大学院国際情報通信研究科

Master's Thesis
修　士　論　文

論　文　題　目

Mobility Management in Information Centric Networking

Student ID 学籍番号	5115FG01 - 4
Name 氏　　名	AMBULI Alloys Michael

Supervisor 指導教員	NAKAZATO Hidenori　　印

２０１7年01月30日

Mobility Management in Information Centric Networking

A Thesis Submitted to the Department of Computer Science and Communications Engineering,
the Graduate School of Fundamental Science and Engineering
of
Waseda University
in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering

January 30th, 2017

By

AMBULI Alloys Michael
5115FG01-4
Of
NAKAZATO Laboratory
Professor NAKAZATO Hidenori

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my academic advisor Prof. NAKAZATO for his knowledge, motivation, patience and the invaluable support he offered me throughout my period of study. It is true that, his guidance and at times difficult questions always served to widen my horizon and enhance the authenticity of my ideas.

My sincere thanks also goes to Japan International Cooperation Agency (JICA) and the government of Kenya for providing me an opportunity to join the ABE Initiative program and study for Master Degree at Waseda University. Without their precious support it would be impossible for me to conduct this research. I also thank my laboratory mates for the stimulating discussions, for the sleepless nights we worked together to beat deadlines, and for all the fun we had in the last two and a half years. It is from them that I learnt the spirit of team work and endurance.

Finally, I must express my very profound gratitude to my family for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without their indulgence.

ABSTRACT

Information Centric Networking (ICN) is a new paradigm in computer networking that uses named data as its main abstraction. It shifts from TCP/IP architecture’s point to point communication model to content centric dissemination. All content is identified, addressed and retrieved by name instead of physical location. The change has been necessitated by the fact that the main role of the internet has evolved over time from the initial function of communication between hosts to data sharing and retrieval.

Mobility management is one of the key challenges to seamless access of network resources in ICN wireless networks. ICN receiver driven nature supports consumer mobility in that, after handover, mobile consumers are required to retransmit interests for lost data packets. However, content producer mobility occasions challenges such as frequent routing tables updates which puts unnecessary strain on network resources and could result in long service disruption.

In this thesis, we explain how Content producer mobility can be handled by use of resolvers at each ICN node and offer a simple technique for handling producer mobility in Information Centric Networks without putting unnecessary strain on network resources. We propose introduction of a new data structure; Binding Information Table (BIT) at each ICN node to record the location information of all migrated mobile producers and their foreign Access Point (AP_F) prefixes. This is to ensure that all interests for migrated data can be redirected accordingly to the current attachment points of the mobile producers.

We experimented our solution on AT&T network topology which is a real ISP topology that is part of the Rocketfuel project. Results from our simulation scenarios show that our algorithm is more efficient and effective in handling data packet loss, overall latency and handover delay.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS/ ACRONYMS

ICN	Information Centric Networking
NDN	Named Data Networking
TCP/IP	Transmission Control Protocol/ Internet Protocol
CCN	Content Centric Networking
AP	Access Point
ISP	Internet Service Provider
QoS	Quality of Service
CS	Content Store
PIT	Pending Interest Table
BIT	Binding Information Table
FIB	Forwarding information Base
NAT	Network Address Translator
OSPF	Open Shortest Path First
BGP	Border Gateway Protocol
AP_F	Foreign Access Point
AP_H	Home Access Point
AP_N	Neighboring Access Point
MP	Mobile Producer
MC	Mobile Consumer
DoS	Denial of Service

Chapter 1
INTRODUCTION

1.1. Introduction to ICN

Information Centric Networking is a new paradigm in computer networking that uses named data as the main abstraction [1]. It shifts from TCP/IP architecture's point to point communication model to content centric dissemination. All content is identified, addressed and retrieved by name instead of physical location. The change has been necessitated by the fact that the main role of the internet has evolved over time from the initial function of communication between hosts to data sharing and retrieval.

ICN has the advantage that it minimizes upstream bandwidth demand since requests for a given content can be aggregated and sent towards potential sources. Also, in-network caching avails multiple sources for the same data hence a request can be serviced locally without having to be sent to the server which has the potential of reducing downstream latency. ICN can utilize multiple paths freely because it has built in loop prevention in the forwarding process unlike TCP/IP which uses a single best next hop or limits its forwarding to multiple equal cost paths in order to avoid forwarding loops [18]. Whereas TCP/IP leaves the responsibility of security to the endpoints, ICN secures the data itself by requiring content producer to cryptographically sign every data packet. This allows a consumer's trust in data, and checks whether a public key owner is an acceptable publisher for a specific content. Embodying security in content and not hosts, avoids many of the host-based vulnerabilities that plague IP networking [1].

In this system, Content receivers request data via interest packets. These requests are responded to by content producers which send data packets with the requested names to the receiver following a symmetric reverse path of the interest packet. Proposed hierarchical names are assumed to correlate with underlying network topology and can offer performance gains through aggregation [1, 6]. However, names that correlate with underlying network topology may pose challenges if content has high mobility.

ICN inherently supports receiver mobility where lost data packets can be recovered by interest retransmission. However, content source mobility brings challenges such as frequent routing tables update and long service disruption [3]. Standard ICN requires name operations to handle producer mobility which is expensive in a network. The proposed algorithm makes data packets stored near the old location available before the routing table is updated so that data packets re-requested after handover are not delivered from a remotely located content source. This thesis proposes how producer mobility can be handled by use of resolvers at each ICN node and attempts to offer a simple way of handling mobility in ICN without putting unnecessary strain on network resources.

Due to the complex nature of the internet, a real ISP topology has been used for simulation purposes to test the proposed algorithm. Results from simulation scenarios show that our algorithm is more efficient and effective in handling data packet loss, overall latency and handover delay. Seamless handover guarantees a high quality of service (QoS) even when mobile nodes transit from one point of attachment to the other. This result could be deployed in continuous video delivery and streaming to wireless mobile devices moving at high speeds.

1.2. Thesis Organization

Chapter 2 gives an overview of basic Named Data Networking (NDN) data structures, packet forwarding operation and challenges in NDN. In chapter 3, we look at mobility management in ICN and related work. Our proposed mobility management scheme is presented in chapter 4, results and discussions in chapter 5 while chapter 6 summarizes our thesis and shows our direction for future research.

Chapter 2

NAMED DATA NETWORKING

2.1. NDN Overview

NDN is an acronym of Named Data Networking and it is a prototype of information centric networking [9]. NDN changes the semantics of network service from delivering packets to a given destination address to fetching data identified by a given name. It however keeps the same hourglass-shaped architecture which makes original internet design elegant and powerful. NDN differs from IP in terms of strategy and security which are shown as new layers in its protocol stack. The former makes dynamic optimization choices needed to best exploit multiple connectivities under changing conditions while the later guarantees that NDN secures content itself, rather than the connections over which the content is sent and received. A comparison between NDN and IP protocol stacks is depicted in Figure 1 below:

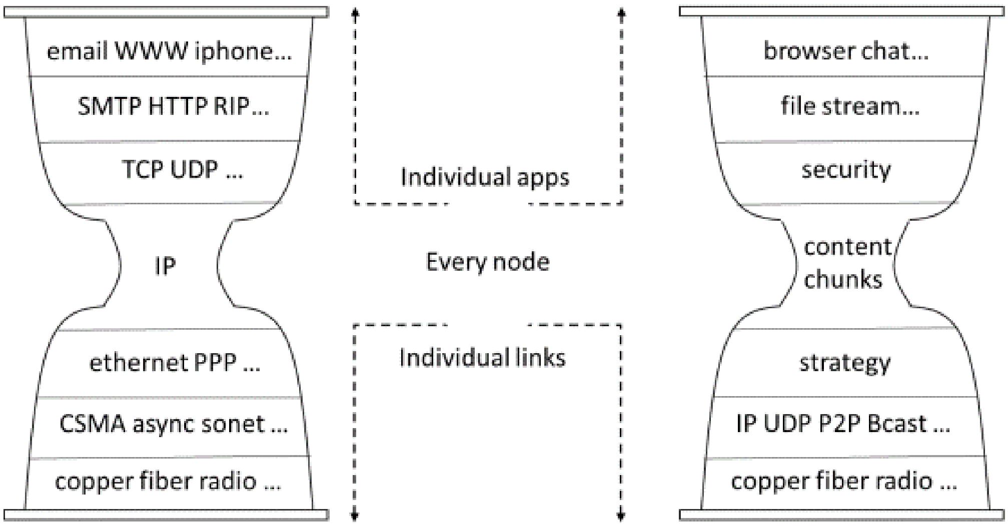

Figure 1 NDN and IP protocol stacks [10]

The current usage of the internet that involves sharing of high volume content is not compatible with current internet architecture. This is because the internet was designed at the time when the major interest was to facilitate resource sharing- remotely using scarce and expensive devices like card readers or high speed tape drives or even supercomputers. The communication model that resulted was a conversation between two machines, one wishing to use the resource and one providing access to it [1]. TCP/IP is the current internet protocol and it facilitates host-to-host communication. In a TCP/IP network, if we want to access data, first, we have to connect to the host where our required data is located. After connecting to the host, we can retrieve the data contents. It is not a scalable solution for high volume network traffic especially for the case where a single popular content is concurrently accessed by millions of users.

NDN architecture was designed to evolve the internet to its current usage requirement of content distribution while preserving the design options that make TCP/IP simple, robust and scalable [1]. In this design, data is retrieved without caring where it is located on the network. The architecture includes functionality designed to be conducive to user as the network evolves, such as multipath forwarding and in network storage [10]. The strategy layer makes dynamic optimization choices needed to best exploit multiple connectivity under changing conditions while the security layer ensures that NDN secures content itself and not the connections over which the content is sent. This saves NDN from the many host-based vulnerabilities that beset IP networking [1].

2.1.1 Interest and Data Packets

Communication in NDN is driven by data consumers, through the exchange of two types of packets; Interest and Data, see Figure 2.

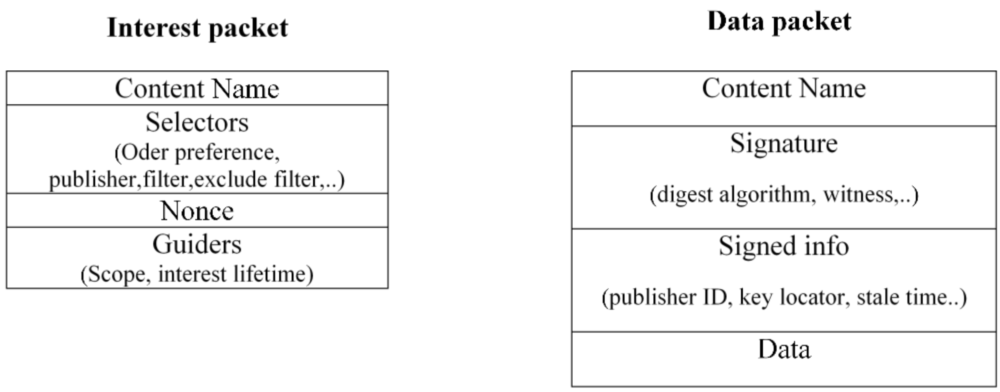

Figure 2 NDN packet types

Interest packet is used by the consumer for requesting a given piece of data by name. The consumer puts the name of the desired piece of data into an *Interest* packet and sends it upstream. Interest packet carries a name as a unique identifier for identifying the requested data. It is defined according to the hierarchical naming structure. Another important parameter in interest name is the *"nonce"* which is a random number and it is used to prevent looping of interests.

Data satisfies an interest if the content name in the interest packet is a prefix of the content name in the data packet. Once the interest reaches a node that has the requested data, the node will return a data packet that contains both the name and the content, together with a signature by the producer’s key which binds the two. One interest packet is satisfied by one data packet containing the same name.

2.1.2 Data Structures and Basic Operation

The basic operation of a NDN node is very similar to an IP node in that, a packet arrives on a face, a longest match lookup is done on its name and then an action is performed based on the result of that lookup. Each router maintains three data structures:

- Content store (CS) - which is a buffer to cache data packets for maximizing content delivery performance by delivering it to future consumers. It is a very prominent feature of NDN relative to existing IP network which forgets a packet after forwarding it.

- Pending Interest Table (PIT) - which stores all the interests that a router has forwarded but not satisfied yet. Each PIT entry records the data name carried in the internet, together with its incoming and outgoing interface(s). The entries in PIT are used by data packet to retrace its return path.
- Forwarding Information Base (FIB) – which keeps the name prefix along with next hop information and related metrics. It is used to forward interest packets towards potential source (s) of matching data. It allows for a list of outgoing faces rather than a single one and query them all in parallel.

The operation of NDN with its three data structures is shown in Figure 3 below.

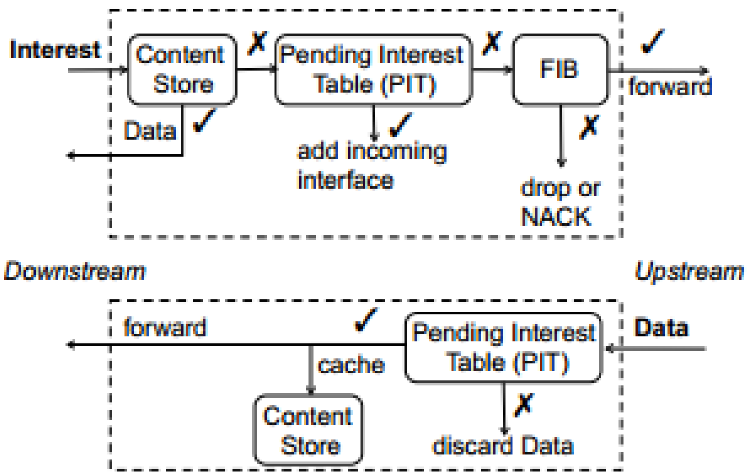

Figure 3 NDN basic operation [1]

Packet forwarding operation in NDN is as follows:

a. A consumer transmits an interest packet for requesting a given data item for example
(/Waseda.jp/nakazatolab/ccn.pdf/_ver2/_s3).

A NDN router receives the interest packet and checks its CS for matching data with the requested name. If the requested content is found in CSs, the router responds with a data packet. If it is not found in CS, the NDN router checks its PIT table.

b. If incoming request matches the content name in the PIT, the interest is suppressed and incoming face is added to the PIT entry. If incoming request is not found in PIT, incoming face is listed to the PIT entry and then proceed it to FIB.
c. If the NDN router finds a matched prefix in its FIB, the interest is forwarded to next hop using the face in the matched entry in the FIB.
d. If matching data is found from anywhere in the network, data packets are delivered according to the entry in PIT and data packets are cached in the CS for future use. Using PIT entry information, data packets can be delivered through the same path in reversed direction of interest packet.

2.2. Transport Layer in NDN

NDN architecture does not have a separate transport layer but instead moves the transport protocols (demultiplexing, reliable delivery and congestion control) in to applications, supporting libraries and the strategy module of the forwarding plane. [9] When interest or data packets are lost or damaged on the way, NDN provides a reliable and resilient delivery through retransmissions. The application that originates the interests (consumer) is responsible for re-expressing unsatisfied interests if it still wants the data. Interest packets contains a random once value so that duplicates received over different paths may be discarded. [1] NDN is created to work over the highly dynamic environment and network caching. The packet delivery system in NDN is best effort and no guarantee for packet loss. Moreover, since data are the central focus of the NDN communication, it is required more dedicated scheme to identify it. There are two portions in NDN packet sequencing, firstly how naming structure is organized and secondly, how to locate the specific segment of an object. Data name structure is organized as the human readable, hierarchical naming in [1] and we could simplify as in Figure 4.

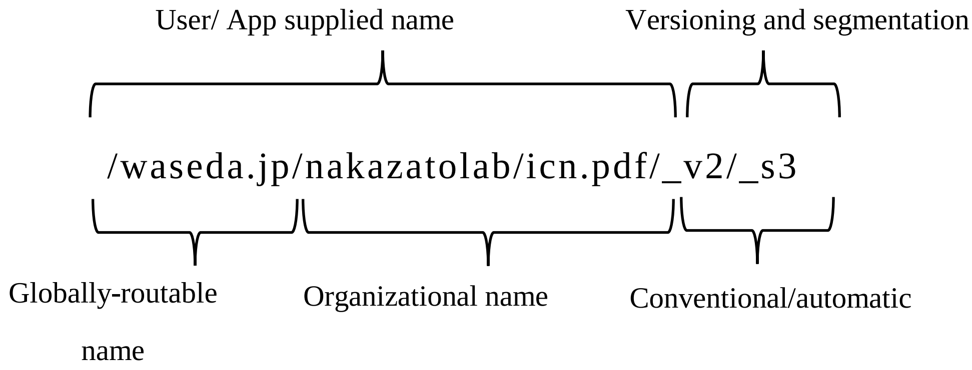

Figure 4 Readable data name

This hierarchical structure allows applications to represent the context and relationships of data elements. For example, segment 3 of version 2 of a waseda nakazatolab document might be named Waseda.jp/nakazatolab/icn.pdf/_v2/_s3. It also allows name aggregation, e.g., /waseda could correspond to an autonomous system originating the document. Flat names can be accommodated as a special case, and are likely useful in local environments, however hierarchical namespaces are essential both in scaling the routing system and in providing necessary context for the data [9]. A hierarchical name tree traversal is shown in figure 5 below.

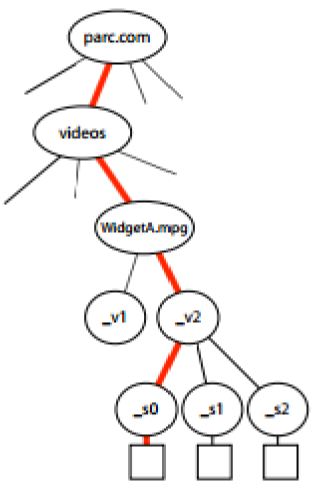

Figure 5 Name tree traversal [1]

2.3 Packet Routing and Forwarding in NDN

Routing and forwarding is achieved in NDN based on names. This eliminates the three problems caused by addresses in IP architecture example, address space exhaustion, NAT traversal and address management. There is no address exhaustion problem since the namespace is unbounded. There is no NAT traversal problem since NDN does away with addresses, public or private and address assignment and management is no longer required in local networks [9]. Any routing scheme that works well for IP should also work well for NDN because NDN forwarding model is a strict superset of the IP model with fewer restrictions (no restriction on multisource, multi-destination to avoid looping) and the same semantics relevant to routing (hierarchical name aggregation with longest match lookup) [1]. NDN provides a robust information security model that has the ability to make the routing infrastructure protection almost automatic.

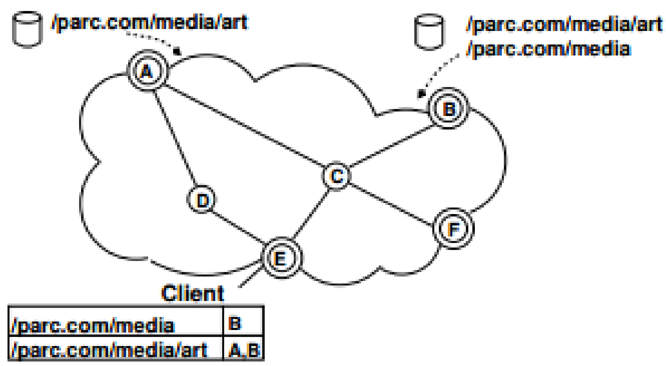

Figure 6 Routing Interest to a domain media content [1]

NDN can use conventional routing algorithms such as link state and distance vector. Instead of announcing IP prefixes, an NDN router announces name prefixes that cover the data the router is willing to serve. The routing protocol propagates these announcements across the network, informing each router's construction of its own FIB. Conventional routing protocols, such as OSPF and BGP, can be adapted to route on name prefixes by treating names as a sequence of opaque components and doing component-wise longest prefix match of a name in an interest packet against the FIB table [9].

2.4 Data Centric Security

TCP/IP leaves the responsibility of security to the end points. On the other hand, NDN is built on the notion of content based security. It secures data itself by requiring data producers to cryptographically sign every data packet [1]. All content is authenticated with digital signatures and private content is protected with encryption which is a critical enabler for NDN dynamic content caching capabilities. If you are to retrieve content from closest available copy you must be able to validate the content you get.

NDN data is publicly authenticated –per packet signatures are standard public key signatures, and anyone, not just the end points of a communication stream, can verify that a name-content binding was signed by a particular key [1]. NDN content routers may choose to verify all, some or none of the data they handle, as their resources allow. Requiring signatures on network routing and control messages (like any other NDN data) provides a solid foundation for securing routing protocols against spoofing and tampering. NDN's use of multipath forwarding, together with the adaptive forwarding strategy module, mitigates prefix hijacking because routers can detect anomalies caused by hijacks and retrieve data through alternate paths [11]. Since NDN packets reference content rather than devices, it is trickier to maliciously target a particular device, although mitigation mechanisms will be needed against other NDN-specific attacks, e.g., interest flooding DoS [12].

2.5 Challenges in NDN

NDN is a new network architecture that is meant to either co-exist with the current protocols or replace them altogether. It is therefore imperative that it demonstrates its capability on a global scale network such as the internet to be sure that it outperforms existing protocols. In this regard we still have many challenges that need to be fixed before it is deployed. Some of the challenges are described below:

Naming

NDN uses named data objects as its main abstraction. It is therefore of much importance that naming convention complies with existing standards and is hierarchical for better performance [13].

Caching

NDN performance is greatly enhanced courtesy of its in network caching ability. Caching management and replacement in terms of real-time traffic, dynamic data, capacity and security needs to be improved and is still of research interest.

Routing

Contents are divided into chunks and names given to them in NDN routing. There is no limitation for namespace length. So the problem is how to maintain the routing table size and how to update the routing information for huge amount of data on a global scale network [13].

Security

NDN has built-in content-based security and data packet has digital signature assigned by PKI (Public Key Infrastructure). The effective security key management and user trust management needs a keen attention for a better solution [13].

Mobility management

ICN receiver driven nature supports consumer mobility in that, after handover, the consumer simply retransmits interests for lost data packets. However, content producer mobility possess some challenges. Content Stores (CS) are not aware of domain change of content producer which would require reconstruction of entire routing information in order to solve this. If renaming is considered, it gives up naming persistence hence too many service access failures. [8].

Chapter 3

MOBILITY MANAGEMENT IN INFORMATION CENTRIC NETWORKING

3.1. Mobility management Concept

Mobility management is one of the key challenges to seamless access of network resources in wireless networks today. It is the main technology used to support mobile devices receive uninterrupted services while simultaneously roaming freely from one network domain to the other. A mobile service should be adaptive to different transmission links, devices and different network contexts.

Mobility models can be divided into three main classes namely: nomadic, cellular and pervasive mobility model [7]. Their differences are depicted in Figure 7 below

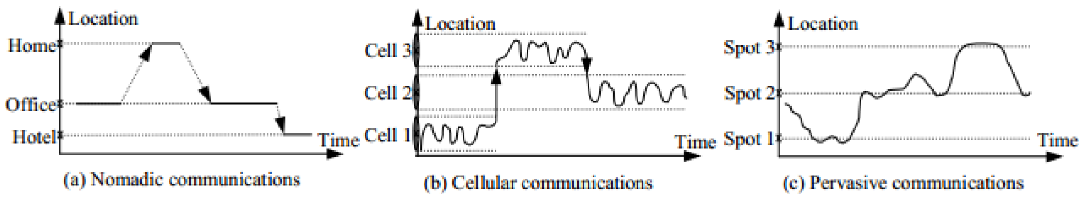

Figure 7 Classes of mobility models

We deal with cellular model in which wireless network takes a cellular structure with each cell having some radius of service. In this case continuous connectivity should be provided when a served mobile node is on transit from one cell to the next either neighboring or overlapping to guarantee a fair quality of service. Proper mobility management can effectively be achieved through two processes:

(i) Location management to locate roaming terminals, track their movement and update their location information in order to deliver interest packets and

(ii) Handoff management in order to maintain connections with terminals moving into new areas.

3.1.1 Location management

This concerns with locating mobile nodes to deliver interest packets despite the nodes having migrated from one access point to the next. The essence of location management is constituted by the mechanisms for mapping the name of a mobile node to its address [7]. This process involves location registration/update which is the procedure through which a node informs the network and other nodes of its new location through special messages. Location information is usually stored in some database in the network.

Location paging/searching is another procedure that is used to find the exact locality of a mobile device that packets need to be delivered to.

Areas that are still open as far as location management is concerned include:

- Addressing- this refers to how to represent and assign address information to mobile nodes. A global addressing scheme is needed to locate roaming nodes since the future of mobile communications will be based on internetworking and interoperability of heterogeneous networks.
- Location update time- refers to a situation when a mobile node should update its location information in corresponding databases. Location update schemes can be either static where update is triggered by some fixed condition eg time period or network topology change or dynamic which is more personalized and adaptive and based on some situations such as counter, distance, timer or even predicted factors
- Database structure-refers to how to organize storage and distribution of location information of mobile nodes. The structure can either be centralized, distributed, or hybrid.
- Paging scheme- refers to how to ascertain the exact location of a mobile node within a limited period of time.

3.1.2 Handoff management

It involves identifying a new access point and the allocation of data and control signal channels associated with the new access point to a mobile node. Handoff must be performed successfully, as infrequent as possible and must be imperceptible to the user.

Signal strength and bandwidth insufficiency triggers the handoff process. To achieve performance requirement in terms of per packet QoS, two techniques are used:

(i) Movement prediction and detection and

(ii) Buffering of interests that arrive at the old attachment point during handover process.

Connection re-establishment must take place before breaking the previous link ie make before break in order to minimize packet loss rate and latency. The main task of this operation relates to the discovery and assignment of a new connection resource. Packet routing to change the delivering route of the succeeding data to the new connection path after the new connection has been successfully established is required.

Wireless networks vary in both service capabilities and technological aspects therefore no single wireless network technology can fulfil the different requirements on latency, coverage, data rate and cost. Some packet level QoS parameters are more important to real-time multimedia services including packet latency, packet loss rate, throughput, signaling bandwidth overhead and device power consumption.

3.2 Mobility Support in IP

The problem of IP mobility has been in existence since the birth of IP networks, when most of the hosts were stationary. Early protocol designs took the mobility issue for granted by assuming that hosts could always be uniquely identified by their IP address. For example, a TCP connection can be identified by a 5-tuple; source IP address, source port, destination IP address, destination port, and the protocol type. However, this assumption no longer holds once the hosts start to roam around, prompting researchers to propose various designs to remedy the problem.

The concern in IP mobility support is on how to send data to a moving receiver. IP's point-to-point communication model is the reason as to why the IP mobility support solutions generally aim at solving essentially two problems ie finding the new location of a mobile and keeping the data communications uninterrupted despite the movement. Three essential components are necessary in any IP mobility solution in order to solve these two problems:

- A stable IP address as a mobile identifier

- A locator which is usually an IP address representing the mobile's current location
- A mapping between the locator and the identifier

A survey through existing IP mobility solutions leads to the following observations; the common core of all solutions is a rendezvous mechanism that tracks each mobile node (MN) and directs IP packets towards it [14]. Existing solutions can be divided into three categories namely:

i. Routing- this approach uses the routing plane as a RV. A MN can keep its IP address unchanged while moving. The MN is required to continuously send routing updates to inform all routers of its whereabouts. Its limitations include routing scalability.

ii. Mapping – This approach scale much better by using stable mapping servers as RV. The mobile node MN reports its current IP address to the RV whenever its address changes. When mapping is implemented at the network layer such as in Mobile IP [16] the RV (home agent) keeps the mapping of a stable home address of the MN to its current care of IP address. Packets meant for MN reach the RV which tunnels them using IP encapsulation to MN current IP address.[15]

iii. Tracing – In this approach, MN sends signaling messages to RV after each move to create a hop by hop reverse path from RV back to itself. This signaling messages set up the forwarding entry for the MN at each router between the RV and the MN so that RV can forward packets without tunneling. This approach is prohibitively expensive because it requires that each router keeps a per–mobile routing state.

3.3 Mobility Support in NDN

NDN mobility problem can be split into two:

- Consumer mobility and
- Producer mobility.

This is because of the two way interest /data flow in NDN.

3.3.1 Consumer Mobility

NDN receiver driven nature supports receiver mobility in that after handoff, the receiver/ consumer just resends requests for data that was not received. However, Overhead such as resource consumption and service latency may occur. Also, Interest packets are repeatedly transmitted after Hand over (for interests not received). The consumer mobility support in NDN may look remotely similar to the tracing based mobility support in IP, however they differ in a fundamental way. Tracing based mobility support performs a routing process separated from user communication while consumer mobility is a byproduct of stateful data plane built into the architecture. [15]

3.3.2 Producer Mobility

Content source mobility poses a lot of challenges that have attracted much attention from the research community Figure 8. When moving away a mobile node MP requests all routers to update their routing tables for successful reception of future/ ongoing content requests.

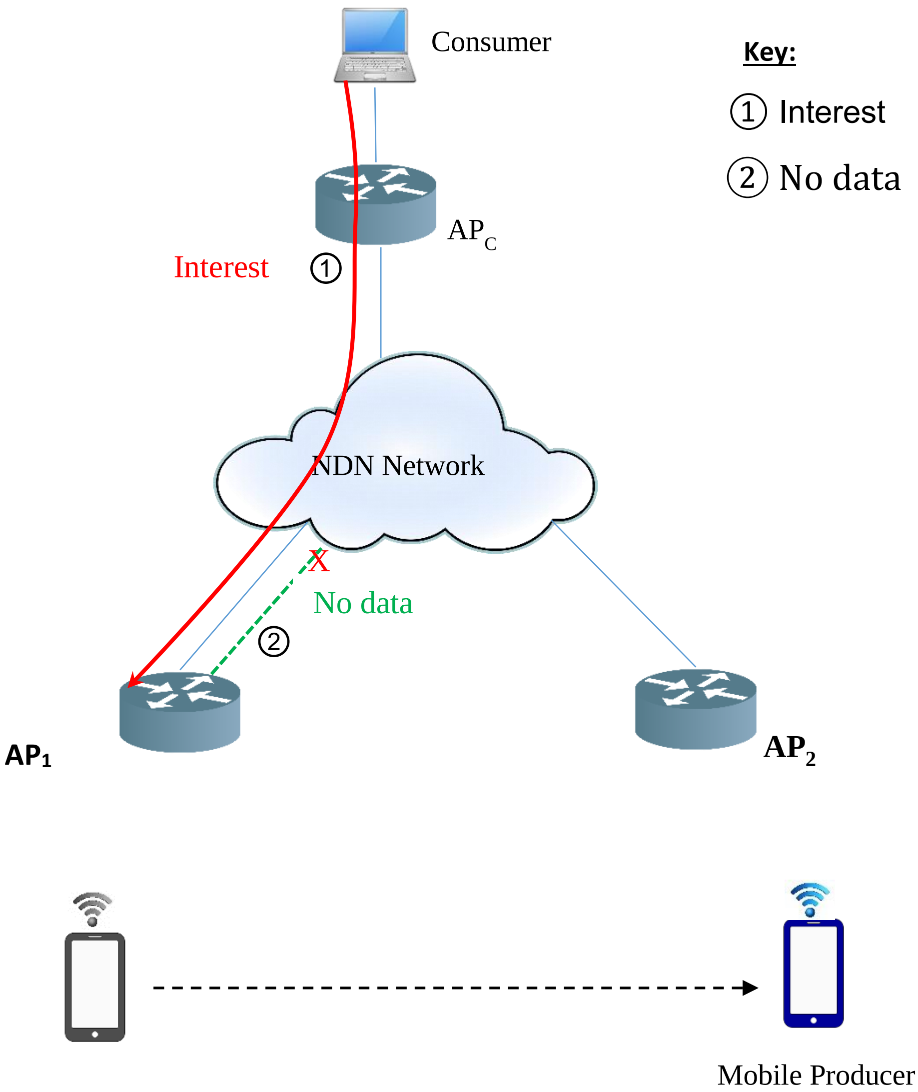

Figure 8 Producer Mobility Problem

Content source mobility brings about challenges such as frequent routing tables update and could result in long service disruption. CS are not aware of domain change of content Source hence reconstruction of entire routing information needs to occur to solve this. If renaming is considered it gives up naming persistence hence too many service access failures. Many mobile sources would pollute routing tables with specific prefixes tarnishing the advantages of prefix aggregation and hierarchical name structure [8]. One of the proposed solutions is to use a RV to find out where a MP is, namely MP chasing. In this approach, interests are steered towards an MP to retrieve data. Interests may not have to reach the MP if they find requested data in router caches along the way.

Another direction is to use a data rendezvous to ensure that mobile produced data can be retrieved with relative ease. Data produced by a MP can be moved to a stationary and easily accessible location.

3.3.3 Producer Mobility Solutions

There exists several proposed mobility management schemes in [2], which include;

- Rendezvous point scheme- Users update their location to a rendezvous point periodically when handoff occurs. However requires name operations which are expensive to the network. Also, there is a single point of failure.
- Sender driven control message- Moving node uses control messages to communicate new names to producers and receivers, however this scheme cannot effectively handle simultaneous movement of both producer and consumer.
- Indirection point- uses a separate server to relay all traffic. Interests are buffered at the indirection point in the event of handoff then forwarded later until the names are updated at the indirection point. Single point of failure and name updates are some of the difficulties experienced in this scheme.
- Interest Forwarding- mobile user must send a notification to the current attached router when it notices an imminent handoff. Router buffers incoming Interest for the user. Then the user can send a virtual interest for the buffered Interests. FIB are updated in intermediate routers for correct forwarding of Interests.
- Mobility support with greedy routing- uses standard CCN protocol and greedy protocol to embed a virtual coordinate into the content name that directs an interest to its destination. In order to forward a packet, the router first extracts destination coordinate from the packet, then it calculates the distance between the destination and each of the neighbors. The packet is forwarded to the neighbor who is close to the destination.

Most of the above schemes only supports consumer mobility and producer mobility with little efficiency and effectiveness.

Chapter 4
PROPOSED SCHEME

4.1. Introduction

This proposal aims at using resolvers at each NDN node to help redirect interests for migrated data to the new attachment point of the mobile producer (MP). Once the MP moves to the new attachment point, it triggers a mechanism that establishes a route between the home location and the new location hence subsequent interests can be redirected to the new attachment point to fetch required data. If the interests find data that matches the request within the intermediate routers ie before reaching the new attachment point, the data will satisfy the interest and the interests will not be further forwarded. This mechanism supports hierarchical naming even in highly mobile situations therefore there is no need for expensive name operations that would otherwise increase communication latency. Name operations in this case involve the change of the MP name prefix to reflect its current position or domain and update of the corresponding FIBs. This scheme ensures that there is ease of retrieval of migrated data and that data loss and excessive control message overhead is checked for smooth communication to take place. However, the scheme has limitations ie it ignores route optimization. That is, interests to the MP will most of the times be forwarded via MP's home first. This may lead to long service latency especially when MP moves many hops away from its home.

4.2 System Description

4.2.1 Binding Information Table

Binding Information Table (BIT) is a proposed new data structure that is used to record the binding information of a MP prefix and its foreign Access Point (AP_F) domain prefix. BIT format is as shown in Figure 9 below:

MP Prefix	Routing tag (AP_F Prefix)
/waseda/nakazatolab	/waseda/satolab

Figure 9 Binding Information Table (BIT) Format

When a MP moves to a foreign access point (AP_F), it sends a special interest called Binding Update (BU) to the previous attachment point $AP_{H.}$ The BU carries the MP prefix and the prefix of the current attachment point $AP_{F.}$ Once the BU is received at AP_H, it triggers the population of the BIT with routing information that points to the current location of the MP as shown in Figure 9. The BU also updates the BIT of all the intermediate nodes it passes through.

The Interest processing procedure is altered so that The BIT is checked first before the FIB for the MP prefix match Figure 12. If there is an entry matching the MP prefix in the BIT, a routing tag which is the prefix of the foreign access router (AP_F) is attached to the interest name and used to redirect the interest to the current location of the MP.

4.2.2 System Operation

Seamless handoffs for interactive applications and mobile content sharing can be effected through forwarding of interests to the next attachment point.

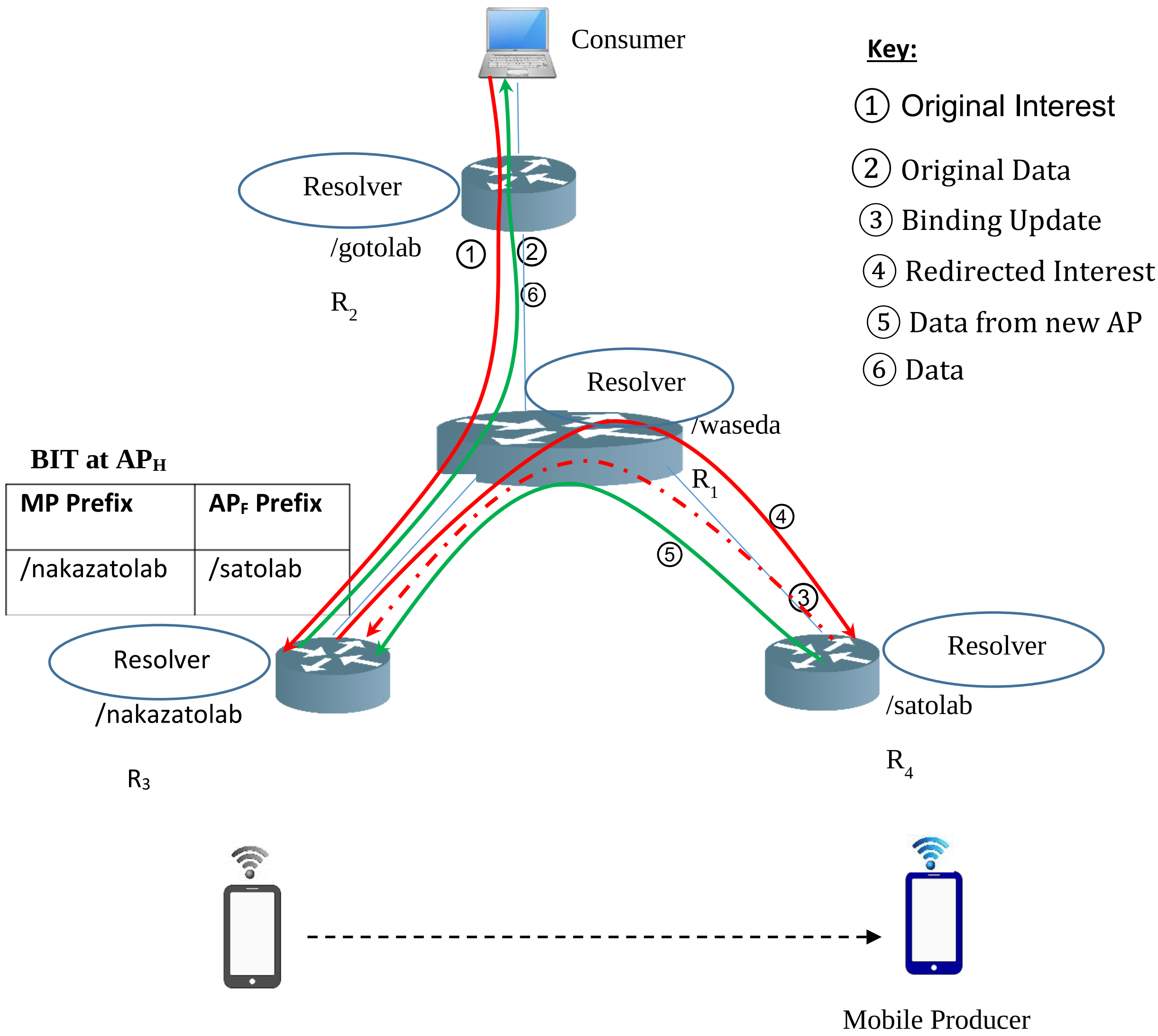

Figure 10 System operation

In Figure 10 above, an interest for migrated data is handled by the following procedure:

<u>Procedure</u>

1. The user generates an interest packet for example /waseda/nakazatolab/icn.pdf/v2/s1 and forwards it to the router R_2. The resolvers in our scheme are assigned names and carry out route resolution as postulated in [19]
2. The resolver /waseda/gotolab/ on R_2 will process the request for the interest /waseda/nakazatolab/icn.pdf/v2/s1 as per the flow chart in Figure 13

3. If resolver /waseda/gotolab does not find any entry for content name /waseda/nakazatolab/icn.pdf/v2/s1 in its BIT the router R_2 forwards the packet using its FIB to the next resolver /waseda on R_1
4. The same process takes place as at R_2 above and eventually the interest packet reaches the resolver /waseda/nakazatolab on R_3
5. At this resolver /waseda/nakazatolab on R_3 the content name is found within the BIT. Details of BIT setup are explained in section 4.2.3. A routing tag /waseda/satolab is then attached to the interest packet. The structure of the new interest packet and binding update packets is as shown in Figure 11 below. See section 4.2.3 for an explanation of binding update packet.

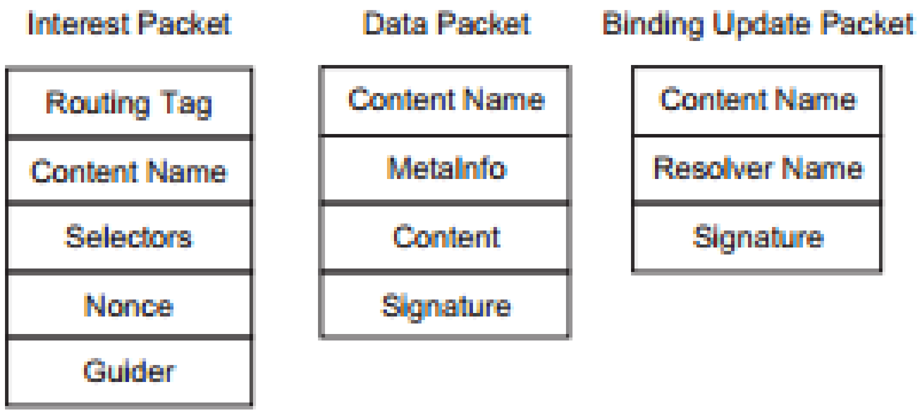

Figure 11 Interest, data and binding update packet format [19]

6. The interest packet is then forwarded to the resolver /waseda/satolab using FIB in the intermediate NDN routers. The PIT entries are also set using the content name. The migrated content is then forwarded to the user backwards through the set PIT. Figure 12 below shows how interest redirection takes place from the home access point (AP_H) to the foreign access point (AP_F)

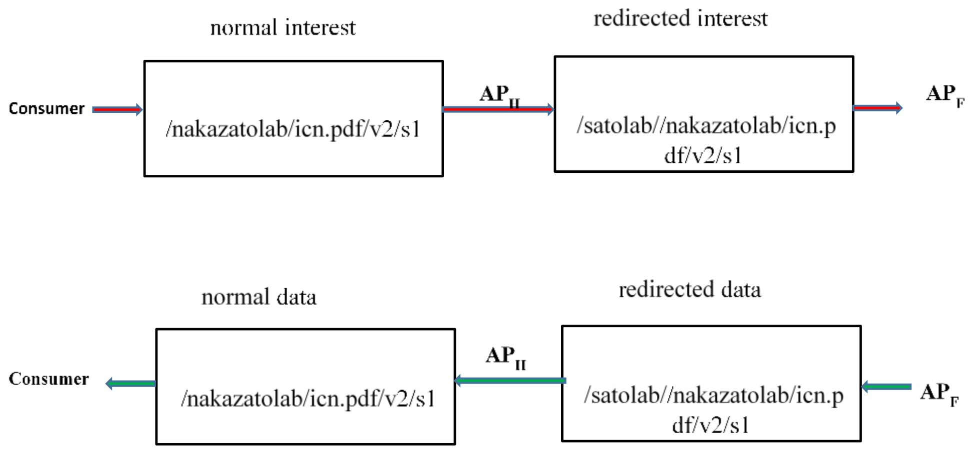

Figure 12 Interest and data Redirection at R_3 (AP_H) and R_4 (AP_F)

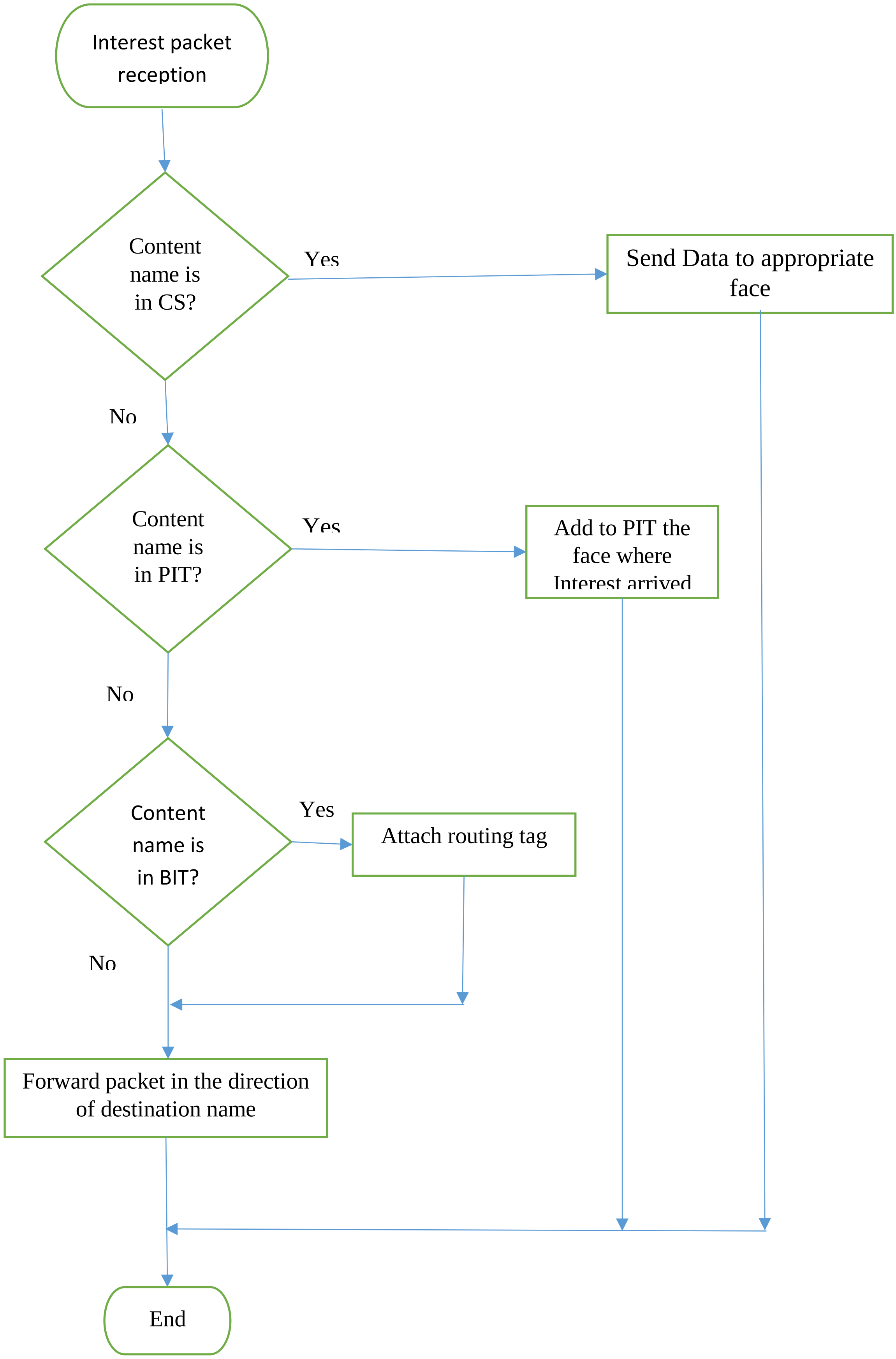

Figure 13 Incoming Interest processing

4.2.3 Handoff Management and BIT setup

Handoff management involves identifying a new access point and the allocation of data and control signal channels associated with the new access point to a mobile node. Handoff must be performed successfully, as infrequent as possible and must be imperceptible to the user. Signal strength, bandwidth insufficiency among others are the factors that trigger the handoff process. To achieve performance requirement in terms of per packet QoS, two techniques are used: (i) Movement prediction and detection and (ii) Buffering of interests that arrive at the old attachment point during handover process. Connection re-establishment must take place before breaking the previous link ie make before break in order to minimize packet loss rate and latency.

Our protocol involves the following steps in handling handoff and BIT setup:

1. The MP detects network status change, by comparing its own prefix with the domain prefix announced by the new access router AP_F.
2. If the MP detects a network change, it sends its home access point (AP_H) a Binding Update (BU) control message, containing its own prefix and its AP_F prefix. A Binding Update packet is used to inform the resolver at AP_H the whereabouts of a content, or a set of contents [19]. BU message is a special interest and is flagged to differentiate it from normal NDN interests. Its structure is depicted in Figure 11. The Signature field carries the signature of the sender of the Binding Update packet.
3. Reception of the BU message triggers the population of the BIT at AP_H with routing information that points to the MP's current location or domain. It also causes entries with similar prefix to be deleted in the same BIT at $AP_{H.}$ This guarantees that there are no multiple redirections for the same MP recorded in the BIT
4. The BU is also broadcast to nodes that neighbor AP_F to update their BIT to increase chances of retrieving migrated data. BU is forwarded by NDN forwarding schemes
5. Subsequent interests that arrive at the AP_H after MP has successfully migrated are processed per the flow chart in figure 13 and are redirected to the new AP_F to retrieve data.

4.3. Experimental setup

We experimented our solution on AT&T network topology which is a real ISP topology. This topology is part of the Rocketfuel project with graph properties as shown in Table 4.1 below. A graphical representation of the topology is shown in Figure 14.

Table 4.1 Number of routers links and POP for the 10 ISPs in Project [17]

AS	Name	ISP		with customer & peer		POPs
		Routers	Links	Routers	Links	
1221	Telstra (Australia)	355	700	2,796	3,000	61
1239	Sprintlink (US)	547	1,600	8,355	9,500	43
1755	Ebone (Europe)	163	300	596	500	25
2914	Verio (US)	1,018	2,300	7,336	6,800	121
3257	Tiscali (Europe)	276	400	865	700	50
3356	Level3 (US)	624	5,300	3,446	6,700	52
3967	Exodus (US)	338	800	900	1,100	23
4755	VSNL (India)	11	12	121	69	10
6461	Abovenet (US)	367	1,000	2,259	1,400	21
7018	AT&T (US)	733	2,300	10,214	12,500	108

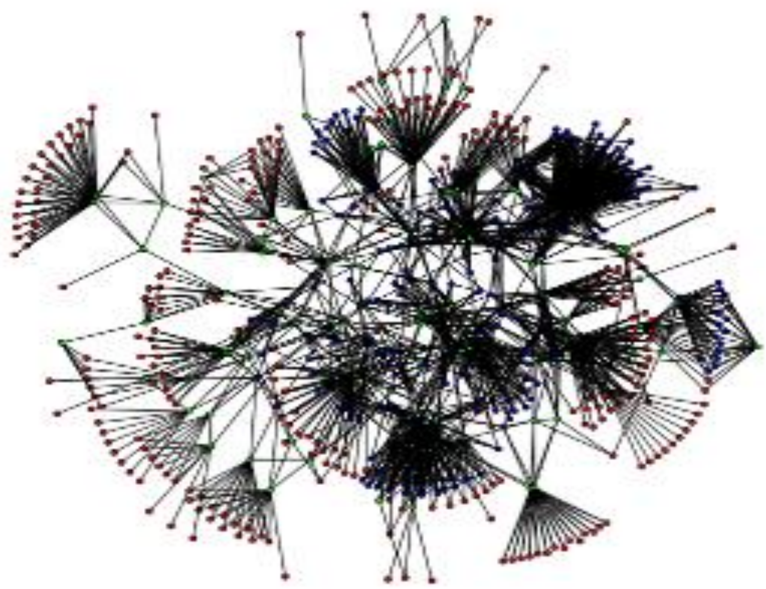

Figure 14 AT&T network topology (Rocketfuel)

Nodes in the rocketfuel topology are classified into three categories as below:

- Client nodes which are nodes with degrees less or equal to RocketfuelParams.clientNodeDegrees
- Gateway nodes which are nodes that directly connected to client nodes
- Backbone nodes (all the rest)

The RocketfuelMapReader was used to read the topology from .cch files which allowed the setting of parameters for all the nodes. The reader allows to keep only the largest connected network graph component since some .cch files may not give a connected network graph.

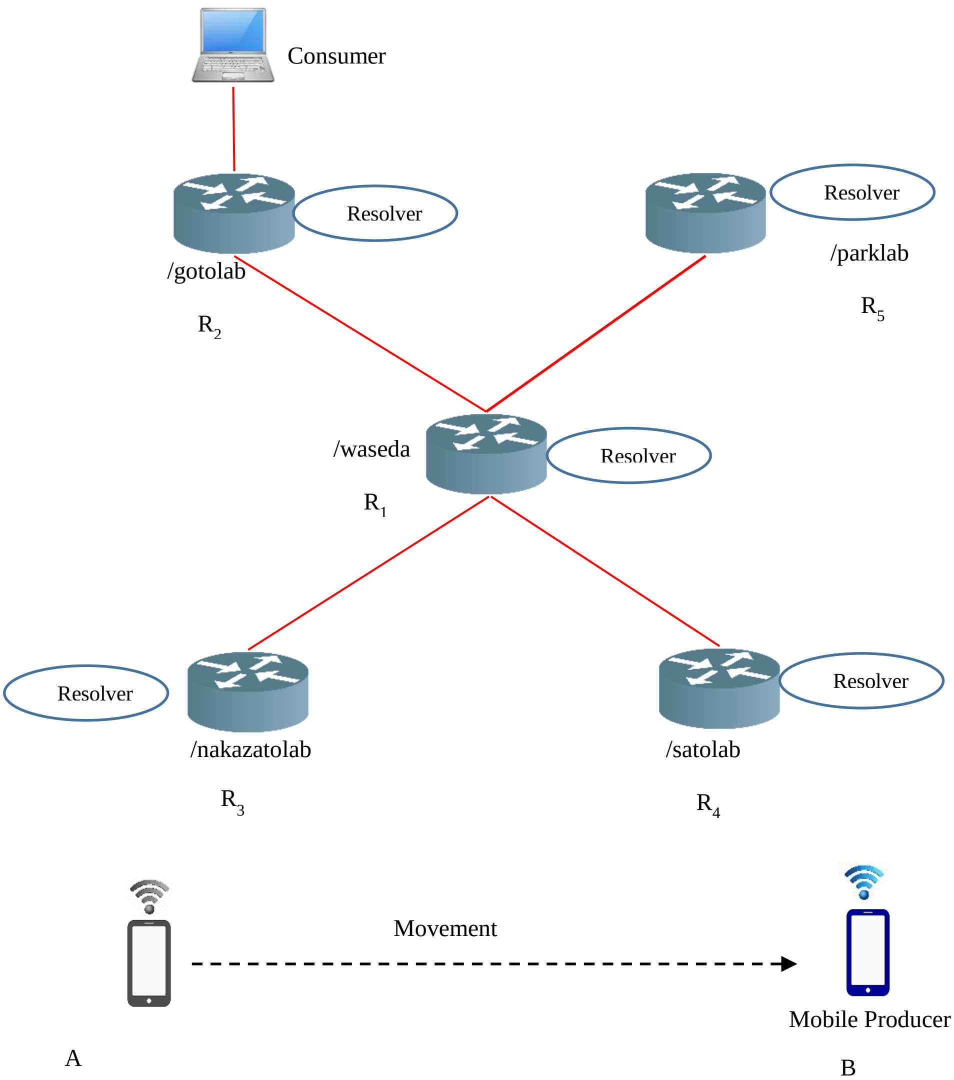

Figure 15 Experimental setup

The network consisted of five routers as in Figure 15 above, each with a name resolver, a mobile consumer and mobile producer. It should be noted that, only a section of the entire AT&T network is shown in the above diagram for clarity of explanation. R_1 is a backbone node while R_2, R_3, R_4 and R_5 are set as gateway nodes of the AT&T network. Each link delay is set to 5ms. The initial placement of the sender and receiver is arbitrary and the selection of the next attachment point of the MP is among nodes within a 2-hop radius. This means R_3 and R_4 are set to be one hop away from R_1 so that they are two hops away from each other. The consumer is set six hops away from the producer as in related paper [2]. The consumer was connected via a wireless link of similar capacity and delay to the wired links. The consumer was set to express 50 interests per second in the /waseda name space while the producer responded to the interests with data packets of payload size 1024 bytes.

The mobile node MP which is the content producer was initially attached to router R_3 then made to move to the next point of attachment R_4 while at the same time responding to the requests made by the consumer on R_2. Simultaneous handover for both Consumer and producer was set to happen after the first 10 seconds of running the simulation. The resolvers were used to determine where the mobile producer had moved to and redirect interests accordingly.

L3RateTracer was used to record packets forwarded at intervals of 0.05 seconds before, during and after successful handover at the initial attachment point AP_H and final attachment point AP_F. L3RateTracer is a ndnsim trace helper that collects and aggregates requested statistical information about number of packets of Interest/Data packets forwarded by an NDN node during simulation time. InInterests which is measurement of incoming interests and OutData which is measurement of outgoing data were considered. App delay tracer was also used to obtain data about delays between issuing interest and receiving corresponding data packet. The results from the tracers were stored in text files and analysis made using R script in order to determine handoff delay, packet drops and average latency. The simulation was set to run for 20 seconds.

Chapter 5

RESULTS AND DISCUSSION

5.1 Handoff Delay

Handoff delay is often used as one of the most important metrics for evaluating mobility solutions. [3, 4] We experimented our solution on a real ISP topology as described in section 4.3 and compared our solution with different mobility schemes as summarized by Liang et al in [2]. Since MobiCCN presents the best result in [2] we only compare our solution with it. Results for other mobility schemes are summarized in Table 1. Figure 16 shows the sequence numbers of the data packets the producer forwarded upstream before and after successful handoff happened.

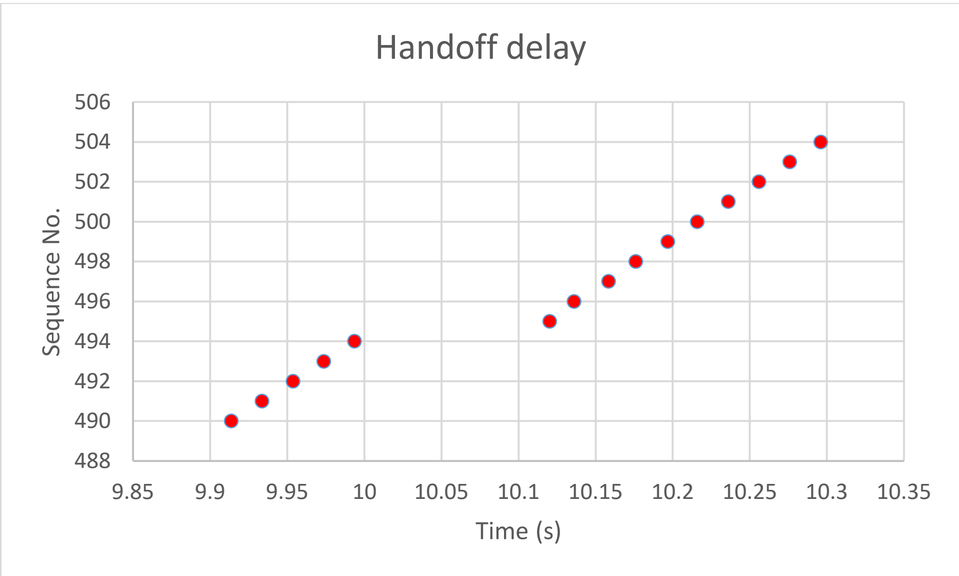

Figure 16 Producer handoff delay

We can see that when the producer finished layer 2 handoff at 10.0 sec, it started responding to redirected interests and sent lost data packets to the consumer. The interest path to the content producer's new attachment point was obtained from the binding information tables present at each router. Re-transmissions for lost data are subject to one round trip time delay (RTT). The producer handoff delay in our proposed mobility management scheme is approximately 126.54 ms as shown in the Figure 15.

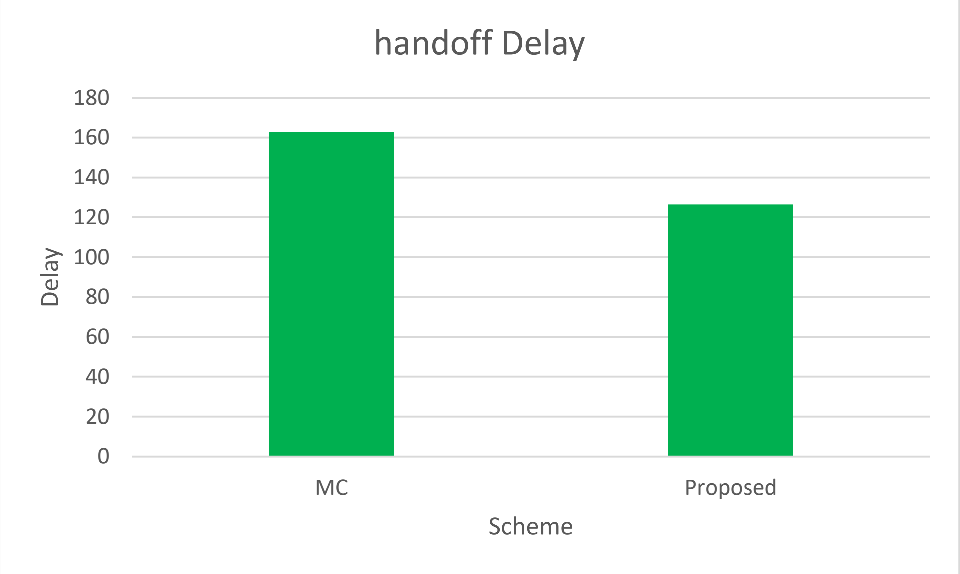

Figure 17 Handoff delay comparison with MobiCCN (MC)

The handoff delay in our scheme (labeled Proposed) is shown in Figure 17 above alongside handoff delay in MobiCCN scheme as presented by Liang et al in [2]. It can be seen that our method offers the least delay of about 126.54 ms which is the best among the other mobility schemes.

5.2 Average Latency

Average latency is a packet level quality of service parameter that is very important to real-time media services and therefore to evaluation of any mobility solution. Average latency for our experiment is shown in Figure 18. It is much lower than results of MobiCCN. This is because our scheme is simple and does not wait for timeout of the interest in order to trigger the mobility scheme. Also it uses normal NDN routing that is faster than greedy routing used in MobiCCN scheme. Based on this premise, we could argue that our proposal's average latency could perform better than all other mobility schemes.

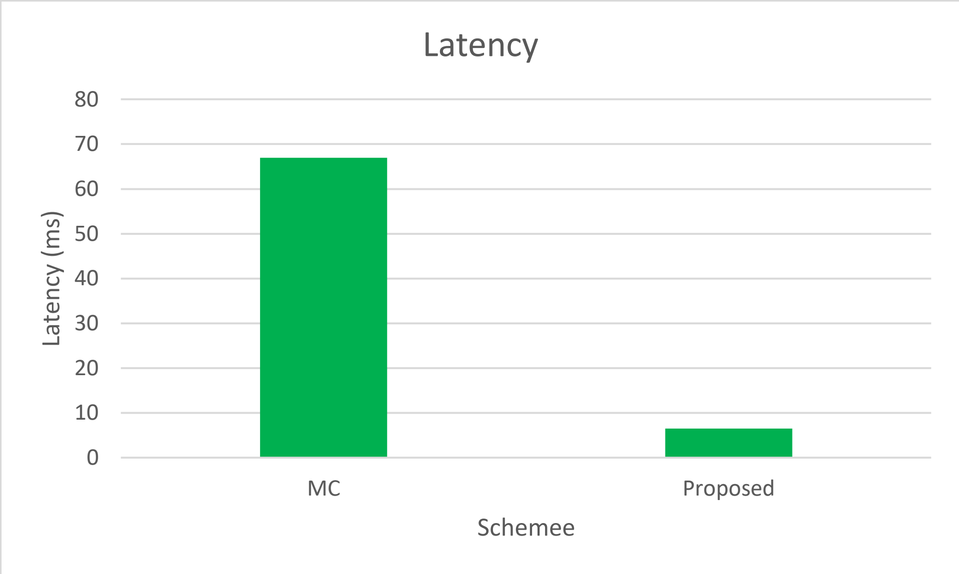

Figure 18 Average Latency Comparison

5.3 Packet Drop

We used L3RateTracer to measure the number of packets forwarded by the NDN routers at both the home access point and foreign access point. Our results are presented in the graphs below and they show that our scheme does not occasion any packet drops.

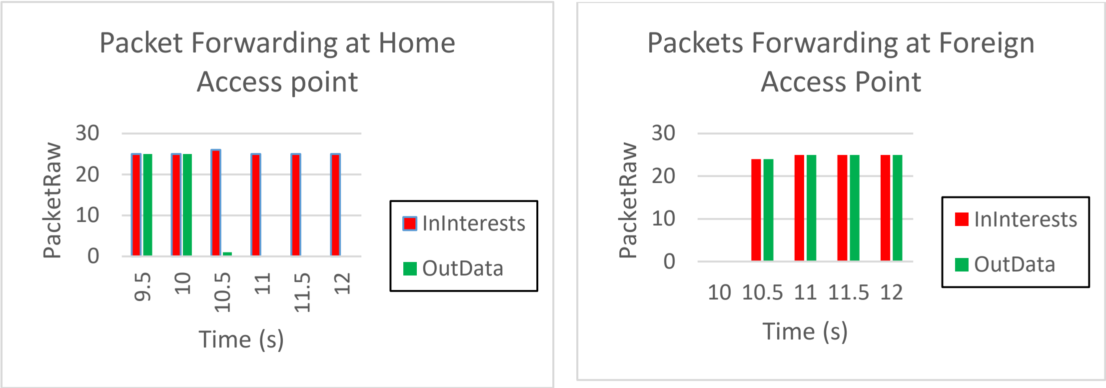

Figure 19 Packet forwarding at AP_H and AP_F

Table 5.1: Comparison of different mobility management schemes

Mobility Scheme	**Avg. Latency**	**Handoff delay**	**Single point of failure**	**Complexity**
Proposed Scheme	Low	Low	No	Low
MobiCCN (MC)	Medium	Low	No	Medium
Sender-driven Msg	Low	High	No	Low
Rendezvous Point	Low	Medium	Yes	Low
Indirection Point	High	Medium	Yes	High
Interest forwarding	Medium	Low	No	High

Part of the results presented in the above table are as summarized by Liang et al in [2].

Chapter 6

CONCLUSION AND FUTURE WORK

NDN is a proposed future clean slate internet architecture that attempts to adapt the current internet to its current demands and usage. This proposed architecture, however has some issues with the way it deals with content source mobility hence much research focus by the research community.

In this thesis, we propose a novel mobility management scheme that supports content source mobility and guarantees seamless handover in wireless information centric networks. Name resolvers and binding information tables at each NDN router were used to find and redirect interests for migrated data to the next point of attachment. Both qualitative and quantitative analyses were carried out on our proposal to check its effectiveness and efficiency in handling mobility issues and utilization of network resources like network bandwidth.

Four benefits were realized through experimentation:

(i) A modest handover delay of 126.54 ms
(ii) Reduced latency
(iii) No single point of failure
(iv) Low implementation complexity.

In future, we aim to improve our solution so that it further reduces latency that is caused when mobile producers migrate to an attachment point that is many hops away from their home access points.

REFERENCES

[1] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs and B. Rebecca, "Networking Named Content," *In ACM CoNEXT,* December 2009.

[2] Liang Wang, Otto Waltari, and Jussi Kangasharju "MobiCCN: Mobility Support with Greedy Routing in Content-Centric Networks", 2013 IEEE Global Communications Conference (GLOBECOM), 2013.

[3] D.-h. Kim, J.-h. Kim, Y.-s. Kim, H.-s. Yoon, and I. Yeom, "Mobility support in content centric networks," in Proceedings of the second edition of the ICN workshop on Information-centric networking, 2012.

[4] Z. Yan, R. Guo and Y. Park, "Network-based Fast Handover for Mobile Receiver in CCN", 2014 IEEE Global Communications Conference (GLOBECOM), 2014.

[5] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher and B. Ohlman, "A survey of Information-Centric Networking", 2012 IEEE Global Communications Conference (GLOBECOM), 2012.

[6] A. Afanasyev, I. Moiseenko and L. Zhang, "ndnSIM: NDN Simulator for NS-3", NDN Project, Tech. Report NDN-0005, July 2012.

[7] J. Sun, J. Sauvola, "Mobility and Mobility Management: A Conceptual Framework", in Proceedings of 10th IEEE International Conference on Networks (ICON 2002)

[8] J. Lee, S. Cho and D. Kim, "Device Mobility Management in Content-Centric Networking", 2012 IEEE Global Communications Conference (GLOBECOM), 2012

[9] G. Xylomenos, C. Ververidis, V. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. Katsaros, and G. Polyzos. A survey of information-centric networking research. IEEE Communications Surveys Tutorials, 2013.

[10] L. Zhang et al. Named data networking. Tech. Rep. NDN-0019, 2014.

[11] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang. A case for stateful forwarding plane. Computer Communications: ICN Special Issue, 36(7):779{791, April 2013.

[12] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang. Interest flooding attack and Counter measures in Named Data Networking. In Proc. of IFIP Networking, May 2013.

[13] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. Thornton, D. Smetters, B. Zhang, G. Tsudik, D. Krioukov, k. claffy, C. Papadopoulos, D. Massey, T. Abdelzaher, L. Wang, P. Crowley and E. Yeh, "Named Data Networking (NDN) Project," Technical Report NDN-001, October 2010.

[14] L. Zhang, R. Wakikawa, and Z. Zhu, "Support mobility in the global internet," in MICNET '09, 2009

[15] Y. Zhang, A. Afanasyev, J. Burke and L. Zhang, "A Survey of Mobility in Named Data Networking", in NOM'2016,IEEE 2016

[16] C. E. Perkins, "IP mobility support for IPv4, revised," RFC 5944, 2010

[17] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP Topologies with rocketfuel", *in Proceedings of ACM SIGCOMM, 2002*

[18] A. K. M. Mahmudul Hoque et al, "NLSR: Named-data Link State Routing Protocol",ICN 13, August 12,2013 Hong Kong, China

[19] H. Nakazato et al, "On-Path Resolver Architecture for Mobility Support in Information Centric Networking" in IEEE Globecom Workshops 2015