Abstract

In the field of Internet-of-Things, Constrained application Protocol (CoAP) has emerged as a new protocol. Recently, some mobility schemes have been proposed based on constrained application protocol based proxy mobile IPv6 (CoAP PMIP). This mobility scheme tends to induce large handover delay and signalling cost because of using a centralized local mobility anchor (LMA) for mobility management and data delivery. To address these problems, a hash-based proxy mobile IPv6 based constrained application protocol is proposed, named CoAP-PMIP-Hash. In the proposed scheme, the functions of Local Mobility Anchor (LMA) are distributed among each Mobile Access Gateway (MAG). The control functions for binding update and query operations are performed based on a hash function. From the simulation results, it is shown that the proposed scheme performs better than the existing scheme in terms of the end-to-end delay, throughput, and signalling cost.

Dedication

I want to dedicate my thesis to my parents. Without their support and prayer, it was not easy for me to complete my thesis.

Acknowledgment

You cannot achieve anything alone. You need the support of your loved ones, your supporters, and friends. Without their prayers and efforts, you cannot achieve your goals. Thanks to **Dr. Moneeb Gohar** my supervisor and Dr. Saleem Iqbal my co-supervisor for their guidance and support. I want to thanks my mother **Rizwana Mushtaq.** Without her support, I will not be able to achieve anything in my life.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Internet-of-things networks

In modern age we can see different things communicating with each other on a complex system is Internet of Things (IoT) [7] [9]. Almost all objects in our daily life are getting digitized and the network of IoT is increasing with each passing day. This could be said as the next generation of innovation where all the objects would be humanized. IoT uses standard internet protocols over which things communicate, the communication could be object to human or object to object [37]. With the introduction of IoT, the communication between machines to machine was also introduced [29].

Simply machines are now sending and receiving messages from each other's. In 2014 George Washington University presented an article in which it was stated that with the development of IoT, the quantity of devices is growing day by day. In article, in 2020 IoT developments will cross 50 billion devices [4].

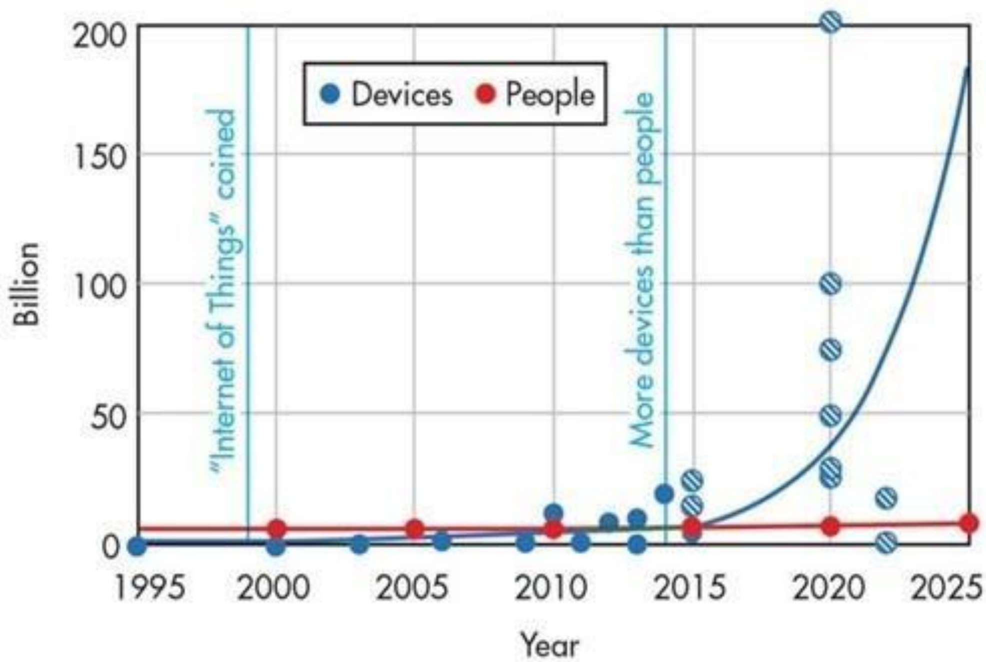

Figure 1.1 Iot Based Devices Consumption[4]

1.2 Wireless Protocols

There are three layers in wireless protocols, the physical layer is layer 1, Network layer is at layer 2 and Third layer is application layer [40].

Physical layer, involves all commonly used wireless technologies such as HART (Highway Addressable), IEEE 802.11 series etc [14] [25].

As network layer or IP /TCP is base for the internet [44] [45]. So communication network over IoT work on Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). As an evaluation between UDP and TCP, TCP is more difficult which is the reason it is not easy to work on resource constrained devices. Most of IoT devices now use UDP. But UDP protocol is not constant. With the combination of Application Layer UDP's stability can be improve [34] [35]. In Application Layer, to provide web services it usually employs HTTP (Hyper Text Transfer Protocol). High computation complexity, high energy consumption and low data rate are some drawbacks of HTTP. So IETF developed many lightweight protocols like Constrained Application Protocol (CoAP), Lean Transfer control Protocol (LTP) [1].

1.3 Constrained Application Protocol (CoAP)

The Constrained Application Protocol (CoAP) is introduced for remote control of multiple sensor devices on WBAN that manages the data packet between the machines and the client server [22]. CoAP can be used on small devices because of its low weight and low processing power and low memory [5] [41]. The Constrained Application Protocol (CoAP) uses a light-weighted User Datagram Protocol (UDP) compared to other principles that support the option of sending the same data to different recipients in the same location [6] [38].

1.4 Research Motivation

As a comparison between constraint application protocols and other protocols in IoT Constrained application protocols are doing very well. CoAP-PMIPv6 was proposed to reduce the handover delay in IoT devices and its results was better than the existing model, CoAP-PMIP. The proposed method focuses on the implementation of CoAp PMIP-hash to reduce handover on CoAP-PMIPv6.

1.5 Problem Statement

In centralized CoAP-PMIP mobility scheme tends to induce large handover delay and signalling cost because of using centralized LMA for mobility management and data delivery. To address these problems, a hash-based proxy mobile IPv6 based constrained application protocol is proposed, named CoAP-PMIP-Hash. In the proposed scheme, the functions of Local Mobility Anchor (LMA) is distributed among each Mobile Access Gateway (MAG). The control functions for binding update and query operations are performed based on a hash function.

1.6 Aim and Objective:

The objective of the proposed scheme is to reduce the handover delay and signalling cost.

1.7 Research Question

Our research will be elaborated by following research questions

1. How to minimize handover delay and signalling cost in Internet of Things environment?

1.8 Thesis Organization

The whole thesis document is divided into four chapters.

I. Chapter 1 provided an overview of mobility management in CoAP based Internet of thing's network. Research objective and research question is also part of this chapter

II. Chapter 2 describes the detail description of IoT and CoAP.

III. Chapter 3 discussion of previous work related to mobility methods and protocols of Internet-of-Things(IoT)

IV. In Chapter 4 it describes our research methodology that what methods we used to address our research problem.

V. Chapter 5 is proposed work.

VI. Chapter 6 is simulation and results.

Chapter 2

Architecture of CoAP and IoT

2.1 Internet-of-Thing's Architecture

Internet-of-things architecture contains 5 layers. These are Perception, Transport, Processing, Application and Business [33] [30].

2.1.1 Perception Layer

This layer is used to observe the characteristics of devices using by different sensors and then convert those data into digital signals so that can be appropriate for network transmission [20]. In perception layer different sensors are like "Network Element" in Telecommunications Network Management. Sensing technology, RIFD technology, bar code etc. are the key techniques in perception layer. To transform the information into digital signals perception layer is used.

2.1.2 Transport Layer

The responsibility for Transport/ Network Layer is to forward information which were received by perception layer through different networks like LAN, Wi-Fi, 3G, Bluetooth etc. This layer is used for transporting the data. Different kinds of protocols are present in this layer like IPv6. IoT connects billion of machines and networks [38]. So, the communication between networks can be critical.

2.1.3 Processing Layer

Processing Layer, it's purpose is to store and then process the data which was received by Transport Layer. Different techniques like cloud computing and database are used to store and process the data because of the large amount of data on layer [15]. And it is very difficult to handle this amount of data.

2.1.4 Application Layer

Processing Layer, after processing the data the Application Layer develop many different applications for the Internet-of-Things like safety, intelligent transportation etc. Application Layer is providing different application to industries. These application can be useful to promote the Internet-of-Things. Application Layer can push Internet-of-Things on larger scale [39].

2.1.5 Business Layer

This Layer acts like a supervisor of Internet-of-Things because it manages the applications and the business models and also research on the model of business and profit. Success of technology depends on the revolution and realistic of business model. Without business model Internet-ofThings cannot have long term development. Business Layer should have to manage the privacy of users which is important in Internet-of-Things[36] [31].

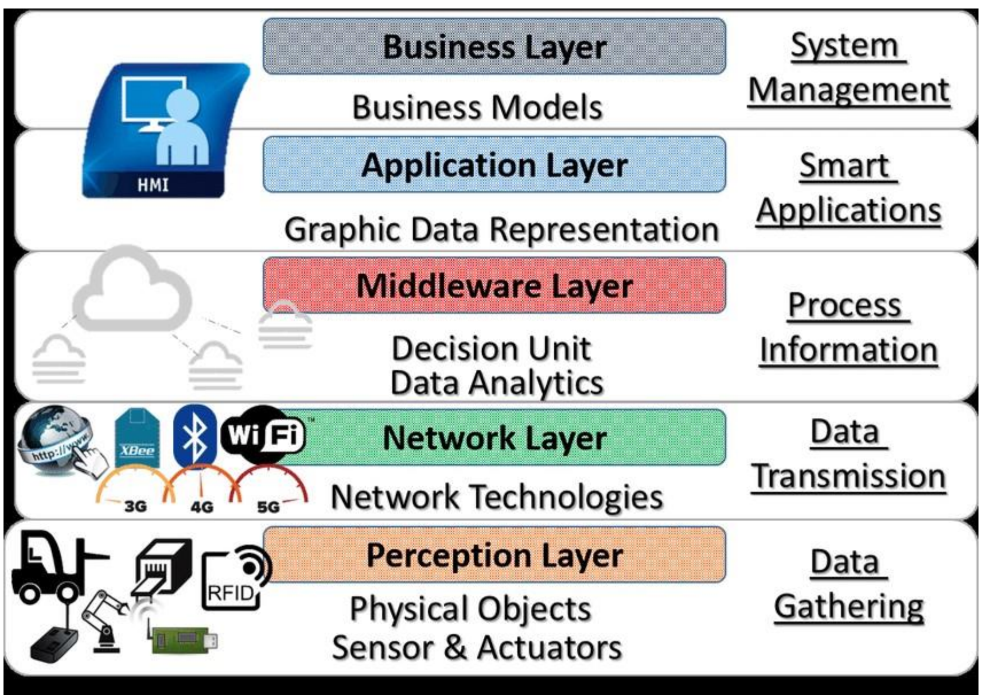

Figure 2.1 Layers of IoT Architecture [36]

2.2 Constrained Application Protocol (CoAP)

Different sensors of remote-control Constrained Application Protocol (CoAP) has been reliable in the Internet-of things (IoT). On the internet many sensors are connected with each other on the Internet-of-Things (IoT). The problem related to constrained sensors like battery consumption,

Internet-Engineering-Task-Force (IETF) has been standardized Constrained Application Protocol (CoAP) to address this problem [48] [13].

In IoT environment, mobility management has been considered as one of the crucial problem. Some workings on Internet of Things mobility management have been made but there were some draw backs [32]. For the continuity of service, Internet-of-Things (IoT) proposed resource mobility scheme which led to a non-optimized problem, by using the tunnel among old gateways and new gateways. Another protocol which did not consider the features of Constrained Application Protocol (CoAP) was proposed which was IP-based wireless sensor protocol [24].

Another scheme was proposed for Constrained Application Protocol (CoAP) which was host based mobility scheme which give possible overhead to sensor devices by increased power consumption and by regular communication through message transmission [2] [12].

For constrained nodes and constrained networks, CoAP used for specific web transfer protocol. It uses same features of HTTP (Hyper Text Transfer Protocol) but it also allows for low overhead, multicast etc. Table 1 reviews protocols [1].

Table 1 Protocols in different layers

Application Layer	COSEM, HTTP, SSH, CoAP, DNS, EBHTTP, SNMP, NTP, DLMS, LTP, IPfix,
Network Layer	IPv4/IPv6, 6LoWPAN, RPL, uIP, SLIP, TCP/UDP

Physical Layer	KNX, Wireless HART, Z-WAVE, IrDA, LonWorks, UWB, PLC

2.2.1 Architecture of CoAP:

CoAP model is same as Client/server model. In CoAP architecture there are two layers. Message layer and request/response layer. Message layer which is bottom layer which is designed according to asynchronous switching and User Datagram Protocol (UDP). Other layer which is request/response layer which deals with the communication and the request/response messages.

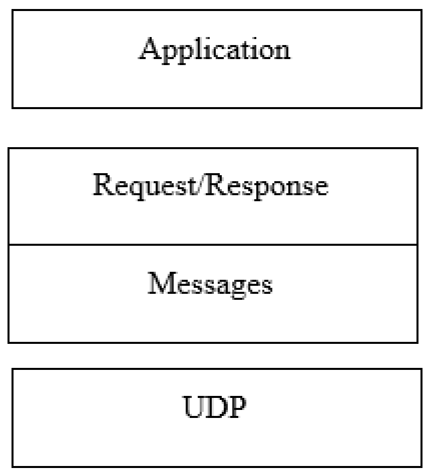

Figure 2.2 Layers of CoAP

2.2.1.1 Message Layer:

This layer supports four types of messages.

- Confirmable.
- Non confirmable.
- Acknowledgment.
- Rest.

In Message Layer all CoAP messages are represented by an ID which is used to find out the same messages.

First category of message is confirmable message. These messages are reliable during the exchange of the messages from both end points. Sender sends the confirmable messages to other end point until it sends the ACK message back. In ACK message there is id of Confirmable of message. If server is facing some issues related to message it will send RST message rather than ACK.

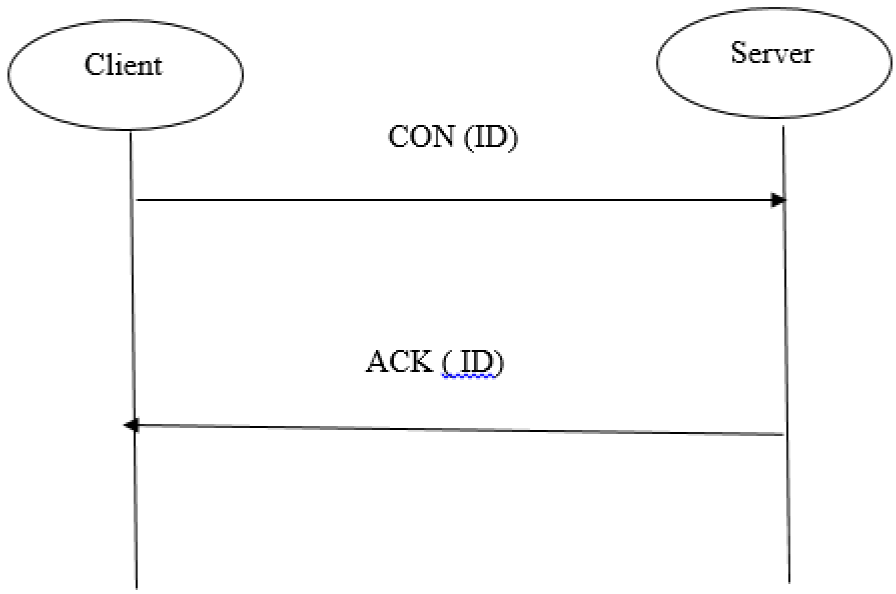

Fig 2.3 Message transferring in CON

Second category of message is Non Confirmable in which there is no ACK message. There is no information of message therefore it is an unreliable message.

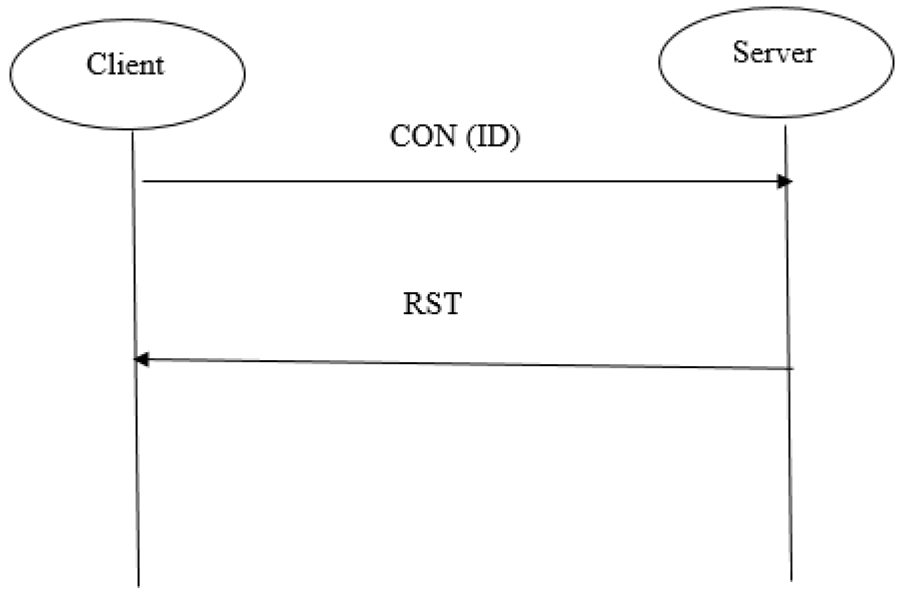

Fig 2.4 Message transferring in NON

2.2.1.2 Request/Response Layer:

In request/response layer both type of confirmable and non-confirmable messages are used to send request. Both type of scenarios can happen if sensor response to the message or not.

If server receives confirmable message it will send back the acknowledge message which will contain error code or response.

If server don't receive the request from the client it will send an empty acknowledgment message. When there is a response from client server will send confirmable message to client.

2.3 Mobile Internet Proxy version 6 (MIPv6)

To solve problems related to Mobile Internet Proxy version 4 (MIPv4), Internet-Engineering-TaskForce (IETF) proposed new mobility scheme which was termed as "MIPv6". For better mobility management as a comparison with MIPv4, MIPv6 provided it [7]. In Mobile IPv6 (MIPv6) it permits Mobile node (MN) to transfer in domain on MIPv6 lacking loss of connection and corruption. There is full need of HA and FA in Mobile IPv4 which is the reason of long communication [8][2].

Fig 3.1 demonstrates the tasks performed by Mobile Internet Proxy version 6 (MIPv6). Home Agent (HA) is local based so every data packet will transfer to Mobile Node (MN) with the use of common routing protocol.

Whenever the Mobile Node move outside with the extra address of MN which is connected by any foreign link from the home agent's local range. Home Agent (HA) receives binding updating information. Acknowledgment is sent back by Home Agent (HA) and also informed that which Mobile Node (MN) is accessed at that time by Care of Address (CoA). All communications will take place between Correspondence Node (CN) and Mobile Node (MN) without Home Agent (HA) when the connection is established in route optimization.

[9] [3]. For Real Time Applications, as MIPv6 has lot of benefits but it is not suitable. Because of Big data packet loss, long handover delay and more signalling cost. One more issue is that whenever Mobile Node moves from its position it will notify the Home Agent (HA) and also updates Care of Address (CoA). For secure communication if IPv6 is created this will cause the change in the size of header in sense of increment, which will dissatisfy the Audio/ Video call applications [10].

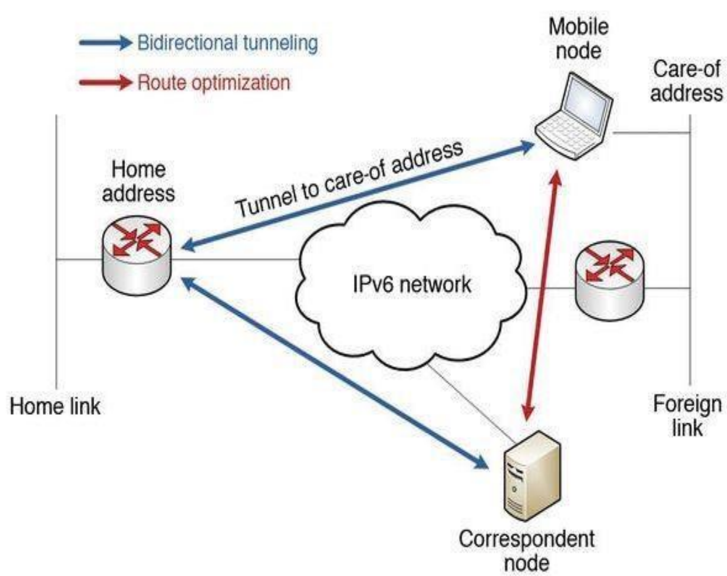

Figure 2.5 Architecture of MIPv6 [10]

Chapter 3

Literature Review

In 2010, Hyon-Young Choi and other authors, In order to minimize the handover, implemented PMIPv6 (Proxy Mobile IPv6) in ns-3 simulator. The simulation performed in IEEE 802.11 wireless network environment for testing the performance and operation of PMIPv6. They compared the implementation on Ns3 simulator with Ns2 simulator. The results showed that the implementation on Ns3 provided better results and short handover than Ns2 simulator [42]. In 2011, Heeyoung JUNG and other authors proposed mobility scheme for distributed mobility control which were based on PMIP to reduce the limitation of centralized approach. Mobility schemes were proposed. Signal driven PMIP (S-PMIP), Signal-driven Distributed PMIP (SD-PMIP) and Data-driven Distributed PMIP (DD-PMIP), By comparing all these three scheme they concluded that the better one is Signal-driven Distributed PMIP (SD-PMIP) and it provides the best performance then other schemes. Before transmission of data packet CN (Correspondence Node) of MAG (Mobile Access Gateway) perform binding query operation in data packet delivery [48].

In 2013, Ishtiaq Wahid and other authors proposed hash function scheme to reduce vertical handover. This model reduces the registering time and time of address resolution on network layer. This model it reduces the handover by using the features of HMIPv6 (Hierarchal MIPv6) and FMIPv6 (Fast MIPv6) [43]. In 2013, Ji In Kim and other authors proposed hash based distributed mobility scheme in Proxy Mobile IP (PMIP). Control functions for binding update and query operations are performed in this method which were based on hash and because of this data traffic is scattered onto Mobile Access Gateway (MAG). In this scheme Local Mobility Anchor (LMA) is distributed at every MAG. In this scheme Corresponding Node (CN) and Mobile Node (MN) are located in the similar domain of PMIP [16]. In 2016, Sang-Il Choi and other author proposed mobility management method which were established on PMIPv6 (Proxy Mobile IPv6) which were CoAP-DPMIP and CoAP-PMIP and for mobility management to minimize handover delay. They compared these schemes and find out that CoAP- DPMIP is better than CoAP-PMIP because CoAPDPMIP provided better performance in terms of delay in handover [26]. In 2014, Ishtiaq Waheed,Masood Ahmad, Nawsher Khan, Abrar Ullah proposed FHMIPv6 (Fast Handover Mechanism IPv6). This scheme with the help of hash algorithm combines Hierarchal mobile IPv6 and Fast handoff scheme. Registration process is done when MN (Mobile Node) is approaching the visiting network informs the HA (Home Agent) and MAP (Mobile Anchor Point). Hash algorithm generates the same CoA (Care of Address) for Mobile Node. Hash function generates same result after every time of same input. The proposed mobility scheme reduces delay and packet loss in the process of handoff [19]. In 2014, Seong-Mun Kim and other authors proposed the scheme in which they used the advantages of the architecture of Open Flow for the network of PMIPv6. This scheme separates the control panel and data. It removed the tunnel to forward the traffic [5].

In 2014, Ishtiaq Waheed and other authors proposed the model to reduce the handover delay. This model had the features of FMIPv6 and HMIPv6. Performance of both schemes varies in different scenarios. By combining two or more than two schemes we can get an improved scheme for vertical handover [48].

Chapter: 4

Base Research Implementation

All common wireless communications technology involves Iot PHY/MAC layers. IoT communication mainly work with TCP and UDP protocols because TCP/IP is the foundation for the internet. Most of IoT use UDP protocols. To improve the stability of UDP it combines with application layer. Application layer works with HTTP. But HTTP has computational complexity that's why IETF (Internet Engineering Task Force) has introduced new protocols and CoAP (Constrained Application Protocols) is one of them [27] [17].

4.1 Communication in CoAP

The Rest Model is used by the Constrained Application Protocol [44]. In figure 4.1 suppose that a client will send a CoN [Oxal5] Get / Easy on a server in case the client need to get a request from the server. So, after sending the CoAP authentication server it directs back the acknowledgment and the payload using the same communication id. Now if there is a packet loss, server receives a message from client to find out about the loss. The client received no response from the server due to packet loss so the client will use the timeout method. So later the client will repeat the same procedure and will send the message to the server again with the same message id. When the server receives the request, it will send the approval with the same message id and upload. In the appearance of a package loss, the client will use a backlog to reduce the time limit. Now suppose, client wants a feedback, the server has to do most of the processing. The server will send an empty acknowledgment with the similar communication id to client. When the server receives the results, it will send a separate acknowledgment to the customer with the same message id [10].

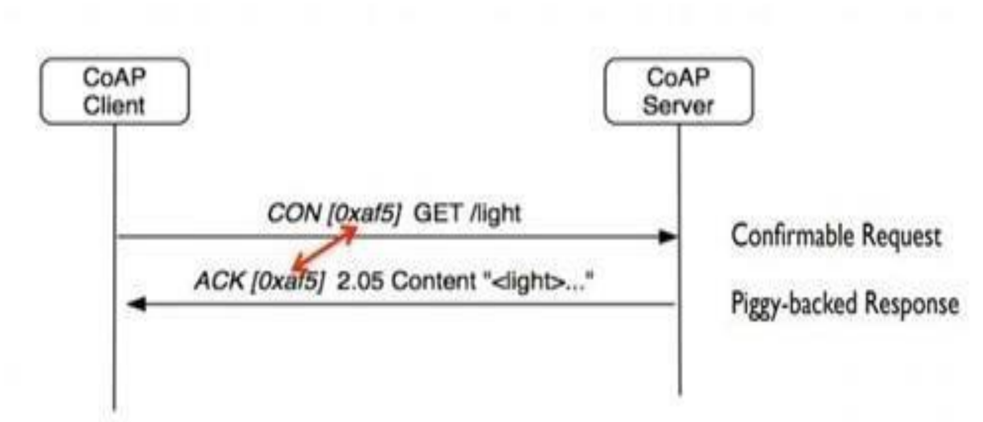

Figure4.1 CoAP Method [10]

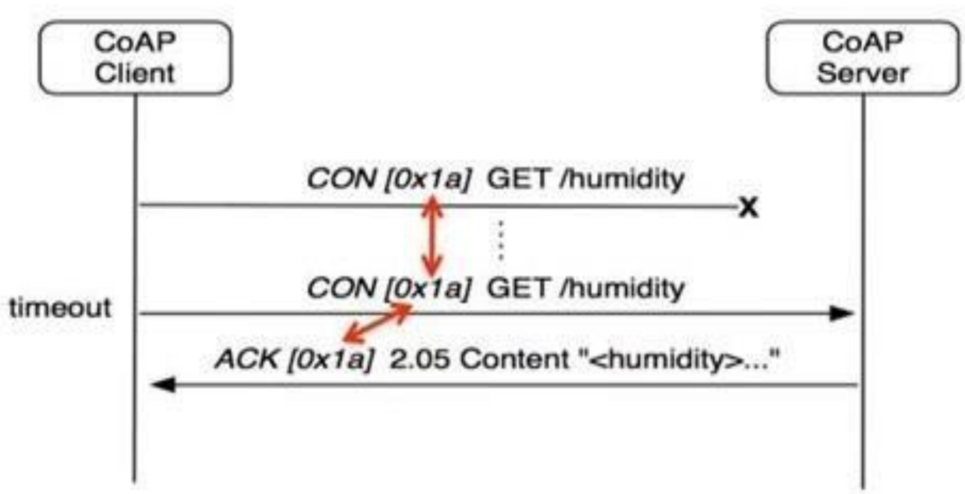

Figure 4.2 CoAP's Packet-Loss [10]

4.2 User Datagram Protocol (UDP)

In the Transmission control protocol (TCP) where server receives data from client, a message about packet authentication is sent by the server. TCP also makes a total amount of error checking. But in a user-defined user protocol the Protocol always sends a message to the recipient without knowing whether it has been accepted or not[28]. Example of UDP is video call [11] [18].

4.3 Existing Work

Existing work is a base of proposed work. So now have look on existing work.

4.3.1 Centralized CoAP

Constrained Application Protocol (CoAP) is used broadly. In Figure 4.3 it displays the process happened in Centralized CoAP.

1. By means of the Router Discovery sensor register resource list in Access Router (AR). It interacts with Router Advertising and Solicitation.

2. Whenever client sends data to sensor, they must perform Multicast based Service Discovery to obtain the sensor address of IPV6 Step (2 to 5).

3. When the IPV6 sensor address is received by client, the communication between sensor and client can be done (Step 6).

4. As there is a movement of sensor so there will be handover too. Centralised- CoAP do not maintain the handover and client is aware of it because client will receive an ICMP error message. (step 8,9)

5. When ICMP message is received by client, the service is inaccessible you know that a sensor service movement has occurred as a result of receiving this error (Step 8, 9)
6. Client will perform the process of Device Detection to find out the location of sensor.(Step10,11,12)

7. Now communication will start again between client and sensor [3] (Step 13, 14, 15)

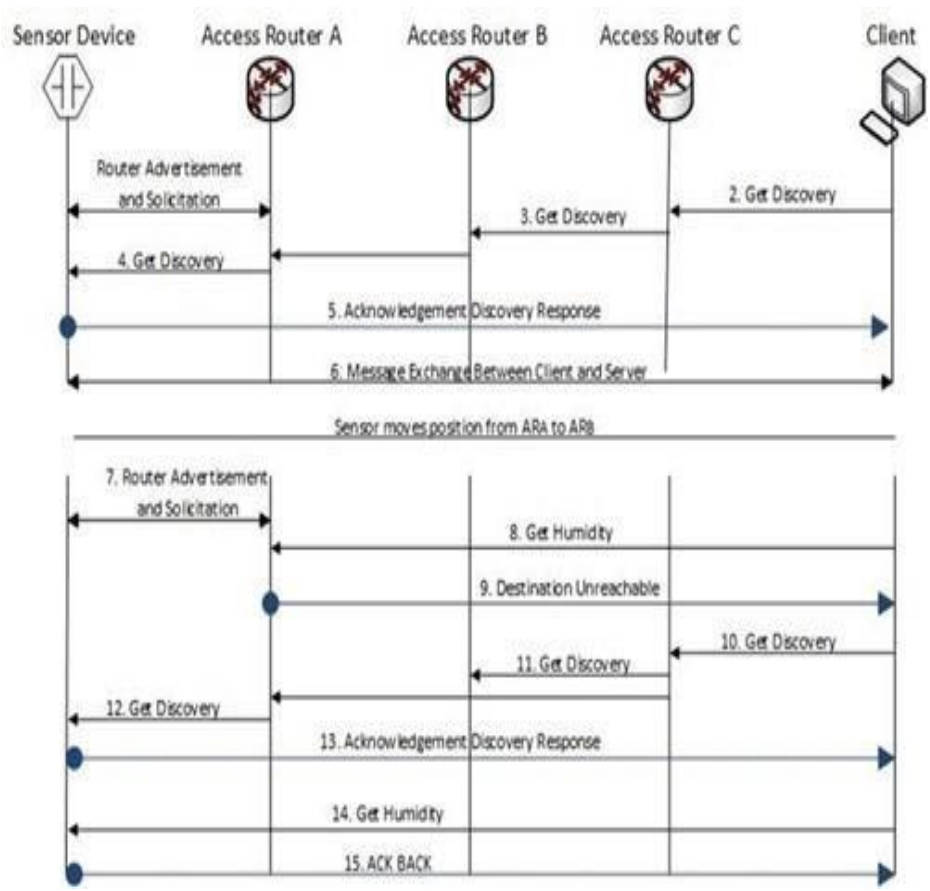

Figure 4.3 Centralized CoAP[3]

4.3.1.1Router Solicitation

To advertise host presence on network a message is send to any router from host.

4.3.1.2 Router Advertisement

When host is available for routing a type of message is received to host from router is Advertisement.

4.3.1.3 Pros and Cons

- In Centralized-CoAP communication can be done easily
- In Centralized-CoAP position of sensor will not change.
- If handover occurs then client will receive the Internet Control Message Protocol (ICMP) to find out the position of sensor.
- Every time client will perform device discovery procedure [46].

4.4 CoAP Proxy Mobile IPv6

PMIPv6 is based on the functionality of MIPv6. PMIPv6 uses the functionality of Home

Agent (HA) of MIPv6s[6][42].To address the limitations of CoAP. New mobility scheme "CoAP-PMIP" was proposed. In CoAP-PMIP the functionality of Access Router (AR) was added as Local Mobility Anchor (LMA).

When sensor is attached to the Mobile Access Gateway (MAG) then Local Mobility Anchor (LMA) will receive a Binding Update (BU) from the Mobile Access Gateway (MAG). Then information related to Mobile Access Gateway (MAG) will be stored in Local Mobility Anchor (LMA). In data transmission client will receive the information which includes the IPv6 address of sensor. In the case of handover the sensor will send Binding Update (BU) through new Mobile Access Gateway (MAG) to the Local Mobility Anchor (LMA). Then Local Mobility Anchor will get notify with the IPv6 address then it will send the data packet to the newly Mobile Access Gateway (MAG).

In CoAP PMIP procedures there were a sensor, client, MAG_A, MAG_B, MAG_C and LMA.

Whenever a sensor is attached to any network, Local Mobility Anchor (LMA) will receive Proxy Binding Update (PBU) message from MAG_A. Then, Local Mobility Anchor (LMA) will update its table and will respond MAG_A *with* Proxy Binding acknowledgement. For the delivery of data Local Mobility Anchor (LMA) will receive a query message from client through MAG_C to get the IPv6 address of sensor. Then Local Mobility Anchor (LMA) will find the data related to sensor from its table and client will receive the Binding Query ACK message from it. Now sensor and client can exchange information. In case of handover occurrence Proxy Binding Update (PBU) operation is performed by newly attached MAG with Local Mobility Anchor

(LMA). Then Local Mobility Anchor (LMA) will respond with the acknowledge message of Proxy Binding message again. Through Local Mobility Anchor (LMA) the client and sensor now can send and receive data with each other.

This approach was centralized because LMA was only responsible to handle the traffic. This is why CoAP-PMIP used the non-optimized path between LMA and MAG and sends the binding update (BU) and messages over the wired links between MAG and LMA. In CoAP-PMIP as wired link delay gets larger the total delay increases. [21] [4]

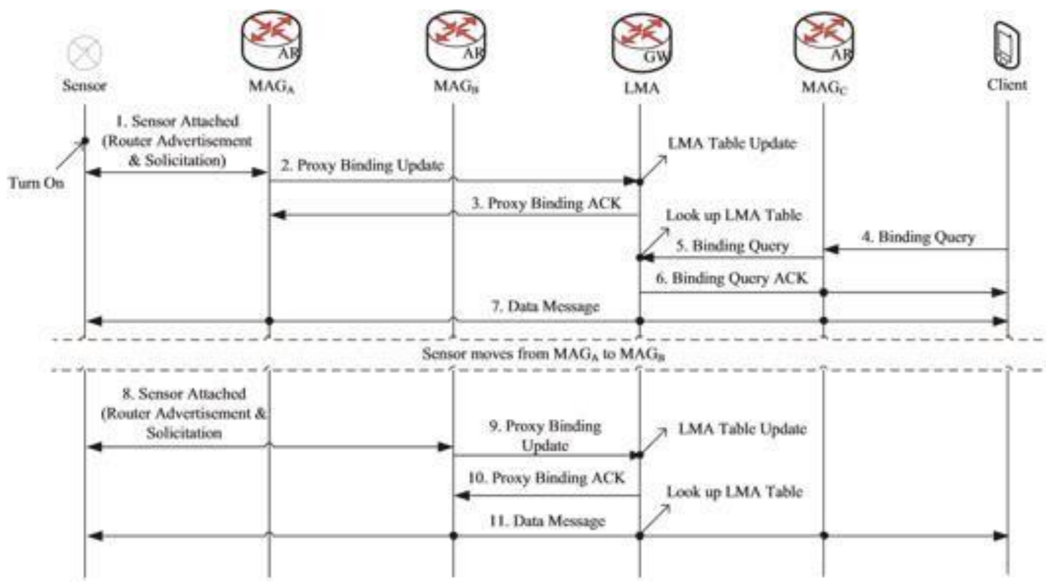

Figure 4.4 CoAP Proxy Mobile IPv6 [21]

4.4.1 Pros and Cons:

- CoAP-Pmip is better for small number of messages.
- It is a centralized approach due to there will be no movement of sensor.
- All messages are transmitted through Local Mobility Anchor (LMA) which causes handover delay.

Chapter 5

Proposed Work

5.1 CoAP-PMIP hash

As our proposed work is related to IoT, so in this hash distributed scheme sensor will send data to machine through different entities. In CoAP-PMIP hash Local Mobility Anchor (LMA) is distributed to each MAG present in the domain of CoAP PMIP. For traffic load balancing and fast route data planes and control planes are distributed to each MAG. Hash function will perform other operations like query operations and binding update.

In hashed based scheme when Mobile Node (MN) receives a message from Correspondence Node (CN). Then with the MAG, CN-MAG performs the binding query operation that maintains the Home Address (HoA) and Proxy-CoA binding information of a mobile node will be determined by using a hash function for a given HoA of mobile node. After that, Correspondence Node (CN) will send the messages over the route from start. The proposed method can improve handover and data communication output.

5.2 CoAP-PMIP hash communication Flow

1. Mobile Node (MN) will attach to Mobile Access Gateway of Mobile Node (MN-MAG).
2. By using Hash function, MN-MAG will determine the designated MN-MAG and then performs Binding Update (BU) operation with the Mobile Access Gateway (MAG).
3. Mobile Node (MN) receives data from Correspondence Node (CN).
4. By using Hash function, Corresponding Node Mobile Access Gateway (CN- MAG) will recognize the Mobile Access Gateway (MAG) that is responsible for Mobile Node And performs the Proxy Binding Query(PBQ) with the identified MAG.
5. Data Packets are forwarded to Mobile Node (MN).

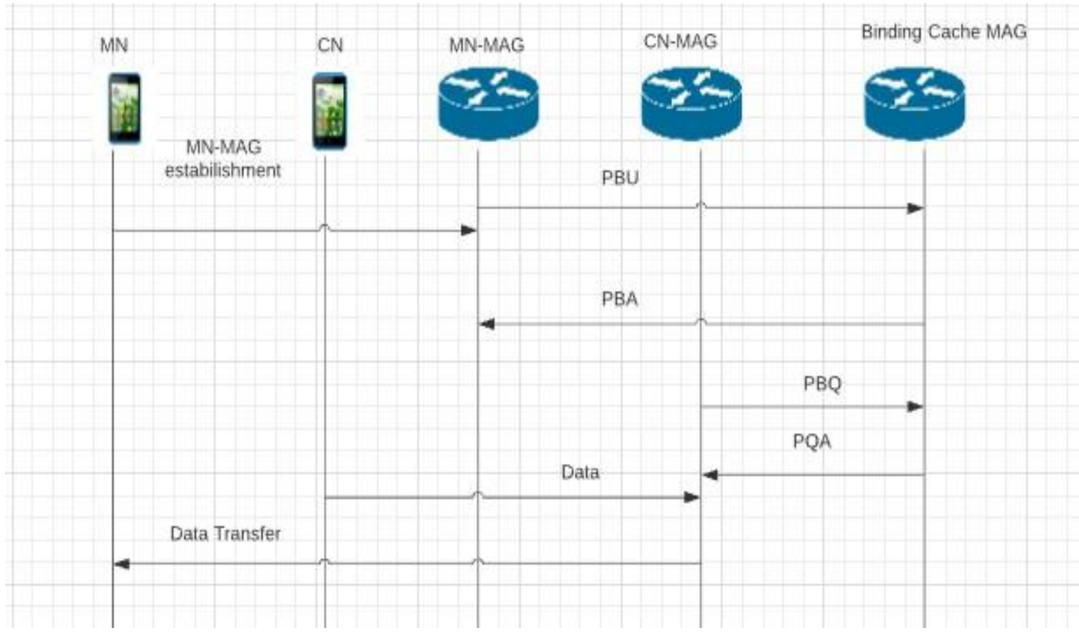

Figure 5.1 CoAP-PMIP-Hash

5.2.1 Proxy Binding Update (PBU):

It is a message about IP address for establishing binding between Mobile Node-MAG (MN-MAG) and Care of Address (CoA).

5.2.2 Proxy Binding Acknowledgment (PBA):

It is a reply of Proxy Binding Update which is send to Local Mobility Anchor (LMA).

5.2.3 Proxy Binding Query (PBQ):

This operation is used to find out the proxy CoA of Mobile Node (MN)

Chapter 6

Simulation and Results

6.1 Simulator:

We will use Ns-3 simulator. Ns3 simulator is organized with the set of modules. The core module of Ns-3 provides C++ language which makes programming easy.

Other modules present in Ns-3 simulator includes data types which relates to the manipulation of packets and headers. A Mobility Model item may be aggregated with a Node item to provide the node with the capacity to realize its own function [47].

6.2 Simulations

6.2.1 Simulation of CoAP-PMIP with Handover Delay

Once the handover occurs, sensor will start to communicate again

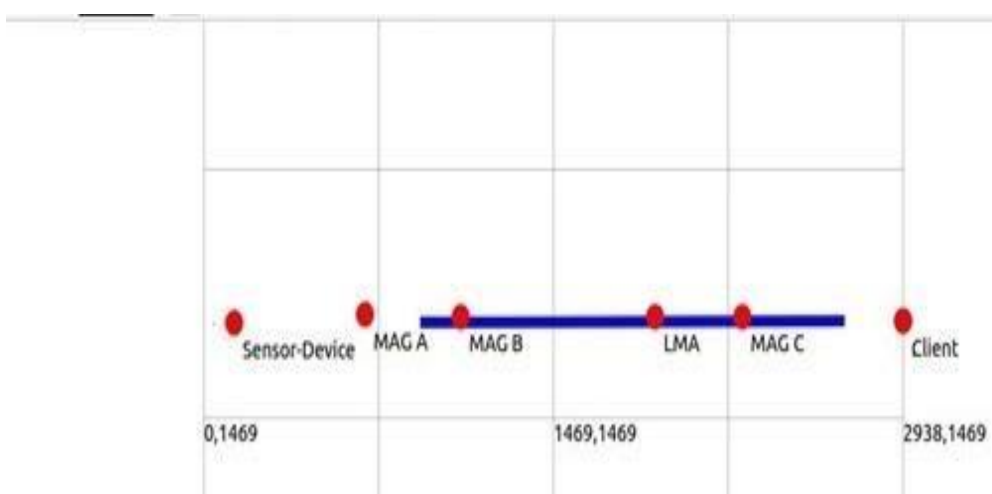

Figure 6.1 CoAP-PMIP Simulation

Figure 6.1 shows the communication between sensor device, MAG_A, MAG_B, LMA, MAG_C and client.

6.2.2 Simulation of CoAP-PMIP without Handover Delay

In figure 6.2 the communication starts from sensor and will pass through MAG_A, MAG_B, LMA, MAG_c to client.

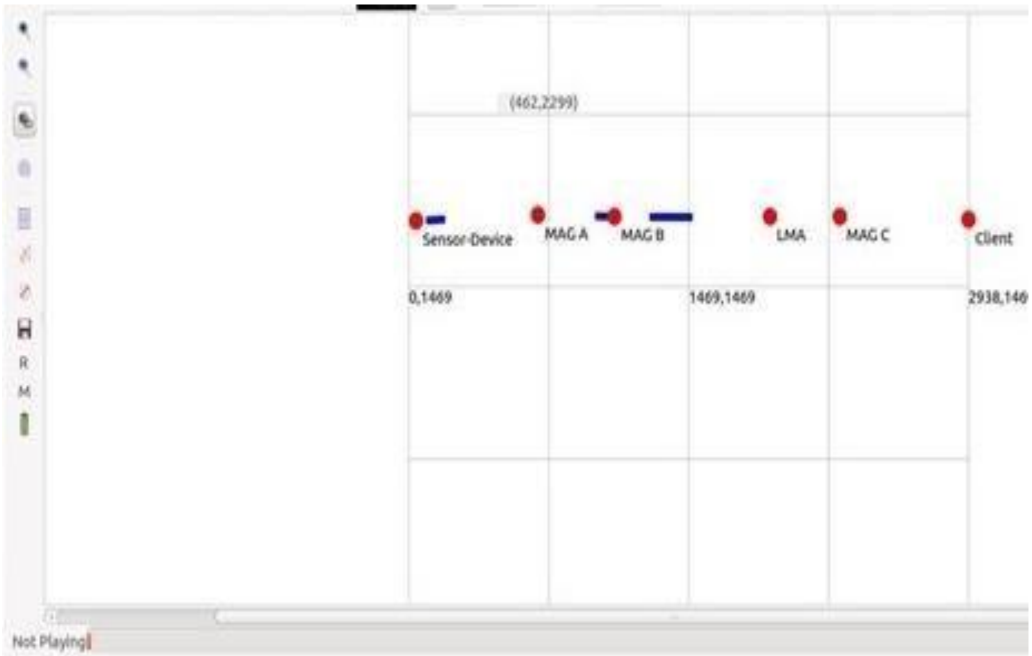

Figure 6.2 Simulation of CoAP-PMIP

6.3 Simulation of CoAP-PMIP-Hash without handover

In figure 8.1 MN will start sending messages to client

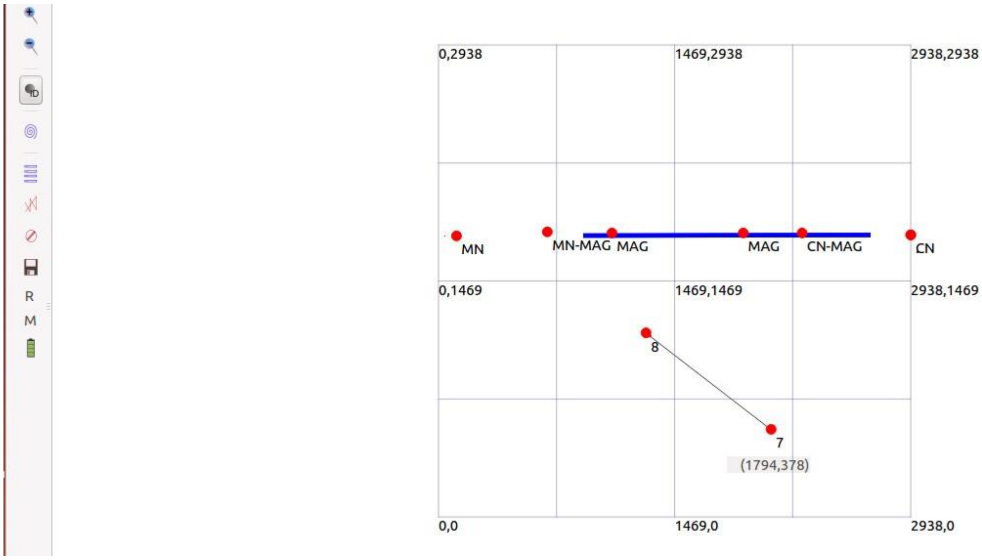

Figure 6.3 Simulation of CoAP-PMIP- Hash

6.3.1 Simulation of CoAP-PMIP hash with handover.

In figure 6.4 After the handover all devices will start communicating. MN will be able to send messages through MAG's present n the domain

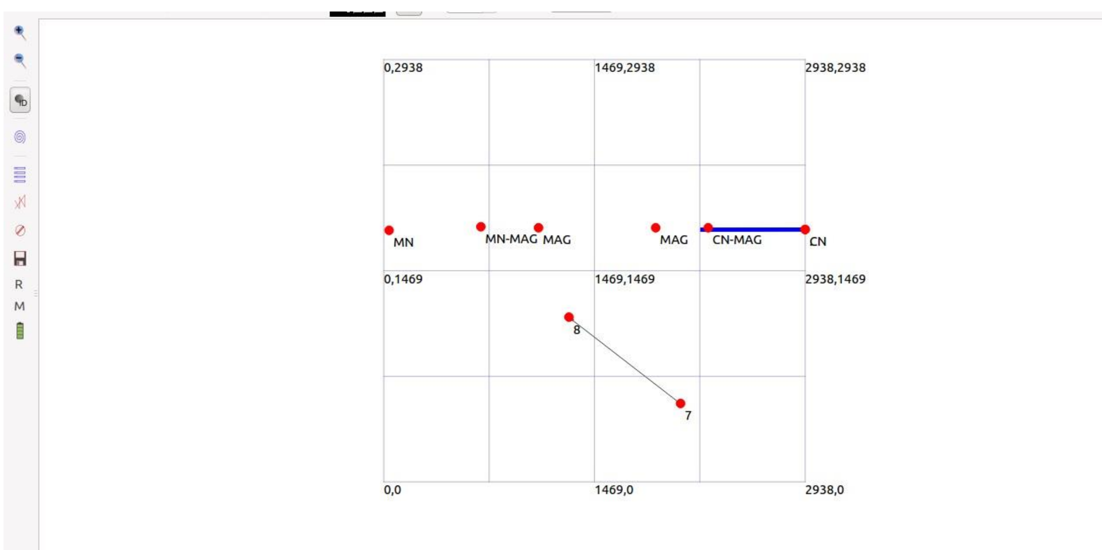

Figure 6.4 Simulation of CoAP-PMIP-Hash

6.4 Analysis of performance.

6.4.1 Parameters of simulation

Table 2 shows the simulation parameter.

Table 2 Simulation Parameters

Operating System	Ubuntu 14.04 LTS
Simulator	Ns-3.19
Animation Software	Netanim
Graph plotting and Data Tracing	Gnuplot and MS Excel
No. of messages sent by client	45
Data Tracing Software	Wireshark
Handover occurance	3.9
Link Delay	0.11ms

6.4.2 Throughput

Throughput is how much amount of data packets are send from source to destination at any time. Throughput of existing and proposed system are given. In the graph as it shows that the performance of throughput is better in CoAP-PMIP hash as compared to CoAP-PMIP. In CoAPPMIP hash the network consumption is less because of the distribution of the working of LMA on every MAG present in the domain.

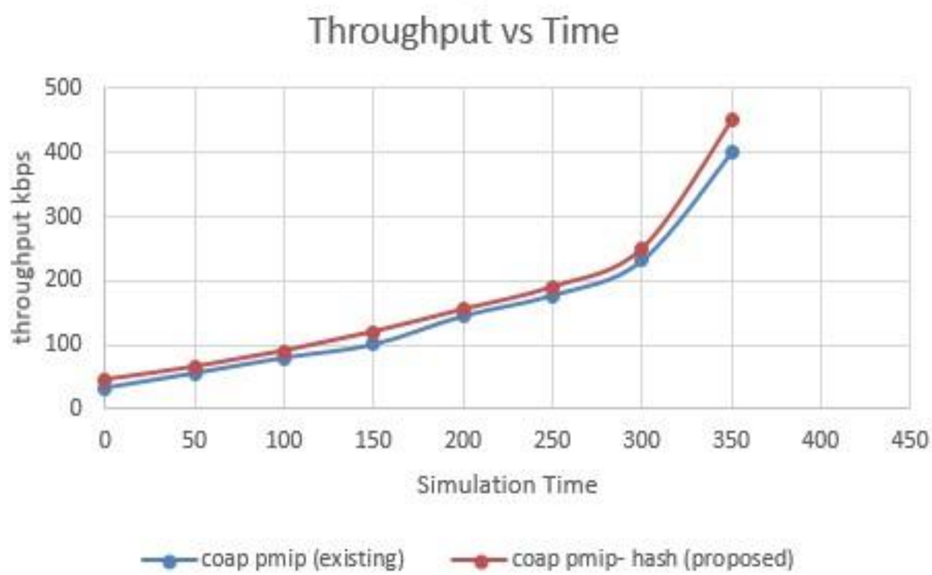

Figure 6.5 Time vs Throughput

In figure 6.5, the performance of throughput is better in CoAP PMIP-hash as compared to the CoAP-PMIP.

6.4.3 End to End Delay

In Figure 6.7 we can see that in the start there is no difference between CoAP-PMIP and CoAPPMIP hash. Because of the processing of communications is normal. When handover occurs at 2.1 secs the performance of CoAP-PMIP becomes poor because when mobility occurs the communication of sensor with MAG will be disconnected. So after the handover, client will be informed about the position of sensor has changed. To inform the client, the sensor will start device discovery procedure. But in CoAP-PMIP hash the communication time is decreased at 2.1 secs because of fast processing.

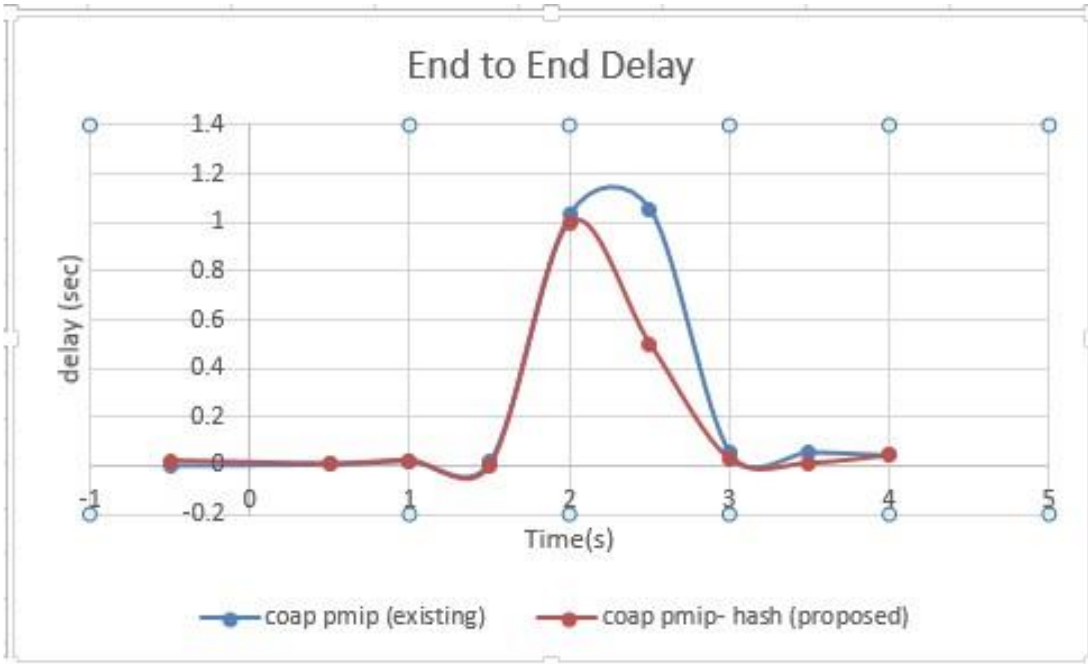

Figure 6.6 End to End Delay

6.4.4 Tracing of Data Packets

In figure 6.8 shows the tracing of data packets. This graphs shows the number of data packets send from the client to the sensor. Total number of data packets are 45. When handover occurs in CoAPPMIP the packet arrival time is 3.9 secs. In CoAP-PMIP hash, on the occurrence of handover the packet arrival time is 3.7. So as the comparison between CoAP-PMIP and CoAP-PMIP hash the packet arrival time of CoAP-PMIP hash is less then COAP-PMIP. So the performance of CoAPPMIP hash is better than CoAP-PMIP.

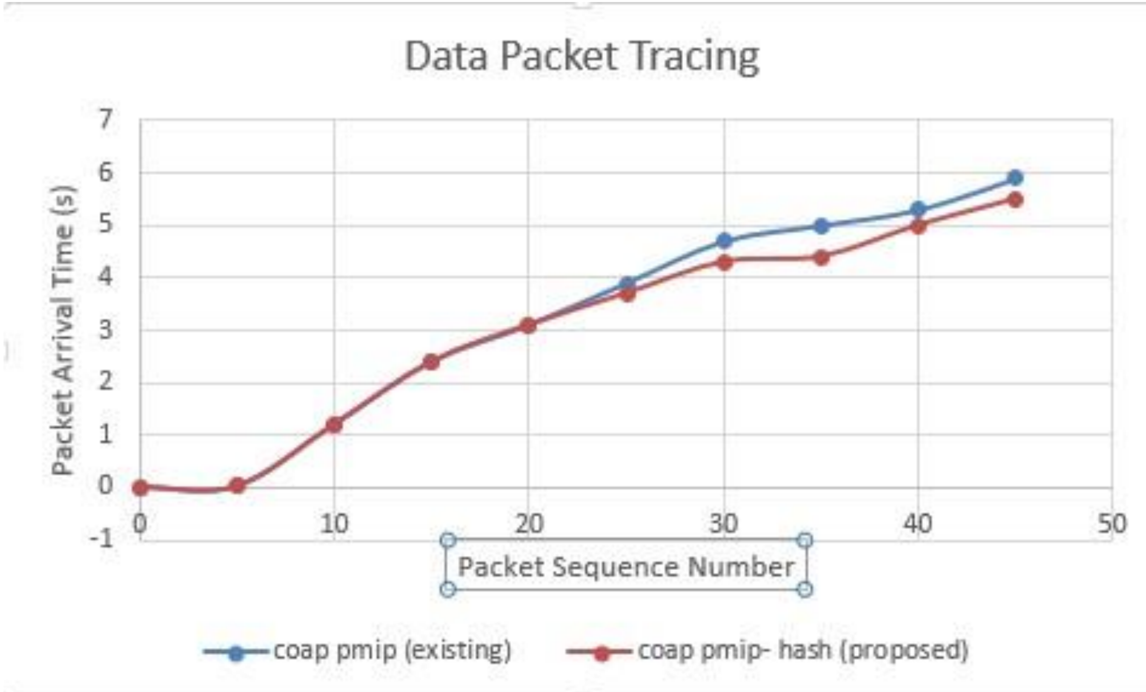

Figure 6.7 Data Packet Tracing

6.4.5 Signalling Cost

In figure 6.8

Signalling Cost and No. of Hops are shown. We can see the comparison between of hop count in CoAP-PMIP and CoAP-PMIP hash. As CoAP-PMIP hash is distributed so there is no Local Mobility Anchor (LMA) and in CoAP-PMIP data is transferred to Local Mobility Anchor (LMA) through Mobile Access Gateway (MAG). So hop count of Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA) is not affected in CoAP-PMIP hash. So CoAP-PMIP hash has better results than CoAP-PMIP.

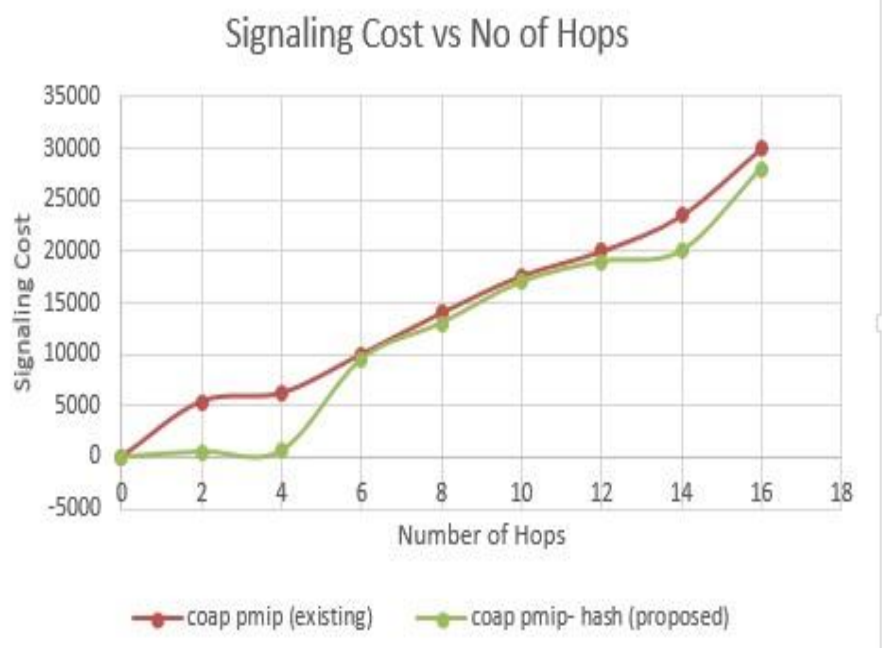

Figure 6.8 Signalling cost vs No of Hops

6.5 Conclusion and Future Work

The existing mobility scheme tends to induce large handover delay and signalling cost because of using centralized local mobility anchor (LMA) for mobility management and data delivery.

To address these problems, a hash-based proxy mobile IPv6 based constrained application protocol is proposed, named CoAP-PMIP-Hash. In the proposed scheme, the functions of Local Mobility Anchor (LMA) is distributed among each Mobile Access Gateway (MAG). The control functions for binding update and query operations are performed based on a hash function. From the simulation results, it is shown that the proposed scheme performs better than the existing scheme in terms of the end-to-end delay, throughput and signalling cost.

In the future, there should be more models introduced for controlling handover delay by which data transferring more be easy and data communication would be clear and easy.

References

[1] 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 .

[2] Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash, 'Internet of things: A survey on enabling technologies, protocols, and applications.' IEEE communications surveys & tutorials 17, no. 4 2015.

[3] Conti, Marco, and Silvia Giordano, 'Mobile ad hoc networking: milestones, challenges, and new research directions.' IEEE Communications Magazine 52, no. 1 2014.

[4] Giust, Fabio, Carlos J. Bernardos, and Antonio De La Oliva, 'Analytic evaluation and experimental validation of a network-based IPv6 distributed mobility management solution', IEEE Transactions on Mobile Computing 13, no. 11 2014.

[5] Kim, Seong-Mun, Hyon-Young Choi, Pill-Won Park, Sung-Gi Min, and Youn-Hee Han,'OpenFlowbased Proxy mobile IPv6 over software defined network (SDN).' In Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11t h, pp. 119-125. IEEE, 2014.

[6] Modares, Hero, Amirhosein Moravejosharieh, Jaime Lloret, and Rosli Bin Salleh, 'A survey on proxy mobile IPv6 handover.' IEEE Systems Journal 10, no. 1 2016.

[7] Montavont, Julien, Damien Roth, and Thomas Noël, 'Mobile ipv6 in internet of things: Analysis, experimentations and optimizations.' Ad Hoc Networks 14 2014.

[8] 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 2016.

[9] Asghar, Mohsen Hallaj, Atul Negi, and Nasibeh Mohammadzadeh. 'Principle application and vision in Internet of Things (IoT).' In Computing, Communication & Automation (ICCCA), 2015 International Conference on, pp. 427-431. IEEE, 2015.

[10] Pujar, Shamprasad M., and K. V. Satyanarayana. 'Internet of Things and libraries', Annals of Library and Information Studies (ALIS) 62, no. 3 2015.

[11] Petrov, Vitaly, Sviatoslav Edelev, Maria Komar, and Yevgeni Koucheryavy,'Towards the era of wireless keys: How the IoT can change authentication paradigm.' In Internet of Things (WF-IoT), 2014 IEEE World Forum on, pp. 51-56. IEEE, 2014.

[12] Dhar, Sourav Kumar, Suman Sankar Bhunia, and Nandini Mukherjee,'Interference aware Scheduling of Sensors in IoT enabled Health-care monitoring system.' In Emerging Applications of Information Technology (EAIT), 2014 Fourth International Conference of, pp. 152-157. IEEE, 2014.

[13] Lee, Jay, Behrad Bagheri, and Hung-An Kao, 'A cyber-physical systems architecture for industry 4.0based manufacturing systems.' Manufacturing Letters 3 2015

[14] 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.

[15] Singh, Meena, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar. "Secure mqtt for internet of things (iot),' In Communication Systems and Network Technologies (CSNT)' 2015 Fifth International Conference on, pp. 746-751. IEEE, 2015.

[16] 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 2015.

[17] Pignataro, Carlos Maria, Joseph Michael Clarke, Rajesh Kumar, Mohammed Baseer Khan, Mohamed Saad Mostafa, Sanjeev S. Ukhalkar, Michel Khouderchah, and Mark Allan Son-Bell,'Messaging and presence protocol as a configuration and management bus for embedded devices.' U.S. Patent 8,640,036, issued January 28, 2014.

[18] Ferris, James Michael. 'Migrating data among cloud-based storage networks via a data distribution service.' U.S. Patent 8,984,269, issued March 17, 2015.

[19] Beckmann, Kai, and Olga Dedi, 'sDDS: A portable data distribution service implementation for WSN and IoT platforms.' In Intelligent Solutions in Embedded Systems (WISES)', 2015 12th International Workshop on, pp. 115-120. IEEE, 2015.

[20] Pereira, Pablo Punal, Jens Eliasson, and Jerker Delsing,'An authentication and access control framework for CoAP-based Internet of Things.' In Industrial Electronics Society, IECON 2014-40th Annual Conference of the IEEE, pp. 5293-5299. IEEE, 2014.

[21] Montavont, Julien, Damien Roth, and Thomas Noël. 'Mobile ipv6 in internet of things: Analysis, experimentations and optimizations.' Ad Hoc Networks 14 2014.

[22] Sadiq, Ali Safa, Kamalrulnizam Abu Bakar, Kayhan Zrar Ghafoor, Jaime Lloret, and SeyedAli Mirjalili, 'A smart handover prediction system based on curve fitting model for Fast Mobile IPv6 in wireless networks.' International Journal of Communication Systems 27, no. 7 2014.

[23] Modares, Hero, Amirhosein Moravejosharieh, Jaime Lloret, and Rosli Bin Salleh, 'A survey on proxy mobile IPv6 handover.' IEEE Systems Journal 10, no. 1 2016.

[24] Chen, Yuh-Shyan, Chih-Shun Hsu, and Ching-Hsueh Cheng,'Network mobility protocol for vehicular ad hoc networks' International Journal of Communication Systems 27, no. 11 2014.

[25]

[26] Do, Truong-Xuan, and Younghan Kim,'EPD-NEMO: efficient PMIPv6-based distributed network mobility management.' Wireless Networks 21, no. 7 2015.

[27] Jelschen, Jan, C. A. Küpker, Andreas Winter, Alexander Sandau, B. Wagner vom Berg, and Jorge Marx Gómez,'Towards a Sustainable Software Architecture for the NEMo Mobility Platform.' 30th International Conference on Environmental Informatics Stability, Continuity, Innovation: Current trends and future perspectives based on, vol. 30.

[28] Chan, H., D. Liu, Pierrick Seite, H. Yokota, and J. Korhonen,'Requirements for distributed mobility management'. No. RFC 7333. 2014.

[29] Gani, Abdullah, Golam Mokatder Nayeem, Muhammad Shiraz, Mehdi Sookhak, Md Whaiduzzaman, and Suleman Khan. 'A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing.' Journal of Network and Computer Applications 43 2014.

[30] Khan, Abdul Waheed, Abdul Hanan Abdullah, Mohammad Hossein Anisi, and Javed Iqbal Bangash, 'A comprehensive study of data collection schemes using mobile sinks in wireless sensor networks.' Sensors 14, no. 2 2014.

[31] Wu, Miao, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du,'Research on the architecture of Internet of Things.' In 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5, pp. V5-484. IEEE, 2010.

[32] Tunca, Can, Sinan Isik, M. Yunus Donmez, and Cem Ersoy,'Distributed mobile sink routing for wireless sensor networks: A survey.'IEEE communications surveys & tutorials 16, no. 2 2014.

[33] Haseeb, Shariq, and Ahmad Faris Ismail,'Comparative performance analysis of mobile IPv6 protocols: Special reference to simultaneous bindings.' Journal of Computer Sciences 2, no. 2 2006.

[34] Salsano, Stefano, Andrea Polidoro, Chiara Mingardi, Saverio Niccolini, and Luca Veltri. "SIP-based mobility management in next generation networks." IEEE Wireless Communications 15, no. 2 2008.

[35] Shelby, Zach,'Embedded web services.' IEEE Wireless Communications 17, no. 6 2010.

[36] Rahman, Akbar, and Esko Dijk,'Group communication for the constrained application protocol (CoAP)'. RFC 7390, October, 2014

[37] Bormann, Carsten, and Zach Shelby,'Block-wise transfers in the constrained application protocol (coap).' Internet proposed standard RFC 7959 2016.

[38] Ludovici, Alessandro, Pol Moreno, and Anna Calveras,'Tinycoap: a novel constrained application protocol (coap) implementation for embedding restful web services in wireless sensor networks based on tinyos.' Journal of Sensor and Actuator Networks 2, no. 2 2013.

[39] Jimenez, Jaime, J. Lopez-Vega, Jouni Maenpaa, and Gonzalo Camarillo,'A constrained application protocol (coap) usage for resource location and discovery (reload).' RFC7650, IETF 9 2015.

[40] Castellani, A., Salvatore Loreto, Akbar Rahman, Thomas Fossati, and Esko Dijk,Guidelines for mapping implementations: http to the constrained application protocol (coap).' Internet Engineering Task Force (IETF): Fremont, CA, USA 2017.

[41] Bormann, C., S. Lemay, H. Tschofenig, K. Hartke, B. Silverajan, and B. Raymor,‘CoAP (constrained application protocol) over TCP, TLS, and WebSockets.’ Internet Requests for Comments, RFC Editor, RFC 8323 2018.

[42] Shelby, Z., K. Hartke, and C. Bormann. ‘The Constrained Application Protocol (CoAP). Internet Engineering Task Force (IETF)’ RFC-7252." 2014.

[43] Chang, C. E., F. Mohd-Yasin, and A. K. Mustapha,’An implementation of embedded restful web services.’ In 2009 Innovative Technologies in Intelligent Systems and Industrial Applications, pp. 45-50. IEEE, 2009.

[44] 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.

[45] Gohar, Moneeb, Sajid Anwar, Moazam Ali, Jin-Ghoo Choi, Hani Alquhayz, and Seok-Joo Koh,’Partial Bicasting with Buffering for Proxy Mobile IPV6 Mobility Management in CoAP-Based IoT Networks.’ Electronics 9, no. 4 2020.

[46] Jung, Heeyoung, Moneeb Gohar, Ji-In Kim, and Seok-Joo Koh,’Distributed mobility control in proxy mobile IPv6 networks.’ IEICE transactions on communications 94, no. 8 2011.

[47] Choi, Hyon-Young, Sung-Gi Min, Youn-Hee Han, Jungsoo Park, and Hyoungjun Kim, ‘Implementation and evaluation of proxy mobile IPv6 in NS-3 network simulator.’ In 2010 proceedings of the 5th international conference on ubiquitous information technologies and applications, pp. 1-6. IEEE, 2010.

[48] Wahid, Ishtiaq, Masood Ahmad, Nawsher Khan, and Abrar Ullah,’A Novel Approach with Hash to Reduce Vertical Handover Latency.’ J. Appl. Environ. Biol. Sci 4, no. 7S 2014.