Research Thesis

Partial Bicasting With Buffering for Proxy Mobile IPV6 Mobility Management in CoAP-Based IoT Networks

SUBMITTED BY

Sajid Anwar
01-245171-017
MS (Telecommunication and Networks)

SUPERVISED BY

Dr. Moneeb Gohar

Department of Computer Science

Bahria University Islamabad Campus

Session 2017-2019

Bahria University
Discovering Knowledge

MS-13

Thesis Completion Certificate

Scholar's Name: Sajid Anwar **Registration No:** 49887

Program of Study: MS (Telecom & Networks)

Thesis Title: Partial Bicasting with buffering for Proxy Mobile IPV6 Mobility Management in CoAP-Based IoT Networks

It is to certify that the above student's thesis has been completed to my satisfaction and, to my belief, its standard is appropriate for submission of Evolution. I have also conducted plagiarism test of this thesis using HEC prescribed software and found similarity index at __16%____ that is within the permissible limit set by HEC for the MS/MPhil degree thesis.

I have also found the thesis in format recognized by the BU for the MS/MPhil thesis.

Principal Supervisor's Signature:

Name: DR. Muneeb Gohar

Date: Feb. 12, 2019

Bahria University
Discovering Knowledge

MS-14A

Author's Declaration

I, Sajid Anwar hereby state that my MS thesis titled "Partial Bicasting with buffering for Proxy Mobile IPV6 Mobility Management in CoAP-Based Internet of Things Networks" is my own work and has not been submitted previously by me for taking any degree from Bahria University or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my Graduate the university has the right to withdraw/cancel my MS degree.

Name of scholar: Sajid Anwar

Date: Feb. 19, 2019

Bahria University
Discovering Knowledge

MS-14B

Plagiarism Undertaking

I, solemnly declare that research work presented in the thesis titled "Partial Bicasting with buffering for Proxy Mobile IPV6 Mobility Management in CoAP-Based Internet of Things Networks" is solely my research work with no significant contribution from any other person. Small contribution / help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Bahria University towards plagiarism. Therefore I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred / cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the university reserves the right to withdraw / revoke my MS degree and that HEC and the University has the right to publish my name on the HEC / University website on which names of students are placed who submitted plagiarized thesis.

Name of the Student: Sajid Anwar

Student / Author's Sign: _____

Acknowledgment

Being grateful to Allah, to whom belongs all the powers and magnificence, this research work is materialized in final shape.

Achievement of anything cannot be done without the involvement of other people. I personally like to say thanks to the Head of Department **Dr. Faisal Bashir** for providing me this wonderful opportunity to learn in his environment. Heartiest thanks to my research supervisor **Dr. Moneeb Gohar** for his support and friendly behavior which never let my mind to think that I'm doing some sort of hard tasks. He makes everything so easy and interesting. Thank you so much to all my teachers specially **Dr. Imran Shafi** (Research Methodology) for making me able to do research work. It was like impossible for me to carry out some research work, but his hard work and dedication was the base of conducting the research for me.

I have no words to say thanks to my **Parents** for so much supportive and having belief that I will complete my degree on time. At the end I would like to thank my friends specially **Ijaz Ahmad**, **Zeeshan Asghar**, **Hafiz Daniyal Aslam**, **Muhammad Sajid** and **Tassawar Abbas** who helped me throughout the completion of my thesis work.

Dedication

To My Parents, Uncle Fazal Malik, Family & Friends.

Abstract

From recently, the innovative technology named as Constrained Application Protocol (CoAP) has been classified for numerous sensors in the field of IoT. Service discovery should be performed again in CoAP to support handover in mobile device. By this the handover delay and packets losses improved expressively. To reduce certain amount of packet losses and delay we will use a partial bicasting with buffering scheme. In proposed scheme, the bicasting is implemented in the "partial" region between the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) when a sensor node comes in the handover domain. At MAG_{new} data packets are buffered throughout handover to forward to sensors nodes and to decrease data losses.

Table of Contents

List of Table

LIST of Figures

Abbreviations

IoT	Internet of Thing
CoAP	Constrained Application Protocol
OSI	Open Systems Interconnection
MQTT	Message Queue Telemetry Transport
SMQTT	Secure Message Queue Telemetry Transport
AMQP	Advanced Message Queuing Protocol
XMPP	Extensible Messaging and Presence Protocol
QoS	Quality of Services
UHM	Ubiquitous Health Monitoring
EMRS	Emergency Response System
PDA	Personal Digital Assistant
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union-Telecommunication
WCDMA	Wideband Code Division Multiple Access
3GPP	3rd Generation Partnership Project
WBAN	Wireless Body Area Network
WSN	Wireless Sensor Network
DDS	Data Distribution Service
MN	Mobile Node
CN	Correspondent Node
AP	Access Point
MAG	Mobile Access Gateway

LMA	Local Mobility Anchor
RA	Router Advertisement
RS	Router Request
BU	Binding Update
BCE	Binding Cache Entry
BA	Binding Acknowledgement
PBU	Proxy Binding Update
PBA	Proxy Binding Acknowledgement
MIP	Mobile IP
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
PMIPv6	Proxy Mobility IPv6
HMIPv6	Hierarchical MIPv6
FMIPv6	Fast Handovers for Mobile IPv6
TCP	Transport Control Protocol
UDP	User Datagram Protocol
HTTP	Hypertext Transfer Protocol
CoA	Care of Address

CHAPTER 1

Introduction

Introduction

In the area of networks wireless networks are the main mechanisms where computer networks can be established through wireless connections connecting the nodes of the network [1]. Basically, this eliminates the barrier of cable usage costs, which is why it is called a wireless network. This implementation will be carried out in physical layer of the network of the Open Systems Interconnection (OSI) model [2]. Communication will be possible having OSI models from the source to the destination, therefore, data is divided into data packets, Internet protocol distributes essentially based on the IP addresses in packet headers [3]. Currently most commonly used IP adaptation is version 4 (IPv4). But also, version 6 of the Internet Protocol (IPv6) begins to be compatible. Internet Protocol version 6 (IPv6) supports longer addresses, providing the opportunity for many more Internet users. IPv6 integrates IPv4 features. Various devices such as phones have become a need. Therefore, a specific Internet protocol is required for mobile devices, so the permanent Internet Protocol (IP) address must be maintained even when moving from one network to another [4]. The problem is that MIP is basically host-based. With every movement, problems such as delay, data loss and signal overload occur. Solution of this problem, the IP of the mobile proxy has been introduced in terms of mobile IP technology. Functionality is updated by the system responsible for tracking the host's developments and launching the required versatility tag in its name. [5].

It is expected that the demand for mobile computing, called "always and everywhere", and a high level of quality of service, will multiply in future. Many types of applications that mobile users expect from wireless networks and many specific QoS those mobile computing environments require will dramatically increase. The rapid increase in demand for high speed Internet- access "anytime, anywhere" is the main concerns, for network operators [6]. The most recent tendency of the central network has been, in general, attentive to appreciate all mobile IP networks (Internet Protocol). The totally Internet Protocol mobile networks, which can be linked to the transmission of media (Telecommunications) and the Internet, organize networks emphatically, where the networks in which IP operates from a mobile user to (AP) that link wireless systems to the Internet. Mobility management are the main and greatest problem for next generation networks [7].

1.1 Internet of Things (IoT)

Communication between different devices through internet is called, "internet of things" [8]. In simple terms, we discuss the machine send and receive data. With progress of the IOT, an article [9] found that the amount of communications equipment on this world is steadily increasing. The article found that the consumption of devices is greater than the total number of inhabitants of the earth. This is the alarming situation in which we expect the number of devices is greater than the number of people. It may be that limit increases, as it is not confirmed on heritage of humans on other planets. From this, we can say that in 2020, in the use of devices to increase people, there will be a huge increase in things that connect with the Web universe, which previously did not exist, or even the introduction, this too use function. The consumption of these devices is greater than the total number of inhabitants of the earth. This is the alarming situation in which we expect the number of devices is greater than the no of people on this earth. Maybe this limit exceeds, but it is not confirmed on the heritage of humans on other globes. As we know people are in huge number in this world the author [9] also abstract that by 2020, the IoT will exceed fifty billion linked gadgets. We can say that in 2020, in the use of devices to increase people, there will be a huge increase in things that connect with the Web universe, which previously did not exist, or even the introduction, this too use function.

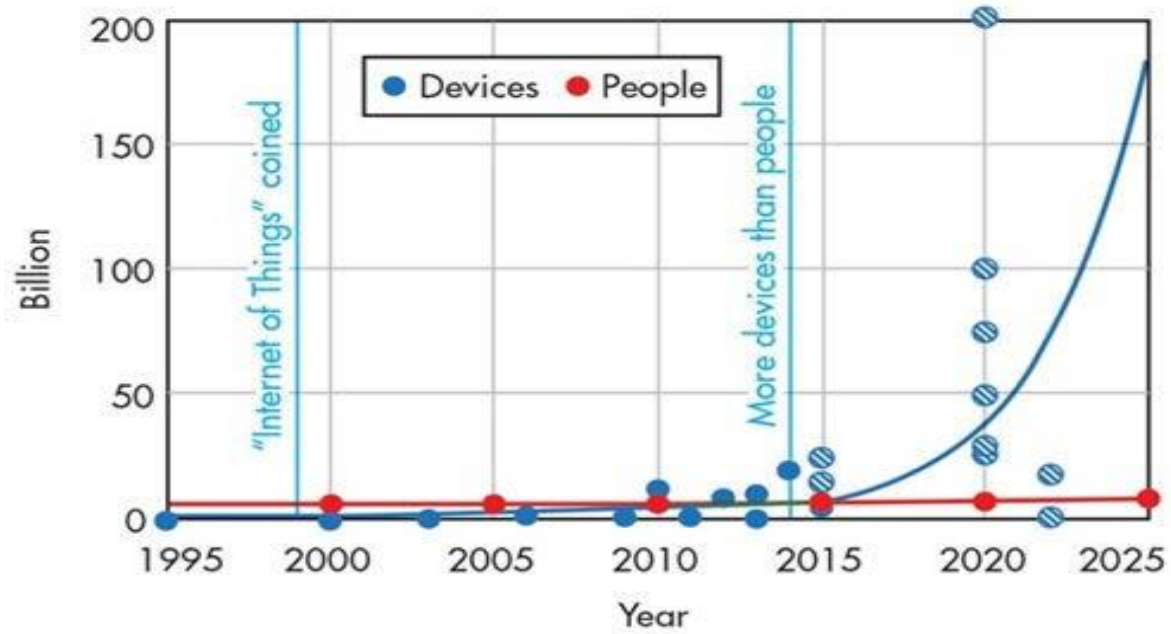

Figure 1. 1 Devices Consumption of IoT [9]

1.2 Wireless Body Area Network

It is the era of 2018, in which we have already touched the sky of technology, and we are becoming more and more involved in making people feel good. A WBAN (Wireless Body Network) and a dedicated human body network were developed to monitor, direct and communicate various vital functions, including blood pressure, temperature, and electrocardiogram (ECG) etc. Several sensors connected to clothing, to the body to control the important functions of various components of the body. WBANs have huge range of new applications; these include the Computer-Assisted Rehabilitation, medical emergency response system (EMRS, ubiquitous health monitoring (UHM) and even life-style promotion healthy [10]. In general, WBAN in UHM helps people stop visiting the hospital that is very difficult for everyone and also reduces the high dependency of a specialized workforce in the health sector.

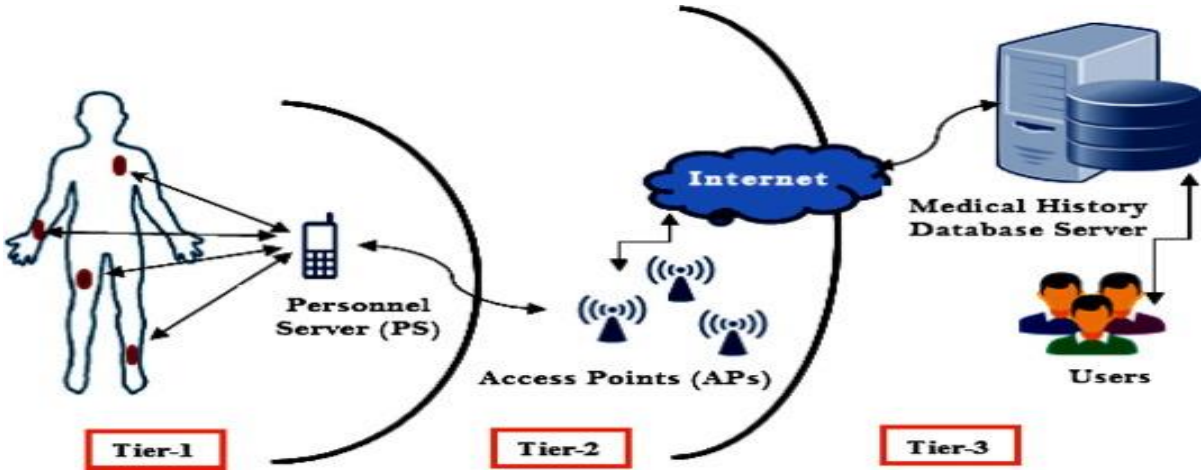

Figure 1. 2 Three-tier Architecture of WBAN [10]

However, in countries where the medical infrastructure and associated personnel are inadequate, it is recommended, and it is difficult to quickly establish a cost-effective health care system. The structure of the wireless body zone network using a three-tiered model is illustrated in Figure 1.2. Basically, the WBAN is a communications network that integrates human and computer peripherals through portable devices. In the WBAN, the common sensor node should ensure the signal to handle the correct signal, take the signal sensor low sensor signal, and wirelessly signal processing to the local processing unit.

1.3 Constraint Application Protocol CoAP

In WBAN for remote control, a special protocol, called CoAP [9], has been introduced, a limited application protocol that transports the data in packets from client to server. CoAP have a much lower weight, so it's easy to use them in smaller devices that have less processing capacity and less memory. Uses the User Datagram Protocol (UDP), which in itself is relatively light compared to others that support options such as forwarding the same message to different recipients simultaneously.

1.4 Problem Statement

To ease the session, reduce packet loss and avoid handover delays is the significance of mobility management, among MN, MAG and LMA, when the MN moves from one network to another network. After entering to a new network domain of Sensor Node (Mobile Node) from MAG_A to MAG_B MN change point of attachments. MAG_B senses the mobile node detachment and achieves the proxy binding update (PBU) functions with local mobility anchor to remove binding state linked with mobile node at the same time. So in this process a certain amount of handover delay and packet losses occur.

1.5 Research Contribution

The research implementations will be divided into 2 phases in 1st phase the Implementation of existing CoAP IoT Based Networks mobility and the 2^{nd} phase based on the Implementation of partial bicasting with buffering for IoT scheme.

1.6 Research Expected Output

From the comparisons in form of Handover in packet loss, End to End Delay, Throughput, Energy consumption, Data packet traces results it will be analyzed that the performance of proposed scheme will be better as compared to the existing system.

Chapter 2

Literature Review

Literature Review

With the speedy development in numerous of mobile users and portable devices like cellular phone, smart phones, other technologies modern systems and laptops, need for “anywhere, anytime, and anyway” speedy Internet is an important alarm [7]. Recent improvements in many wireless technologies, like WCDMA and IEEE 802.16 d, and many other standards such as IETF, ITU-T and third generation partnership project (3GPP) to rise the opportunity of realizing ubiquitous computing environments and mobile devices. However, several challenges still persist to be resolved for achieving such goals.

Internet of things is a platform where day by devices becomes smarter, modern communications becomes more informative as compare to actual internet and processing becomes intelligent. But the Internet of Things communication possible through middleware’s and some basic protocols [12]. When talking about IoT, it is very important to understand that the connection works well. The main factor is that the communication between the endpoints should be done so that less energy and less time is needed from one data transfer to another. All of these IOT procedures must understand communication protocols and determine which is best for work.

2.1 IoT Communication Protocols

Protocols normally utilized in the IoT systems are the following:

2.1.1 Constrained Application Protocol (CoAP)

The CoAP protocol is specified in RFC 7252 and complies with the open IETF standard. This is a web transmission protocol used in nodes or restricted networks such as IoT, WSN, M2M, and so on. The protocol is designed for IoT with less memory and lower power consumption. Because it is designed for web applications, it is also referred to as the "Web of Things Protocol" [13]. It can be used to transport data in web applications from a few bytes to 1000 bytes. The main features of the CoAP protocol as a very efficient RESTful protocol are the integrated web transfer protocol (CoAP: //) and the methods used GET, POST, PUT and DELETE. Use a simple and small 4-byte header. The use of CoAP for message security is used as certificate protection based on PSK, RPK, and DTLS. For reliability, the mechanism uses confirmable messages and non-confirmable messages. The CoAP port number is 5683 and is used for Secure CoAP [9].

The CoAP protocol has two parts

1. Messaging
2. Request Response

Messaging: Messaging is liable for copying and submitting messages.

Request Response: For general communication this layer is useable. Figure 2.1 shows the four messages types of CoAP.

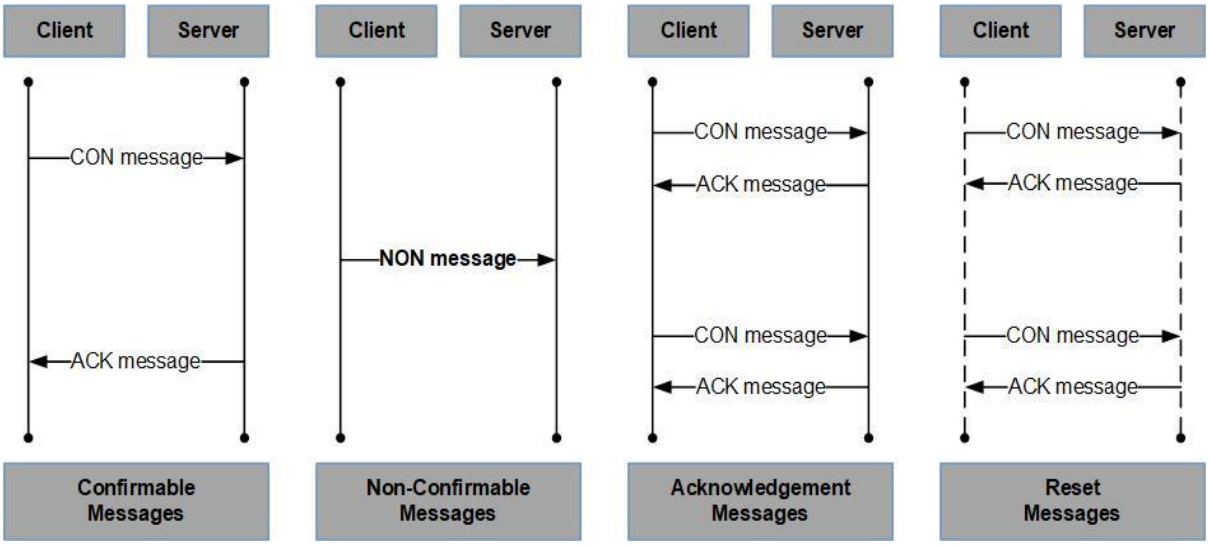

Figure 2. 1 Constrained Application Protocol (CoAP) Operations [9]

Confirmable: This mode shows communication reliability.

Non-Confirmable: This mode shows incredible communication.

Acknowledgement: This part is based on client-server communication. An Acknowledgement message acknowledges that a specific Confirmable message arrived. The server communicates directly with client to forward an answer with additional acknowledgment [14].

Reset: The specified name indicates that the response is sent from the server to the client, but sometimes a reply is sent after the response. A Rest message indicates that a specific message has been received (confirmable or non-confirmed), but a context to process it correctly is missing [15].

CoAP log messages are exchanged in two modes between the CoAP client and the CoAP server without separate response and with separate response. With a separate response, the server informs the client of the receipt of the request message. This increases processing time but

avoids unnecessary retransmissions [13]. Figure 2.2 shows the two ways to exchange CoAP log messages between the CoAP client and the CoAP server.

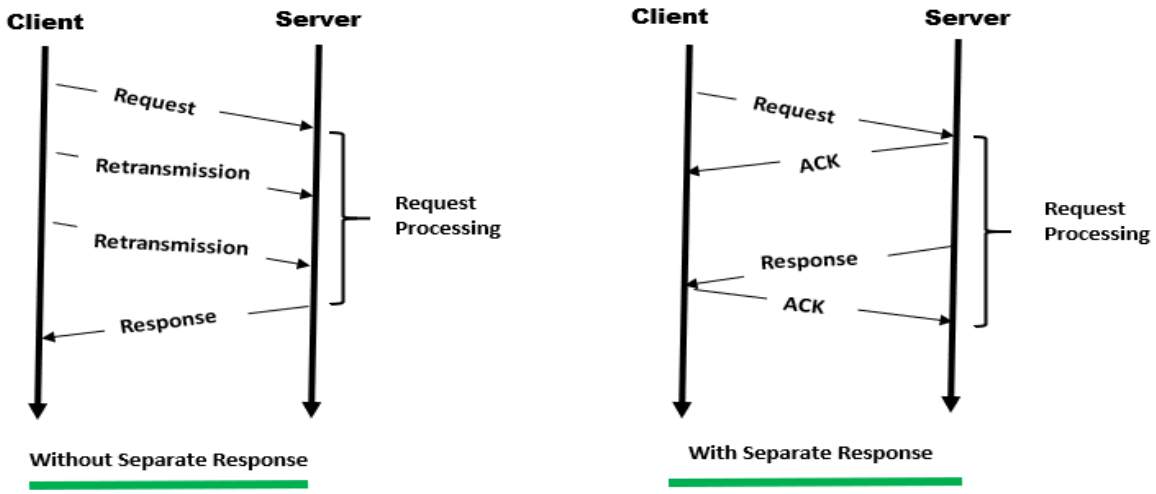

Figure 2. 2 CoAP Message Exchange [9]

2.1.2 Message Queue Telemetry Transport (MQTT)

MQTT is an ISO Standard (IEC/ISO PRF 20922) established on 1999 use the message pattern as Publish/Subscribe based. MQTT considered for small M2M communication. It was established by IBM and now is an open standard. MQTT use for transporting a message is TCP and for security of messages use SSL/TLS. The port number of MQTT is 1883 and 8883. MQTT works on top of TCP/IP protocol and give flexibility in communication patterns. MQTT Use a Topic-based publish/Subscribe Architecture [16]. This architecture is based on 3 components.

1. Publisher
2. Broker
3. Subscribe

Publishers: In the IoT case, publishers act as sensors that need to communicate with subscribers through brokers for communication purposes. The most important thing is that publishers can sleep whenever they need it.

Brokers: Brokers are a bridge for publishers and subscribers. If all information collects from publishers, the broker is responsible for the categorization and subscribers who have subscribed. The broker transmits sensor data to these subscribers.

Subscribers: In IoT subscribers [17], these are applications where brokers need to have an

interest each time the publisher transfer new data to the broker.

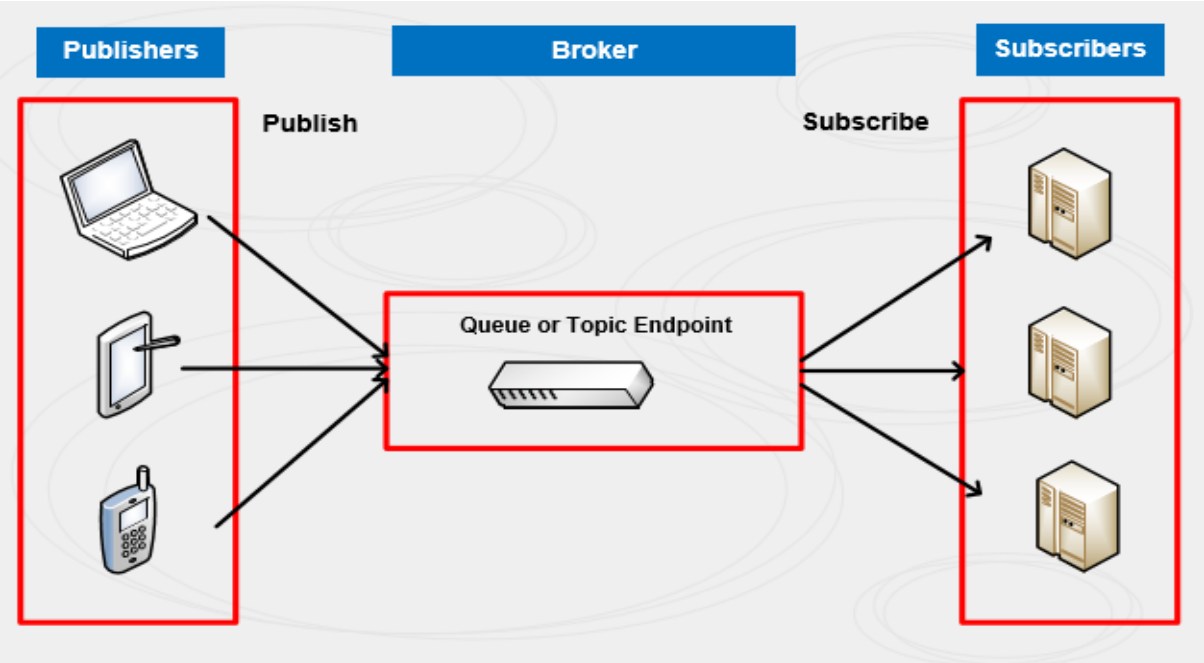

Figure 2. 3 Message Queue Telemetry Transport (MQTT) [16]

2.1.3 Secure Messages Queue Telemetry Transport (SMQTT)

SMQTT [18] is the improved form of MQTT. Everything in this log works like the Message Queue telemetry transport. Security is main concern. In this protocol, a security is functionality added to improve the properties of MQTT. This algorithm uses 4 parts.

1. Setup
2. Encryption
3. Publish
4. Decryption

The brokers are registered with subscribers and publisher and receive a key. Once the data is prepared to be published, publishers will encrypt it. Subscribers receive broker information. Subscribers with same passkey could therefore decrypt the message. It should be noted that the key generation algorithm is not fixed.

2.1.4 The Advanced Message Queuing Protocol (AMQP)

This protocol also works as an MQTT protocol. It is specifically used for the financial sector. It also uses telecommunication protocol and is based on the publishing and subscription model [19].

1. Queues
2. Exchange

Queues: The queues are essentially the representatives of the subjects and the subscribers are already logged on to these queues. So, when data is queued, it sends data to subscribers who have subscribed to those queues.

Exchange: This primary responsibility for this component is to retrieve the publisher's data and then distribute it to the predefined queues [19].

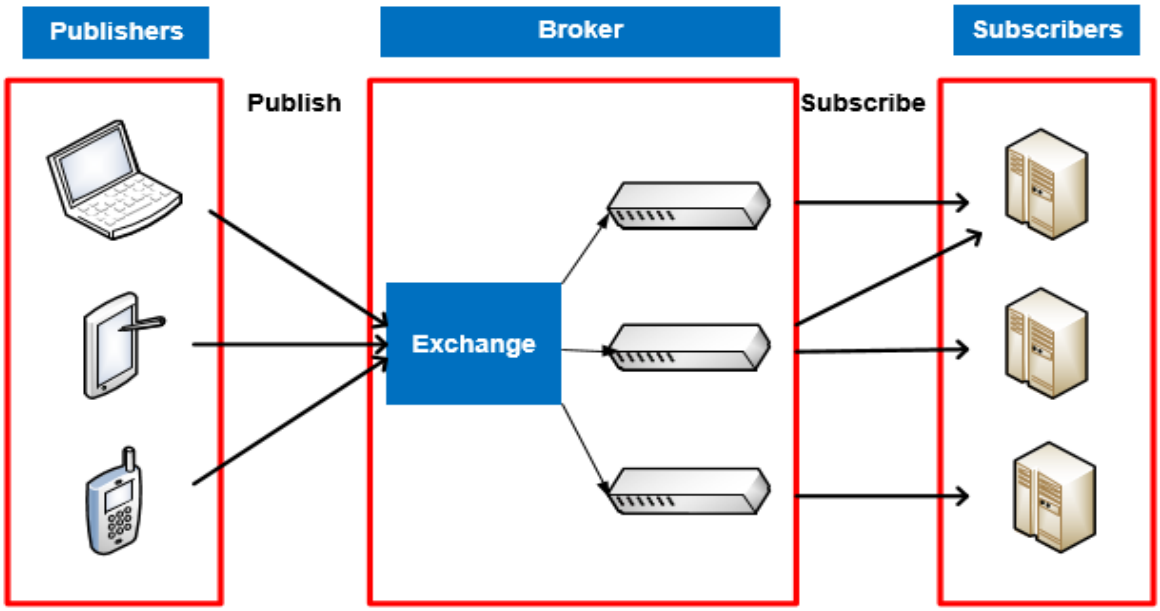

Figure 2. 4 Advanced Message Queuing Protocol (AMQP) [19]

Table 2. 1 Analysis of IoT protocols

Protocols	TCP/UDP	Architecture	QoS Security	Header Bytes	Support LPD
MQTT	TCP	P/S	Both	2	Yes
AMQP	TCP	P/S	Both	8	No
CoAP	UDP	Req/Res	Both	4	Yes

2.2 IoT Mobility Management Schemes

Demand of wireless communication technologies has led to the emergence of numerous new protocols that offer the opportunity to provide mobile users with various superior quality wireless services. Mobility management is key points for direct access to wireless networks and services. This problem allows mobile users who benefit from their services to automatically move without breaking communication systems are changing with the tendency of world-wide connectivity through interconnection and compatibility of varied wireless networks. The movement of a sensor is a very important factor in the IoT range. Mobility in network model is a very complex problem that creates numerous new problems. Thus, the mobility management protocols must be designed with care and efficiency to fulfill the requirements of multimedia applications. In addition, mobility in wireless communication networks affects all communication levels [20].

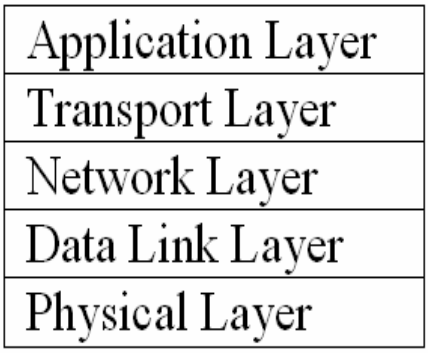

Figure 2. 5 Network Layered Model [20]

At application level, mobility introduces new requirements, service discovery schemas, quality of service and automatic environment configuration. At transport level, an end to end connectivity of the MN may combine wireless and wired connections.

At the network layer level, mobile node mobility means new routing algorithms are needed. Monitoring the movements of a mobile node and maintaining the connectivity of the moving node are two major parts of mobility management, namely location management and provisioning management. On data link level, mobility in wireless networks creates reliability, bandwidth and security issues. On physical level, mobility influences are noticeable due to the characteristics of wireless media. Reusing resources and avoiding interference are two major issues.

2.2.1 Host-based Mobility Management

The mobile node / mobile host (MN / MH) moving from one network to other. All processes related to the signaling that require Protocol modification and changes of the IP address in the mobile node for continuity of session during the handover. That signaling operations contains movement detection, Router Solicitation Request (RtSolReq), Binding updating (BU) and duplicate address detection (DAD) etc. Hierarchical MIPv6 (HMIPv6), fast handover for MIPv6 (FMIPv6) and Mobile IPv6 are the types of Host-based mobility management [21].

2.2.2 Network-based Mobility Management

MN is not involved in signaling process for network-based mobility management. The following protocols have been developed by the IETF working group, mobility management allows communication networks to identify roaming extreme to provide data and maintain connections. Mobility management has two complementary parts [21], namely handover management and location management.

Figure 2. 6 Mobility management classification [21]

2.2.2.1 Handover Phases

Initiation Phase: Mobile user and network or both make the decision to initiate the transfer of deliveries. When the mobile user detects the demand for, the transmission process starts. In network management, network starts the operations.

Preparation Phase: To meet requirements of the quality of service specifications, network of new access point must be prepared for the active call immediately after the startup phase.

Execution Phase: reserved resources have been allocated so that active calls are not interrupted [22].

2.2.2.2 Handover Types

To maintain the mobile user's connections the handover operations used as they move from one network to another these classifications shown in Figure 2.7.

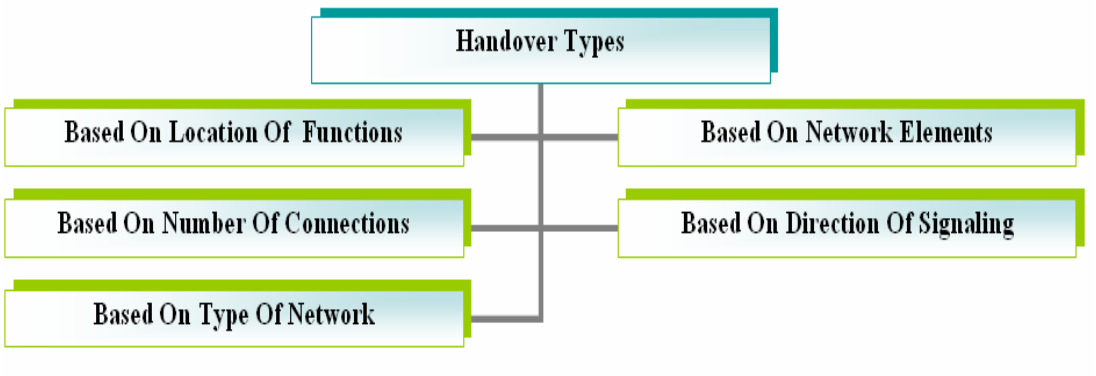

Figure 2. 7 Handover Classification [21]

Mobile Initiated Handover: In this handover transmission where mobile user must manage the transmission. It makes downlink measurement, processes them, decides on the transmission, and determines the destination AR.

Mobile Evaluated Handover: This is like a handover by mobile initiated devices, with the difference that the decision depends on the network.

Network Initiated Handover: In this transmission handover, the networks take over the handover. These include recording uplink measurements, processing them, choosing the transfer, and choosing the destination access router [22].

Intra Cell: The transmission occur with the current coverage area is Intra Cell, where time window is changed for that type of transmission.

Inter Cell: Cell boundary exceeds by mobile user, it is called a inter cell handover.

Inter Network: When the transmission is between different networks, the transmission between networks is referred to Transfers can be classified according to the number of connections made by a mobile user during the transfer process [23].

Soft Handover: The mobile user is simultaneously connected to two accesses. When switching from one cell to another, it is passed "softly" from one access router to another.

Hard Handover: The mobile user forwards the communication from the old connection to the new connection. Therefore, there is only one active connection of the mobile user at a time. There is a brief interruption of the transmission. This disruption must be kept to a minimum to make deliveries transparent.

Forward Handover: Once the mobile user has determined the cell to which they will be transferred, contact the access router that controls the cell. To disconnect the mobile user from the old access router the new access router initiates the handover signal.

Backward Handover: Mobile device has decided which cell you want to transfer, contact the current access router that initializes the signal to be sent to the new router access. This is called reverse handover.

Horizontal Handover: It produces handovers between cells that belong to same network.

Vertical Handover: In this type cells belonging to different network types.

Handover Requirements

The common requirements [22] for the handover process described in this section:

Handover Delay: The total time required to complete the handover must be the mobility rate of the mobile user. Process must be fast.

Scalability: The handover procedure must support handover without data loss within the same network and in different networks

Quality of Service (QoS): The impact of handover on quality of service must be minimal in order to maintain the quality of the requested performance once the transmission is completed.

Signaling Traffic: The traffic needed to make handover minimum.

2.2.2.3 Handover Performance Issues

In addition to the handover requirements described above, performance issues are required to provide uninterrupted service and communication during handover [24].

Fast handover: The handover operations must be fast for the mobile user to receive the data at the new location within a reasonable time frame.

Smooth handover: The handover algorithm must minimize loss, downtime can be long.

Seamless handover: The combination of fast handover and soft hanover is sometimes called seamless handover. While the former is mainly concerned with packet delay, the latter focuses more on packet loss.

Chapter 3

Existing Scheme

Introduction

The Internet of Things is connecting of numerous physical gadgets that interconnect with everyone to implement specific tasks and then sharing data. In Internet of Things For communication, there are separate protocols for each level. As we discussed in the previous chapter, we used the various protocol for each level. We assume in the analysis, that CoAP is the best Internet of Things protocol. For the transport layer we use UDP and for the network layer, since the sensors need to be implemented on the body, so we chose PMIPv6 and inserted the 6LoWPAN into the abstraction layer of the network that works in conjunction with PMIPv6.

3.1 CoAP Communication Execution

Recently, the IETF approved the CoAP [9] as an open standard for M2M and IoT interaction. CoAP uses the same four methods, PUT, POST, GET, and DELETE, as HTTP, when request is sent from a client side to server. However, unlike HTTP, CoAP uses UDP as transport layer protocol to avoid messages congestion and TCP-based extended resource requirements. Reliability & is ensured by confirmable messages, so that the client can specify whether or not to acknowledge a message.

The Constrained Application Protocol (CoAP) is a simple and cost-effective protocol developed for environments such as low-end microcontrollers and high-bandwidth, high-error-burdened networks such as 6LowPANs. It is defined by the open standard IETF RFC 7252. It is available by default for UDP, but it is not limited to it because it can be implemented for others Channel like TCP, DTLS or SMS. The CoAP is based on the request-response communication model and includes support for resource identification, improved reliability, URIs, and more. The protocol was originally developed for M2M requirements, but has also been adapted for the IoT, with support for gateways, high-end servers, and business integration. COAP as HTTP for the REST model with GET, POST, PUT and DELETE, URI, response codes, MIME types, etc., should not be considered as compressed HTTP. CoAP, however, can easily be connected to HTTP Proxy mechanisms where HTTP clients can communicate with CoAP servers, enabling better web services integration and meeting the requirements of the Internet o Things.

CoAP uses a Rest model, for example, by setting a client to the desired temperature so that the client sends Get /Temperature to the server and the server sends 225 ° C/Temperature in reply.

For example, the CoAP client in CoAP in Figure 3.1 wants to obtain a Flash request from the CoAP server so that it forwards “CoN [Oxal5] Get / light” to the CoAP server.

In response, the CoAP server returns the defendant who received same ID, send message, and also include the charge. There is loss of data issue for the CoAP client.

The problem is that the packet is lost between sending and the CoAP client uses the timeout method. When the time is up, the client has not received a response from the server. After this time, the client repeats the same procedure for the server. The identifier of the message should to be identical, after receiving request, the server returns acknowledgment with the same message ID and the payload is included. In the event of a data loss, the client again uses Exponential to reduce the delay.

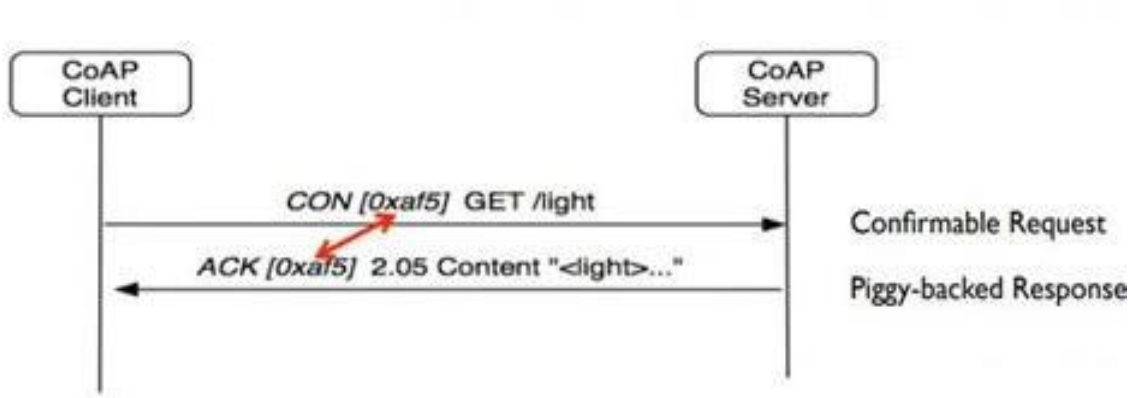

Figure 3. 1 CoAP Request Method [25]

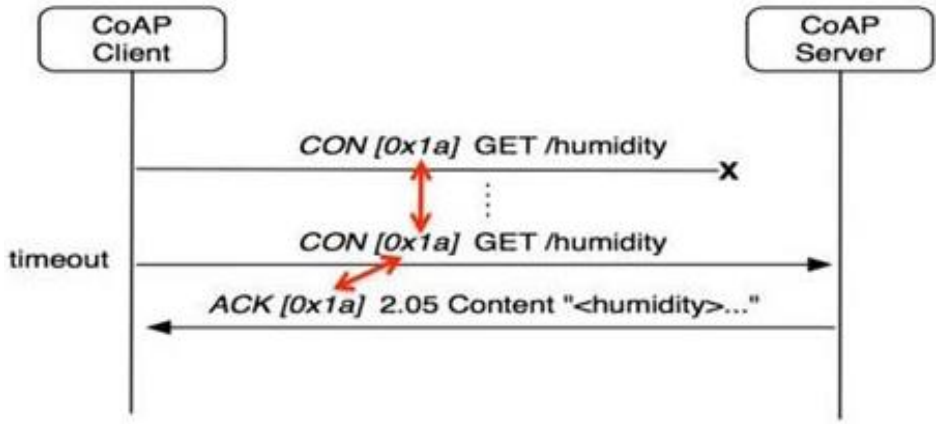

Figure 3. 2 Data Loss in Communication of CoAP [25]

From the server side, we assume that the server needs to do a lot of processing to return to the client. So, the server just sends the blank confirmation with the same message ID. Once the result is achieved, the server separately sends the acknowledgment to the client with a new return using the same token id [25]. Proxy and caching are highly essential points in CoAP. When a client sends information to the CoAP server, the server returns the acknowledgment as a normal process. However, if the client again contacts the server at a specified time through a cache proxy, the acknowledgment is returned within that time interval. This time window is set by the developers.

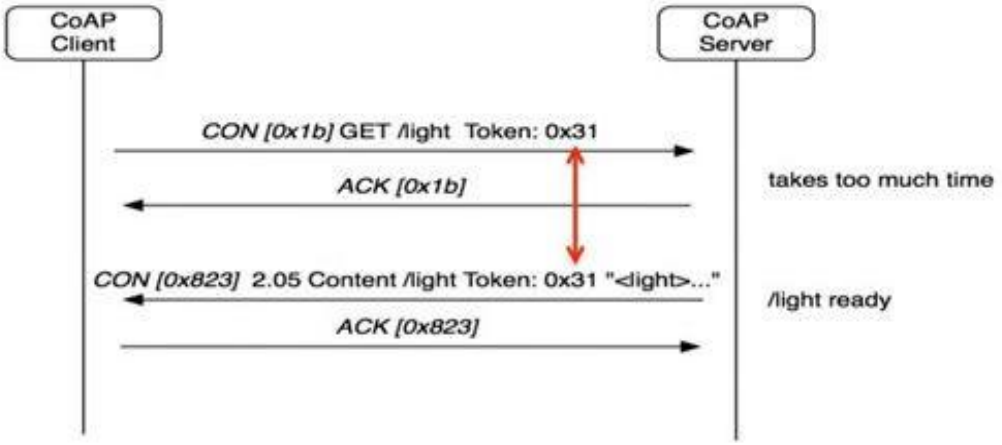

Figure 3. 3 Requests Response in CoAP [25]

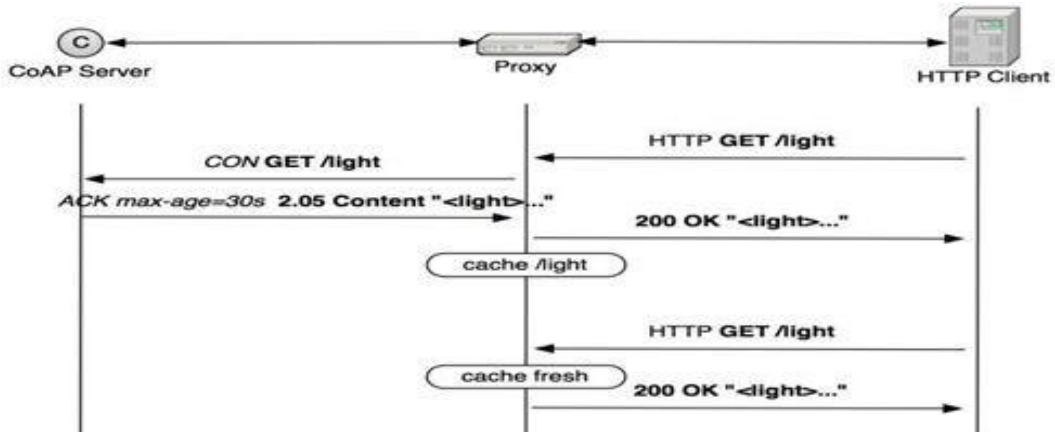

Figure 3. 4 The Process of Proxy and Caching in CoAP Protocol [25]

3.2 User Datagram Protocol (UDP)

The TCP which forwards information to the server, server conveys the message to client as soon as it is received. TCP also executes an error checksum. In UDP [26], the sender constantly sends information to the receiver without ensuring that they are received for that purpose or not. Example is live video streaming, which occurs in the event of loss if the next packet is sent via UDP. The video transmission is blocked at this time but will be accurate in milliseconds.

3.3 Existing Scheme

The proposed model is based on the existing model. We look at the existing scheme 1st and then the go forward to proposed "PBB-PMIP" scheme.

3.4 Proxy Mobile IPv6 CoAP

Proxy Mobile IPv6 (PMIPv6) is a mobility management protocol based on a network designed by the IETF and defined in RFC 5213. Proxy Mobile IPv6 supports a proxy role of the network game operator for the mobile node in IP reporting on mobility. Installation. The mobility substances in the system follow the start of the mobility signal, the MN movement and the configuration of the requested routing status. The most important functional units are the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA). MAG carries out mobility management. The MAG exists on access link where the mobile node is anchored. LMA maintains the reachability status of the mobile node and is the topological anchor of the IP address of the mobile node. The Cisco Wireless LAN Controller (WLC) implements the MAG feature. The key objective of this protocol is to provide mobility support for each IPv6 host in a region of the localized and topologically limited network without the host having to participate in signaling on mobility. Significant PMIPv6 capabilities are supported by support for unmodified IPv4 and IPv6 MNs, efficient use of wireless network resources, independent interconnect technology, and improved crossover performance. The authors [11] proposed approach to CoAP to reduce delayed transmission problems. Figure 3.5 illustrate the process of "CoAP-PMIP" scheme.

1. The sensor is connected to MAG_A. So, MAG_A sends the PBU to LMA, which registers the IP address of the sensor and sends a confirmation PBA to MAG_A (Steps 1, 2, 3).

2. If the Client now wants to convey a request for communication, Client sends his Binding Query to his MAG_C, and the MAG_C sends a Binding Query to LMA. Since LMA has IP address and other sensor values, it receives them and receives an Acknowledgment (Steps 4, 5, 6).

3. Now let's assume a new handover take place.
4. The first sensor is connected to new MAG_B and sends its address to LMA for update so that the new value is inserted into the LMA table after handover. After the update, LMA sends the PBA back to MAG_B (Steps 8, 9, 10).
5. If the Client now wants to communicate with the sensor, Client conveys a Binding Acknowledgment query to the LMA with MAG_C. LMA contains a new sensor device value so it can now communicate (Step 11).

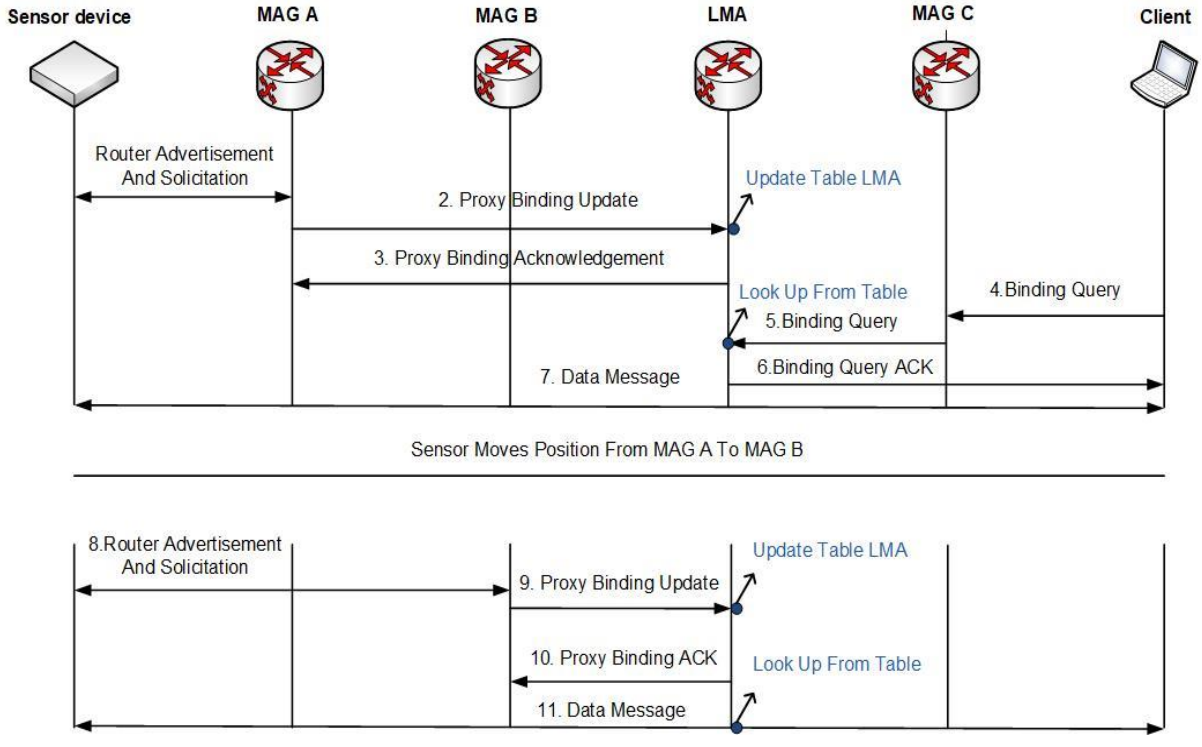

Figure 3. 5 CoAP-PMIPv6 [11]

3.4.1 Internet Control Message Protocol ICMP

Routers used this protocol for sending error messages to client to show that the service is not available.

3.4.2 Solicitation

A kind of message sent by the host to any router to ask those who want to see their presence on the network.

3.4.3 Advertisement

A message type sent by the router to the host to indicate that it is available for routing.

3.4.4 Binding Cache Entry

Caching the LMA connection. An entry contains the MN ID fields, the MAG CoA proxy, and the MN prefix.

3.4.5 Binding Cache

LMA managed cache with ECB.

3.4.6 Binding Update List

MAG managed cache containing information about connected MNs.

3.4.7 Proxy Binding Update (PBU)

MAG sent PMIP packets to LMA to show a new MN. The PBU has the MN ID fields (e.g., MN MAC), the MAG address (Proxy CoA), and a transmission flag to indicate.

3.4.8 Proxy Binding Acknowledge (PBA)

Response to a PBU sent to the MAG by the LMA. The PBA contains the MN ID, the MAG address, and the MN assigned prefix.

Merits: If the sensor moves and the handover takes place, this approach does not use the device discovery procedure. So, the client can therefore perform additional works, and the handover are easy to manage without wasting time.

Chapter 4

Proposed Scheme

Introduction

Up to this section we have studied several IoT communication protocols and their uses in IoT. Then we analyze different mobility systems for IoT groups for IoT networks. We have come to a point where CoAP works fast and PMIPv6 is an improved mobility plan. We begin our implementation by first combining the CoAP with the PMIPv6. This work has already been done by the author, it was necessary to implement it first to carry out our research. In this chapter, we will now discuss our proposed solution Partial bicasting that is how applied on the PMIPv6 CoAP. The PMIPv6 was intended like a network-based mobility model. In [27] the author considers bicasting for the Hanover, which can minimize the loss of packets on a mobile node (MN) during the handover occur. This removes "timing ambiguities" as to when to begin conveying data to the new MN connection. If the bicasting feature is used to support PMIP handover, the following issues still need to be resolved. First, Bicasting PMIP transmission is wasting the resources of the wireless network by forwarding duplicate data. Next, bicasting scheme may still incur data.

From the previous analysis, a new scheme has been proposed that is partial bicasting with Buffering for PMIP handover (PBB-PMIP). In proposed strategy, the bicasting is performed by having the PMIP tunnel in the partial network region between LMA and MAGnew. Data is buffered in the new MAG to reduce data loss during handover. The proposed scheme can take advantage of reduced data loss and handover delay as well as the efficient use of wireless network resources compared to existing handover systems.

4.1 Proposed Scheme

Figure 4.1 shows PBB-PMIP handover with bicasting based for IoT. When MAGold receives a link layer message from the Link-Detected, Then MAGold request to MAGnew to established PMIP tunnel with LMA by sending an INIT message. MAGnew sends a PBU to LMA, then LMA transmits data packets to MAGold and MAGnew. These contain the transmission of Handover INIT from the MAGold to the MAGnew, an exchange of PBU and PBA messages between the MAGnew and the LMA. Thus, the bicasting transmission is performed in the "partial" network area between LMA and MAGnew. Upon receipt of the PBA from the LMA, the MAGnew begins to buffer data from the LMA and asks MAGold to terminate the bicasting by sending a handover ACK message. MAGold will release the old PMIP tunnel by sending a PBU message to the LMA. When the new connection is established, MAGnew transfers the

buffered data packets to the Sensor-device. Thus, a normal data transfer between Sensor-Device and LMA is performed.

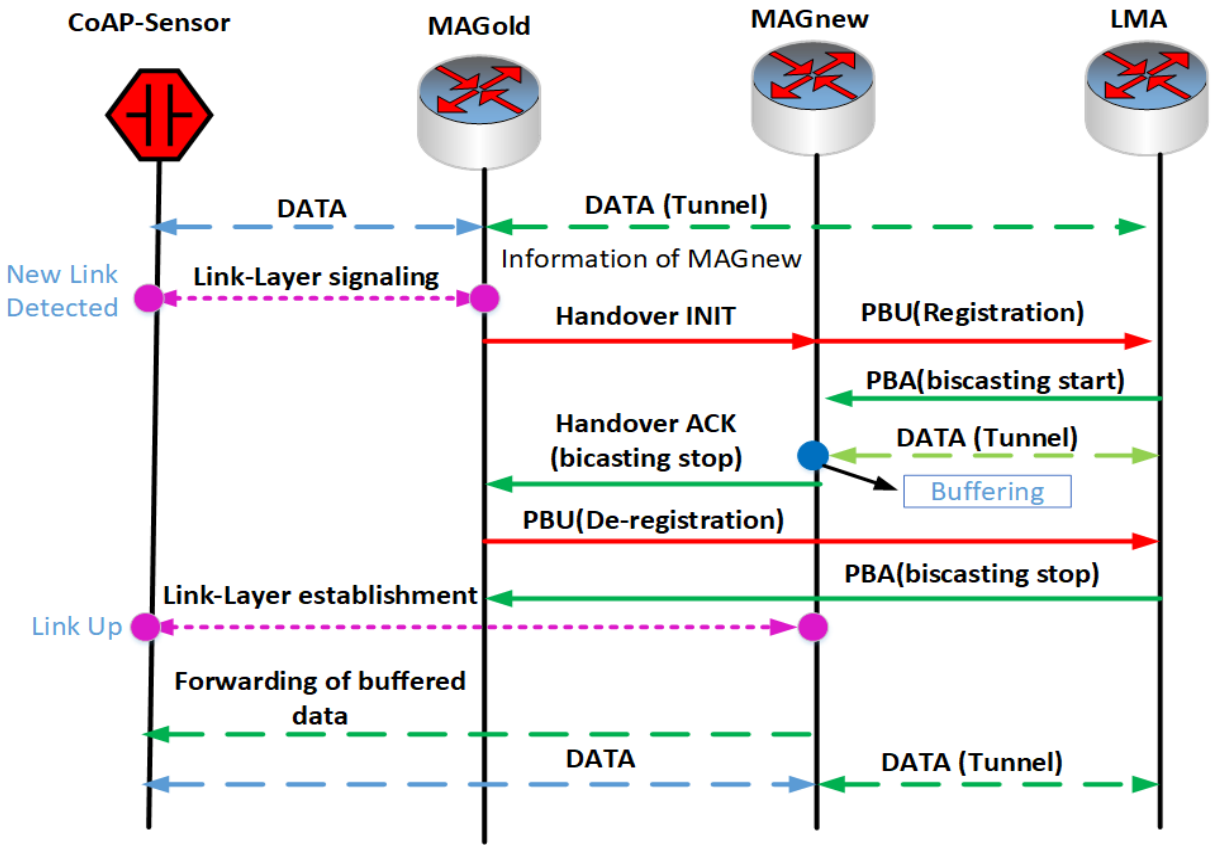

Figure 4. 1 Proposed PBB-PMIP for IoT

In “PBB-PMIP” handover, in the partial region bicasting is performed between the LMA and MAGnew so that the resources of the wireless interconnect network do not need to be used during handover. data loss during handover can be reduced by using MAGnew buffering.

Protocol stack of our proposed partial bicasting scheme in Figure 4.2. In the application layer, CoAP protocol is used which has low overhead and lightweight due to use of UDP, In the transport layer, UDP is used to perform packet delivery.

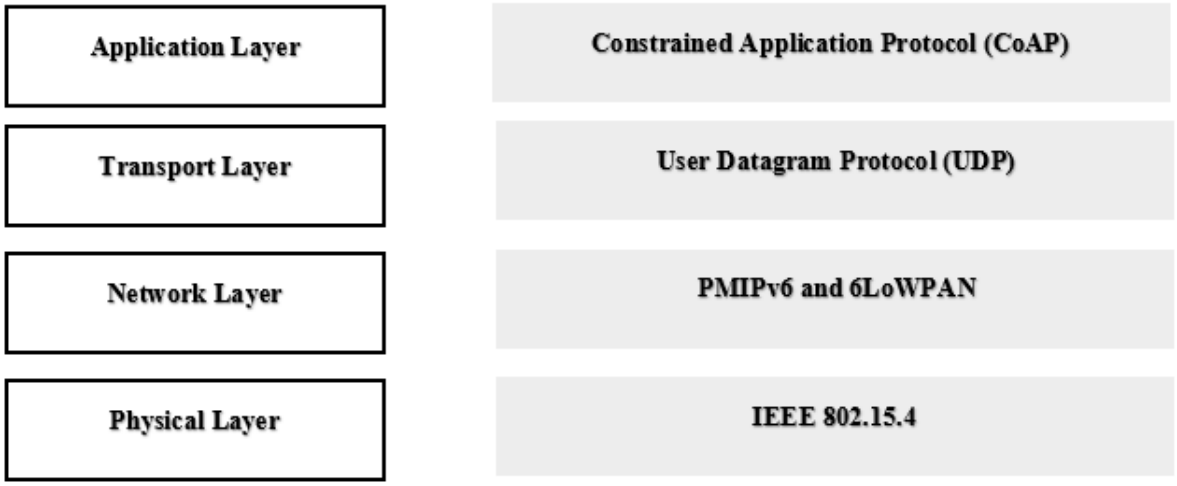

Figure 4. 2 Protocol stack of proposed PBB-PMIPv6 for IoT

Chapter 5

Simulation Analysis & Results

Introduction

Up to this chapter we have implemented Simple CoAP and then Partial Bicasting. We discussed their advantages and disadvantages. We also looked at all the protocols and preview models used for IoT. In this part we are discussing the simulation and performance analysis of these simulations. Improved performance in the less time, less cost, less time consumed handover it is our main goal. Different parameters have been used for simulation These serve essentially as constant values on which the performance evaluation is performed. For development, we use the multipoint network topology. This topology works much better for IoT devices, where there are many sensors and data need to be transmitted in less time and energy. All nodes are interconnected to exchange information. The usage of hub makes communication easier and more reliable.

5.1 Simulation Analysis By NS-3

Simulation is implemented on NS3. NS3 is a network simulation for implementing various protocols. NS3 is widely used due to its efficient simulation and the open platform that allows any developer to implement all network-related work. Figure 5.1 illustrate the simulation network model using ns3.

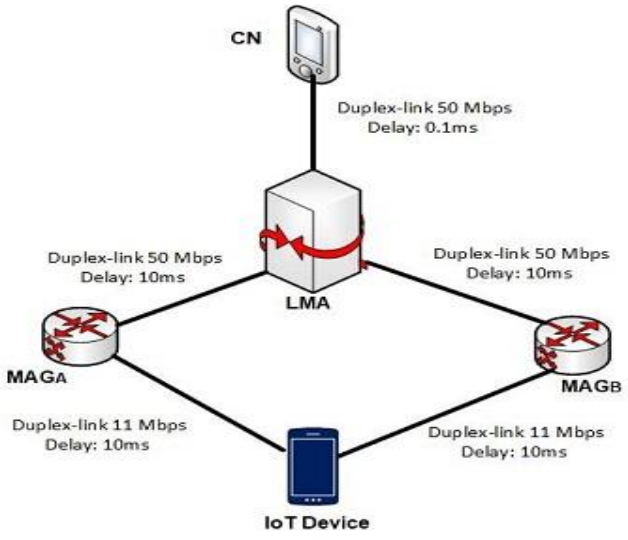

Figure 5. 1 Simulation Network Model

5.2 Simulation of CoAP-PMIPv6

Figure 5.2 illustrate the sensor node transmitting MAG_A to MAG_B to LMA to the Client. The functionality of their communication is discussed in previous chapter. This simulation is

located before the handover state. Figure 5.3 shows that the sensor position has changed. After the transmission handover occur, the sensor restarts the communication.

Figure 5. 2 CoAP-PMIPv6 before Handover (NetAnim View)

Figure 5. 3 CoAP-PMIPv6 After Handover (NetAnim View)

5.3 Simulation of Proposed scheme

Figure 5.4 shows PBB-PMIP for IoT. Figure 5.4 illustrate the sensor device transmitting MAGold to PB-LMA to MAGnew. The functionality of their communication is defined in previous chapter. In PBB-PMIP handover, bicasting is performed in the “partial region”

between the PB-LMA and the MAGnew so that the resources of the wireless interconnect network do not need to be used during handover. Data loss during handover reduced by using MAGnew buffering.

Figure 5. 4 NetAnim view of PBB-PMIP for IoT

5.4 Results

To analysis the performance, we have compared the proposed PBB-PMIP scheme to existing CoAP-PMIP scheme using the ns-3 simulator. To obtain information about the functioning of a proposed scheme, it is important to perform a performance analysis of the existing scheme and the proposed scheme. Table 5.1 shows the parameters we used in simulation.

Table 5. 1 Simulation Parameters

Link between MAGs and LMA	50 Mbps and delays 10 ms
Links between IoT device and MAGs	11 Mbps and delays 10 ms
Handover Occurs	20.5
Operating System	Ubuntu 14.04 LTS
Simulation Software	NS 3.19
Animation Viewer	NetAnim
Data Tracing and Graphs Plotting	Wireshark, MATLAB and Excel

5.4.1 Data packet Traces

Figure 5.5 shows the results describing handover delays and packet losses for the two candidate schemes. CoAP-PMIP and PBB-PMIP, it can be seen that transmission of CoAP-PMIP compared to bicasting handover of PBB-PMIP results in significant packet loss and significant handover delays. Proposed PBB-PMIP scheme produces significantly lower packet losses than the current CoAP-PMIP transmission. In fact, the proposed scheme uses the MAGnew buffer to reduce data loss during transmission.

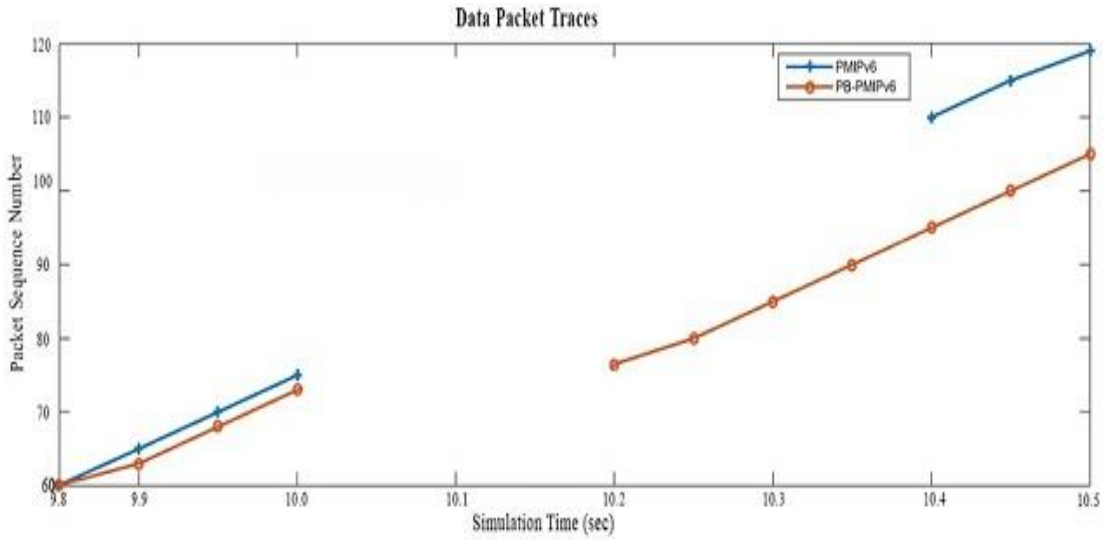

Figure 5. 5 Comparison of data packet trace during simulation

5.4.2 Handover

Figure 5.6 illustrate the handover delays of the two entrant schemes for distinct link switching times. As the link switching time for all entrant schemes increase handover delay increases. It should be noticed that proposed scheme offers less handover delays than CoAP-PMIP handover. PBB-PMIP provide substantially similar handover delays for all link switching times.

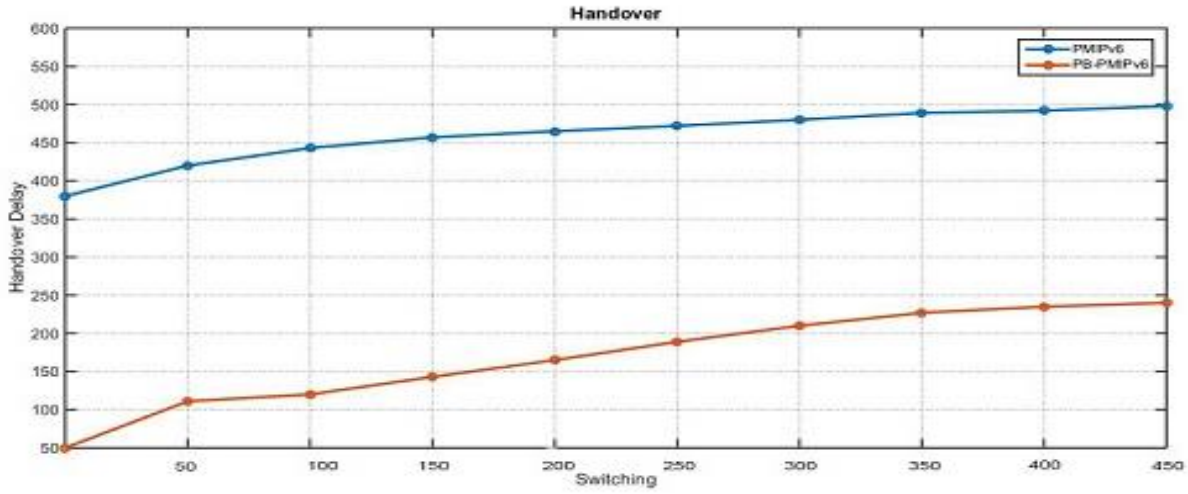

Figure 5. 6 Comparison of Handover Delays during handover

5.4.3 Packet loss during Handover

Figure 5.7 shows number of packets lost during handover. The following figure shows that the existing CoAP-PMIP scheme incur packet loss and increases the number of lost packets as the link switching time increases. If the link switching time is relatively long the proposed scheme is more efficient. In meantime, the PBB-PMIP scheme gives nearly no packet loss even if the link-switching time increases. In fact, in the proposed technique, the data packets are buffered in the MAGnew and then transmitted to the MN when attached to the MAGnew.

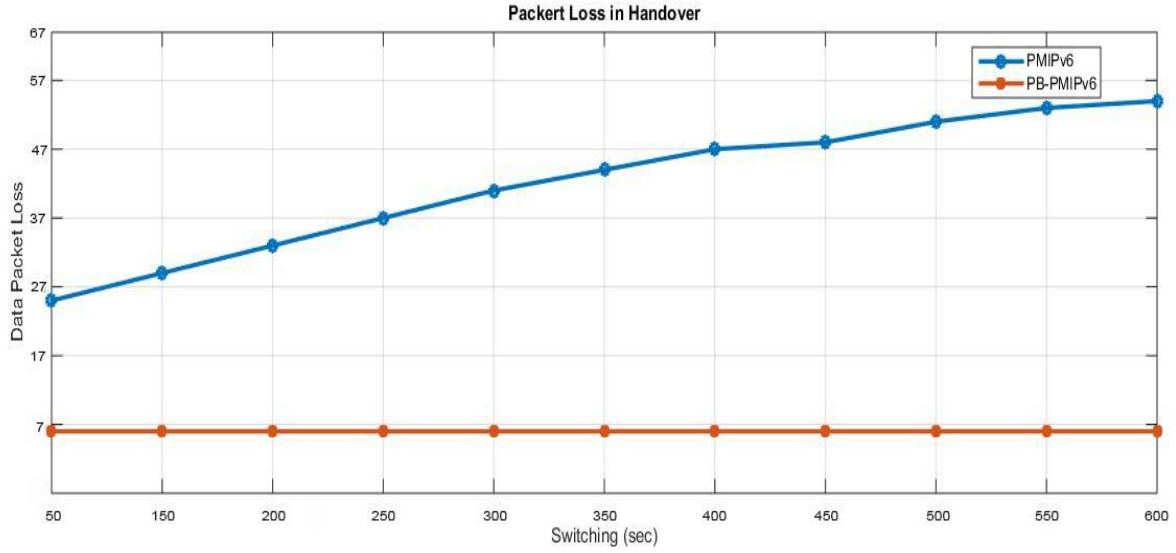

Figure 5. 7 Comparison of lost packets during handover

5.4.4 Throughput

It is stated by total number of packets sent with respect to time. As we can see from Figure 5.8 the exiting scheme shows poor throughput due to dysconnectivity of devices, after handover every device has to connect with each other again for communication, but in our proposed scheme presence of data tunnel between MAGnew and LMA throughput become increases.

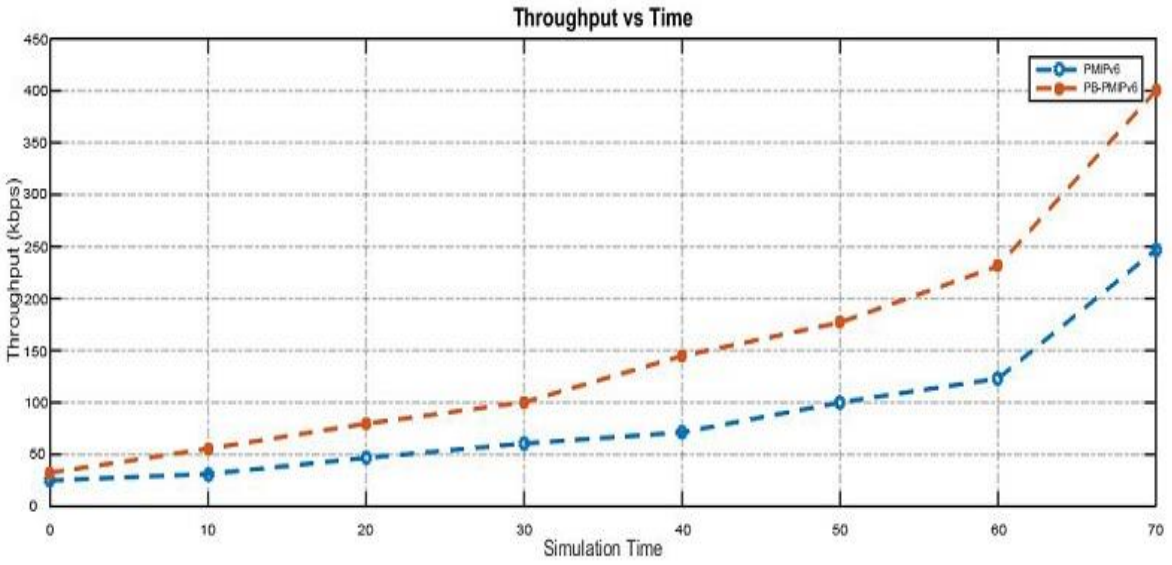

Figure 5. 8 Comparisons of Throughput vs Time

5.4.5 End to End Delay

Figure 5.9 shows end to end delay between entrant schemes. As Figure 5.9 shows at start there is no difference in delay, both schemes show same position because there is no communication, when handover occurs on 20.5 seconds the performance of existing scheme decreases due to mobility, sensors become disconnected. After handover every sensor needs to be connected again to continue communication. On the other hand, delay of proposed scheme increased at a point but when it uses MAGnew the handover reduces.

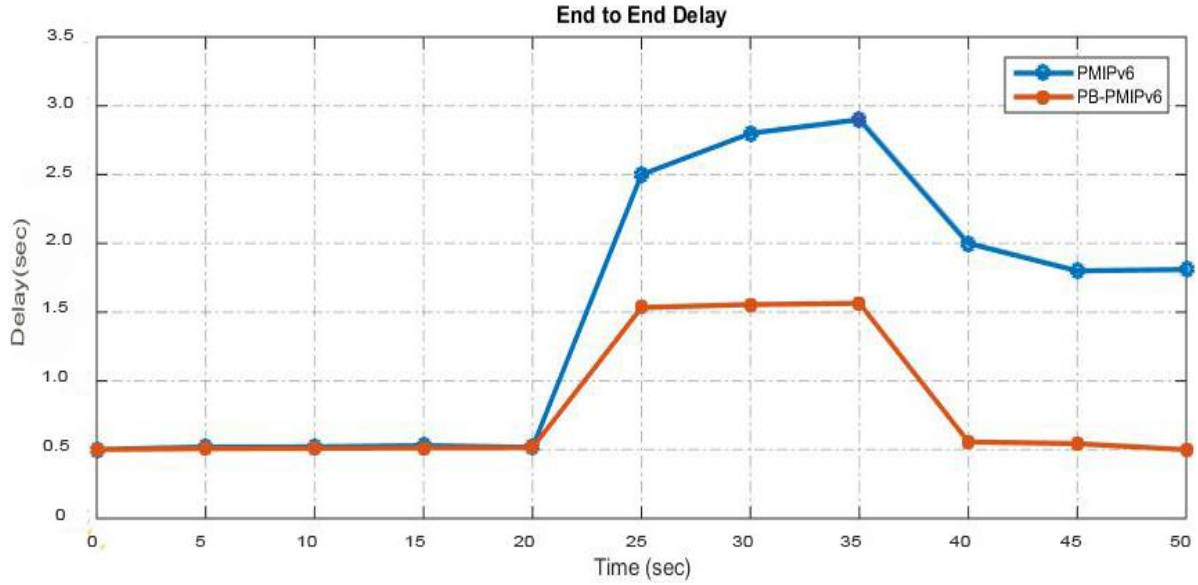

Figure 5. 9 Comparison of End to End delays

5.4.6 Energy Consumption

Energy utilizes by the devices called energy consumption, Figure shows consume energy of different schemes during communication. As shown in Figure 5.10 we can see that PB-PMIPv6 is better than CoAP-PMIPv6, when handover occurs each sensor has to connect with each other again, this process consumes a lot of energy, but in PB-PMIPv6 energy consume is less due to presence of MAGnew, after handover there is no need to utilize network resources.

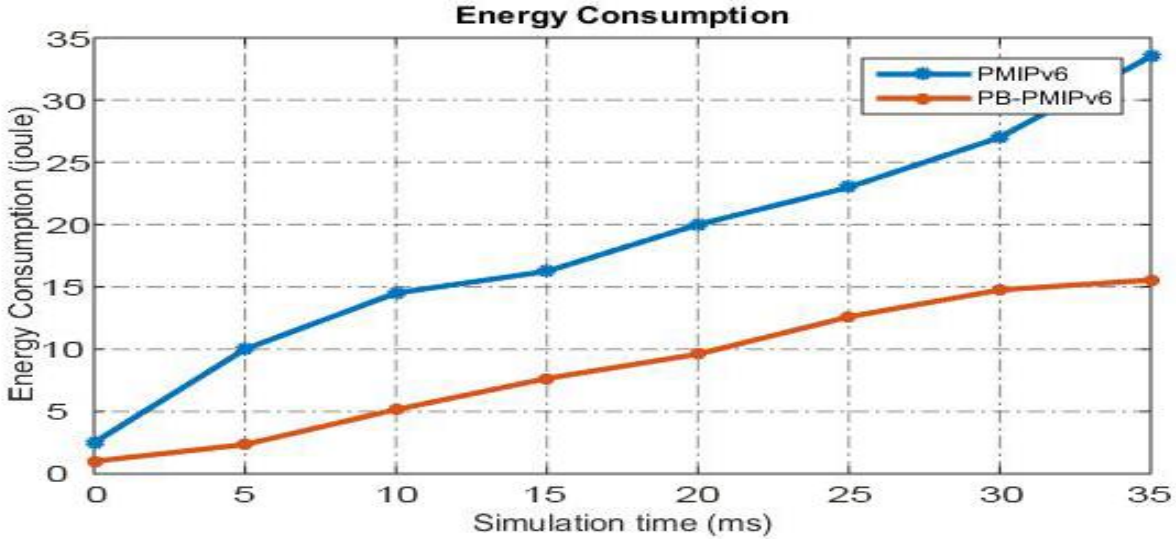

Figure 5. 10 Comparison of Energy Consumed

Chapter 6

Conclusion & Future Works

6.1 Conclusion

It is necessary to summarize everything at the end of this dissertation. This dissertation presented a partial bicasting with buffering to improve performance of the PMIP handover. In proposed scheme, in the partial region bicasting is performed between the LMA and MAGnew and the data packets are buffered in the MAGnew during handover to reduce delay and packet loss so that the resources of the wireless interconnect network do not need to be used during handover. Packet loss during handover can be reduced by using MAGnew buffering. Simulation results shows that the proposed handover scheme in terms of Handover delay, packet loss during handover, End-to-End delay, Throughput, Energy consumption, Data packet traces that the performance of proposed scheme is better as compared to the existing scheme.

6.2 Future Work

In future, we will implement the partial bicasting with buffering scheme (PBB-PMIPv6) for group-based mobility management in IoT.

References

[1] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey", *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] "RFC 7252 - The Constrained Application Protocol (CoAP)", *Tools.ietf.org*, 2018. [Online]. Available: https://tools.ietf.org/html/rfc7252.

[3] V. Cerf and R. Icahn, "A protocol for packet network intercommunication", *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 2, p. 71, 2005.

[4] H. Zolfagharnasab, "Reducing Packet Overhead In Mobile Ipv6", *International Journal of Distributed and Parallel systems*, vol. 3, no. 3, pp. 1-8, 2012.

[5] F. Ganz, R. Li, P. Barnaghi and H. Harai, "A Resource Mobility Scheme for Service-Continuity in the Internet of Things", *2012 IEEE International Conference on Green Computing and Communications*, 2012.

[6] K.E. Malki, H. Soliman, "Simultaneous Bindings for Mobile IPv6 Fast Handoffs", Internet Draft, IETF, November 2001.

[7] Ki-Sik Kong, Wonjun Lee, Youn-Hee Han, Myung-Ki Shin and HeungRyeol You, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6", *IEEE Wireless Communications*, vol. 15, no. 2, pp. 36-45, 2008.

[8] J. Höller and J. Höller, "From machine-to-machine to the internet of things". In *Oxford ; Amsterdam: Academic Press/Elsevier*, 2014.

[9] Woolley, Samuel C., and Philip N. Howard. "Automation, algorithms, and politics| political Communication, computational propaganda, and autonomous agents Introduction." *International Journal of Communication* 10 (2016).

[10] S. Sridharan and H. Shrivastava. "Excogitation of secure data authentication model for wireless body area network". In Computer Communication and Informatics (ICCCI), International Conference on, pages 1–7. IEEE, 2014.

[11] Choi, Sang-Il, and Seok-Joo Koh. "Use of proxy mobile IPv6 for mobility management in CoAP-Based internet-of-things networks." *IEEE Communications Letters* 20, no. 11, 2284-2287, 2016.

[12] Ray, P. "A Survey on Internet of Things Architectures." *EAI Endorsed Transactions on Internet of Things*, 2(5), p.151714, 2016.

[13] "What is CoAP IoT protocol | CoAP Architecture message header", *Rfwireless-world.com*, 2018.

[14] Khattak, Hasan Ali, Michele Ruta, and Eugenio Di Sciascio. "CoAP-based healthcare sensor networks: A survey." In *Applied Sciences and Technology (IBCAST), 11th International Bhurban Conference on*, pp. 499-503. IEEE, 2014.

[15] Levä, Tapio, Oleksiy Mazhelis, and Henna Suomi. "Comparing the cost-efficiency of CoAP and HTTP in Web of Things applications." *Decision Support Systems* 63, 23-38, 2014.

[16] D. Thangavel, X. Ma, A. Valera, H. Tan and C. Tan, "Performance evaluation of MQTT and CoAP via a common middleware", *IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2014.

[17] Kim, Seong-Min, Hoan-Suk Choi, and Woo-Seop Rhee. "IoT home gateway for auto-configuration and management of MQTT devices." In *Wireless Sensors (ICWiSe), 2015 IEEE Conference on*, pp. 12-17. IEEE, 2015.

[18] M. Singh, M. Rajan, V. Shivraj and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)", *Fifth International Conference on Communication Systems and Network Technologies*, 2015.

[19] Karagiannis, Vasileios, Periklis Chatzimisios, Francisco Vazquez-Gallego, and Jesus Alonso-Zarate. "A survey on application layer protocols for the internet of things." *Transaction on IoT and Cloud Computing* 3, no. 1, 11-17, 2015.

[20] J.Z. Sun, J. Sauvola, "Mobility and Mobility Management: A Conceptual Framework", Proc. 10th IEEE International Conference on Networks, Singapore, 205-210, 2002.

[21] Khan, R. and Mir, A. "A Review of Network Based Mobility Management Schemes, WSN Mobility in 6LoWPAN Domain and Open Challenges". *International Journal of Future Generation Communication and Networking*, 7(5), pp.85-104, 2014.

[22] V. Güngör, "Handover Algorithms for Mobile Ipv6", Master of Science., The Middle East Technical University, 2003.

[23] Y.B. Lin, A.C. Pang, "Comparing Soft and Hard Handoffs", IEE Trans. Veh. Technol. Vol. 49, No. 3, p. 792-798, 2000.

[24] C.E. Perkins, "Overview of Mobile IP & Seamoby", Nokia IPv6 Workshop, September 2002.

[25] Jan, Syed Roohullah, Fazlullah Khan, Farman Ullah, Nazia Azim, and Muhammad Tahir. "Using CoAP Protocol for Resource Observation in IoT." *International Journal of Emerging Technology in Computer Science & Electronics, ISSN* 0976-1353, 2016.

[26] Thangavel, Dinesh, Xiaoping Ma, Alvin Valera, Hwee-Xian Tan, and Colin Keng-Yan Tan. "Performance evaluation of MQTT and CoAP via a common middleware." In *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), IEEE Ninth International Conference on*, pp. 1-6. IEEE, 2014.

[27] Mortaza S. Bargh, *et al., "Reducing handover latency in future IP-based wireless networks: Proxy Mobile IPv6 with Simultaneous Bindings," Proceeding of WoWMoM , 2008*.

Sajid-Final Thesis

ORIGINALITY REPORT

16%	11%	9%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jips-k.org Internet Source	4%
2	etd.lib.metu.edu.tr Internet Source	2%
3	Submitted to Higher Education Commission Pakistan Student Paper	2%
4	indigoo.com Internet Source	1%
5	Teklemariam, Girum, Floris Van Den Abeele, Ingrid Moerman, Piet Demeester, and Jeroen Hoebeke. "Bindings and RESTlets: A Novel Set of CoAP-Based Application Enablers to Build IoT Applications", Sensors, 2016. Publication	<1%
6	protocol.knu.ac.kr Internet Source	<1%
7	Le-Trung, Quan, Paal Engelstad, Tor Skeie, Frank Eliassen, and Amirhosein Taherkordi.	<1%

	"Mobility Management for All-IP Mobile Networks", Emerging Wireless Networks Concepts Techniques and Applications, 2011. Publication	
8	voiplab.niu.edu.tw Internet Source	<1%
9	Kim, Ji-In, and Seok-Joo Koh. "Partial Bicasting with Buffering for Proxy Mobile IPv6 Handover in Wireless Networks", Journal of Information Processing Systems, 2011. Publication	<1%
10	www.dsc.ufcg.edu.br Internet Source	<1%
11	Sang-Il Choi, Seok-Joo Koh. "Use of Proxy Mobile IPv6 for Mobility Management in CoAP-Based Internet-of-Things Networks", IEEE Communications Letters, 2016 Publication	<1%
12	pastel.archives-ouvertes.fr Internet Source	<1%
13	s-space.snu.ac.kr Internet Source	<1%
14	Submitted to Middlesex University Student Paper	<1%
15	Submitted to Arab Open University Student Paper	<1%

16	Submitted to Universiti Putra Malaysia Student Paper	<1%
17	diva-portal.org Internet Source	<1%
18	www.macrothink.org Internet Source	<1%
19	Bonam Kim. "A survey of NETLMM in all-IP-based wireless networks", Proceedings of the International Conference on Mobile Technology Applications and Systems - Mobility 08 Mobility 08, 2008 Publication	<1%
20	www.mediateam.oulu.fi Internet Source	<1%
21	Submitted to University of Sydney Student Paper	<1%
22	scholar.sun.ac.za Internet Source	<1%
23	V.C. Giruka, M. Singhal. "Hello Protocols for Ad-Hoc Networks: Overhead and Accuracy Tradeoffs", Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2005 Publication	<1%

Modares, Hero, Amirhosein Moravejosharieh,

24	Jaime Lloret, and Rosli Bin Salleh. "A Survey on Proxy Mobile IPv6 Handover", IEEE Systems Journal, 2014. Publication	<1%
25	Abdelwahed Berguiga, Habib Youssef. "A fast handover protocol for 6LoWPAN wireless mobile sensor networks", Telecommunication Systems, 2017 Publication	<1%
26	T. Ohya. "End-to-end robust IP soft handover", IEEE International Conference on Communications 2003 ICC 03 ICC-03, 2003 Publication	<1%
27	edepot.wur.nl Internet Source	<1%
28	Abel Diatta, Ibrahima Niang, Mandicou Ba. "Cost analysis in FMIPv6 and FPMIPv6-based on HP2P-SIP networks", 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2016 Publication	<1%
29	repository.lib.ncsu.edu Internet Source	<1%
30	ethesis.inp-toulouse.fr Internet Source	<1%
31	uobrep.openrepository.com	

	Internet Source	<1%
32	www.iirs.gov.in Internet Source	<1%
33	www.mdpi.com Internet Source	<1%
34	HyunGon Kim. "Secure and low latency handoff scheme for proxy mobile IPv6", Proceedings of the International Conference on Mobile Technology Applications and Systems - Mobility 08 Mobility 08, 2008 Publication	<1%
35	Ajay Chaudhary, Sateesh K. Peddoju, Kavitha Kadarla. "Study of Internet-of-Things Messaging Protocols Used for Exchanging Data with External Sources", 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2017 Publication	<1%
36	preview-jwcn-eurasipjournals.springeropen.com Internet Source	<1%
37	www.comsoc.org Internet Source	<1%
38	www.freepatentsonline.com Internet Source	<1%

39	Qusay Idrees Sarhan. "Internet of things: a survey of challenges and issues", International Journal of Internet of Things and Cyber-Assurance, 2018 Publication	<1%
40	pure.ltu.se Internet Source	<1%
41	"Recent Advances in Information Systems and Technologies", Springer Nature, 2017 Publication	<1%
42	"Ambient Communications and Computer Systems", Springer Nature, 2018 Publication	<1%
43	"Advances in Wireless, Mobile Networks and Applications", Springer Nature America, Inc, 2011 Publication	<1%
44	Ki-Sik Kong. "", IEEE Wireless Communications, 4/2008 Publication	<1%

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		