF DIFFERENT ROUTING PROTOCOL USING WIRELESS SENSOR NETWORK IN NS3". In: ().

[41] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke. "Middleware for internet of things: a survey". In: *IEEE Internet of things journal* 3.1 (2015), pp. 70–95.

[42] K. Rose, S. Eldridge, and L. Chapin. "The internet of things: An overview". In: *The Internet Society (ISOC)* 80 (2015).

[43] M. Rouse. *Wireless Ad-hoc Network(WANet)*. https://searchmobilecomputing.techtarget.com/definition/ad-hoc-network. Accessed: 2020-04-17.

[44] N. Sakovich. *Internet of Things (IoT) Protocols and Connectivity Options: An Overview*. https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview/. Accessed: 2020-04-15.

[45] S. D. Samo, J. L. E. Fendji, et al. "Evaluation of Energy Consumption of Proactive, Reactive, and Hybrid Routing Protocols in Wireless Mesh Networks Using 802.11 Standards". In: *Journal of Computer and Communications* 6.04 (2018), p. 1.

[46] P. Sethi and S. R. Sarangi. "Internet of things: architectures, protocols, and applications". In: *Journal of Electrical and Computer Engineering* 2017 (2017).

[47] N. Shabbir and S. R. Hassan. "Routing protocols for wireless sensor networks (WSNs)". In: *Wireless Sensor Networks-Insights and Innovations*. IntechOpen, 2017.

[48] S. Shapsough, F. Aloul, and I. A. Zualkernan. "Securing low-resource edge devices for IoT systems". In: *2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI)*. IEEE. 2018, pp. 1–4.

[49] B. D. Shivahare, C. Wahi, and S. Shivhare. "Comparison of proactive and reactive routing protocols in mobile adhoc network using routing protocol property". In: *International Journal of Emerging Technology and Advanced Engineering* 2.3 (2012), pp. 356–359.

[50] M. K. Singh, S. I. Amin, S. A. Imam, V. K. Sachan, and A. Choudhary. "A Survey of Wireless Sensor Network and its types". In: *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*. IEEE. 2018, pp. 326–330.

[51] S. K. Singh, M. Singh, D. K. Singh, et al. "Routing protocols in wireless sensor networks–A survey". In: *International Journal of Computer Science & Engineering Survey (IJCSES)* 1.2 (2010), pp. 63–83.

[52] S. Singh, M. Woo, and C. S. Raghavendra. "Power-aware routing in mobile ad hoc networks". In: *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*. 1998, pp. 181–190.

[53] M. Swan. "Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0". In: *Journal of Sensor and Actuator networks* 1.3 (2012), pp. 217–253.

[54] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson. "Architectural considerations in smart object networking". In: *RFC 7452* (2015).

[55] S. Vanthana and V. S. J. Prakash. "Comparative study of proactive and reactive adhoc routing protocols using NS2". In: *2014 World Congress on Computing and Communication Technologies*. IEEE. 2014, pp. 275–279.

[56] A. Varga and R. Hornig. "An overview of the OMNeT++ simulation environment". In: *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*. ICST (Institute for Computer Sciences, Social-Informatics and ... 2008, p. 60.

[57] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash. “Internet of Things (IoT): A vision, architectural elements, and security issues”. In: *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE. 2017, pp. 492–496.

[58] www.aerohiveworks.com. *Private Pre-Shared Key: Simplified Authentication*. http://www.aerohiveworks.com/Authentication.asp/. Accessed: 2020-04-08.

[59] www.avsystem.com. *What is IoT architecture?* https://www.avsystem.com/blog/what-is-iot-architecture/. Accessed: 2020-04-04.

[60] www.intellectsoft.net. *Top 10 Biggest IoT Security Issues*. https://www.intellectsoft.net/blog/biggest-iot-security-issues/. Accessed: 2020-04-06.

[61] www.lexico.com. *Internet of things*. https://www.lexico.com/definition/internet_of_things. Accessed: 2020-03-30.

[62] www.linfo.org. *Routing Protocol Definition*. http://www.linfo.org/routing_protocol.html. Accessed: 2020-04-18.

[63] www.nearfieldcommunication.org. *About Near Field Communication*. http://nearfield-communication.org/about-nfc.html. Accessed: 2020-04-05.

[64] www.nsnam.org. *What is ns-3*. https://www.nsnam.org/about/what-is-ns-3/. Accessed: 2020-4-23.

[65] www.pcmag.com. *Routing Protocol*. https://www.pcmag.com/encyclopedia/term/routing-protocol. Accessed: 2020-2-30.

[66] www.quora.com. *What is the difference between wireless sensor networks and wireless adhoc networks?* https://www.quora.com/What-is-the-difference-between-wireless-sensor-networks-and-wireless-adhoc-networks. Accessed: 2020-04-17.

[67] www.redalkemi.com. *Pros & Cons of Internet of Things*. https://www.redalkemi.com/blog/post/pros-cons-of-internet-of-things. Accessed: 2020-04-04.

[68] www.scalablenetworks.com. *QualNet - Network Simulation Software*. https://www.scalable-networks.com/products/qualnet-network-simulation-software-tool/. Accessed: 2020-3-20.

[69] www.statista.com. *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025*. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed: 2019-12-12.

[70] X. Xiaohui. “Study on security problems and key technologies of the internet of things”. In: *2013 International conference on computational and information sciences*. IEEE. 2013, pp. 407–410.