UNIVERSITY OF CAMBRIDGE

Availability, Integrity, and Confidentiality for Content Centric Network internet architectures

Mohibi Hussain

Churchill College

This dissertation is submitted on 29 October, 2019 for the degree of Doctor of Philosophy

Abstract

Written by: **Mohibi Hussain**

Thesis title: **Availability, Integrity, and Confidentiality for Content Centric Network internet architectures.**

The Internet as we know it today, despite being "the result of a series of accidents of choices" in Prof. Jon Crowcroft's words, has undoubtedly been an amazing success story. However, it has been constantly challenged by the demands of the overwhelming evolution of data traffic types, non-functional needs of applications and users, and device diversity. The phrase "future internet architecture" can be interpreted as referring to a revised set of design principles [43]. As Dr David Clark rightfully suggested, we need to "allow for the future in the face of the present". Content Centric Networking (CCN) is one of the candidates for a future internet architecture. Security is one of the most significant considerations while designing a future internet architecture. Availability, Integrity, and Confidentiality (AIC) are considered the three most crucial components of security: 1) availability is the assurance of continuous, reliable, and uninterrupted access to the information by authorized people, 2) integrity is the preservation of information and prevention of any change in it caused via accident or malicious intent, and 3) confidentiality is the ability to keep the information secret from unintended audience, intruders, and adversaries. This thesis discusses AIC related security threats and corresponding remedies for Named Data Networking (NDN) which is a promising example of CCN. It also presents a system dynamics modelling approach to bridge the gap between the technical solutions and business strategy by quantifying some of the qualitative variables salient to technology architects, policymakers, lawmakers, regulators, and internet service providers for the design of a future-proof internet architecture.

Declaration

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Preface and specified in the text. It is not substantially the same as any that I have submitted, or am concurrently submitting, for a degree or diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text. I further state that no substantial part of my dissertation has already been submitted, or is being concurrently submitted, for any such degree, diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text. This dissertation does not exceed the prescribed limit of 60 000 words.

Mohibi Hussain
29 October, 2019

Acknowledgements

"Knowledge enlivens the soul". — Imam Ali ibn-e-Abu Talib (SA)

I would like to thank Prof. Jon Crowcroft for his tireless encouragement and support. I opted for the University of Cambridge Computer Science PhD programme with an aspiration to make a difference in the world: in the pursuit to overcome the global digital divide by revolutionizing the Internet architecture. The dream seemed too ambitious in the beginning, but after spending four years under Prof. Crowcroft's insightful guidance, having the privilege of benefiting from his incredible vision, passion for innovation, and tireless commitment to enable his students realize their true potential, I have become increasingly optimistic about fulfilling my dream.

My former and present managers at the UIS namely Dr Mark Ferrar, Dr Martin Bellamy, and Prof. Ian Leslie, and colleagues Louise Marks, Ann Aves, Bob Dowling, Dr Jamie Thorogood, and Mick Paulsma have all been immensely supportive during this exciting PhD journey. The RIFE project introduced me to talented researchers including Dr Dirk Trossen, Dr Adisorn Lertsinsrubtavee, Dr Andrés Emilio Arcia-Moret, Dr Junaid Qadir, Anwaar Ali, Dr Arjuna Sathiaseelan, and Dr Mays F.H. AL-Naday who were very helpful during my research. Dr Zeinab Rezaiefar has been a great friend and collaborator in my work on NDN name privacy. I am also deeply grateful to my friends Dr Aliya Khalid, Florie Brizel, Zara Fateh Qizilbash, Mahwish Zahra, Beenish Parvaiz, Dr Shehar Bano, and Sharmeen Lodhi, and my aunt Andleeb Zahra Bokhari for their love and encouragement.

I am most thankful to my mother Misbah Tasaduq Hussain who has been a constant pillar of support for me throughout my academic and professional career. I am equally grateful to my father Engr. S.T. Hussain who has always believed in me and inspired me to strive higher than I ever thought I could. I would also like to thank my beloved sons Shah Murtaza Hussain and Shah Moataber Hussain who are my true sources of motivation and joy, my exceptional husband Syed Tahawar Hussain for his guidance and encouragement, and my brilliant siblings Zahra Hussain, Syed Zulqernain Hussain, Syed Ali Abid Hussain, and Namvar Hussain for their affection. Above all, I want to express my deepest gratitude for the unconditional love and guidance I received from my late grandmother Saeeda Altaf and my late grandfather Syed Altaf Ali Shah.

Contents

List of Figures

List of Tables

Preface

The work focusing on the three case studies presented in Chapter 5 builds on and extends the work submitted for my M.Sc. dissertation [78]. However, it is imperative to clarify the substantial differences. Although the case studies are the same as in the M.Sc thesis, and some of the data (from 50 interviews) was re-used, additional data (from 200 interviews) was further collected and re-analysed. Moreover, although the same modelling method (i.e., System Dynamics) is applied, it is to a different problem and data, and therefore produces different knowledge, specially in correlation to the technical work presented in the rest of this thesis.

Chapter 1

Introduction

This chapter discusses the problem statement or the falsifiable hypothesis explored in the rest of this thesis, the term “internet architecture” and the need for a new one, enlists some of the prospective future internet architectures, introduces the reader to Content Centric Networking (CCN)/ Named Data Networking (NDN) architectures and the Availability, Integrity, and Confidentiality (AIC) triad, presents the thesis road-map, list of contributions, and the research methodologies used for this thesis.

1.1 Thesis problem statement

“It is possible to address security requirements including Availability, Integrity, and Confidentiality for Content Centric Networking (CCN). We can attempt to do so by evaluating the threats to: 1) Availability of CCN via a DDoS attack, 2) Integrity of CCN through a content poisoning attack and, 3) Confidentiality of CCN through content name privacy threats, and their respective countermeasures. Additionally, we can demonstrate that the trade-offs in doing so imply that these previously overlooked non-functional aspects of CCN could now be quantitatively factored into the design and deployment plans for the prospective future internet architecture”.

The current Internet has been constantly challenged by the demands of the overwhelming evolution of data traffic types, non-functional needs of applications and users, and device diversity: presenting the need for a future internet architecture. There are various prospective internet architectures including Named Data Networking (NDN) which is a promising example of Content-Centric Networking (CCN). This thesis discusses Availability, Integrity, and Confidentiality (AIC) related security threats in NDN, namely Distributed Denial of Service attacks, content poisoning, and NDN name privacy respectively, and the corresponding technical remedies. It is noteworthy that to design an effective future-proof internet architecture, the technical problems and their solutions must not be considered in isolation. To address this concern, this thesis also presents a system dynamics modelling approach to bridge the gap between the technical solutions and the non-functional requirements by quantifying some of the qualitative variables salient to technology architects, policymakers, lawmakers, regulators, and internet service providers for the design of a future-proof internet architecture.

1.2 Future internet architectures

What is an internet architecture and why we need a new one?

According to the Cambridge English dictionary, the word "architecture" means the art and practice of designing and making buildings. The same dictionary defines the word "internet" as "the large system of connected computers around the world that allows people to share information and communicate with each other". The word internet was coined in the 1970s denoting a computer network connecting two or more smaller networks, derived from *inter* meaning 'reciprocal and/or mutual' and *network*. Based on the literal meanings of the words, an internet architecture can be safely described as a set of principles governing the art and practice of designing and developing a system that is capable of connecting computers (and various other connectable devices in the modern world).

As Dr David Clark has fittingly described in his book titled "Designing an internet" [43], the computer scientists tend to design an internet architecture based on what worked in the past for a specific use case, such as the current public global network known as "the Internet", private networks such as those used by defence departments of a country, and special purpose-built networks such as financial networks (e.g., Blockchain), thus misrepresenting the word *"architecture"* as the real design process remains missing from the foundation and is later carried out by other stakeholders.

The Internet is an amazing success story, connecting billions of users, facilitating scientific research, social, industrial, and economic development. However, the ever-changing dynamics of data, devices, and communication media require much more from an internet architecture. In Prof. Jon Crowcroft's words, "the Internet that we use today, is the result of a series of accidents of choices" since the 1970s. It was originally designed to connect computers; primary applications were remote terminal access, file transfer, and e-mail. With the need to connect clients and servers for web browsing content and subsequently video/audio streaming, the Internet had to evolve from computer-to-computer communication, to content-to-user communication.

The constantly evolving diversity of modern-day content and of the devices accessing it and the dynamically evolving needs of scalability, accessibility, affordability, security, and privacy etc.[1], have been indicating the need for a future internet architecture for quite

[1] Some more seemingly non-functional requirements of a future internet architecture are enlisted in Chapter 5.

some time. It is also worthwhile to mention here that whether a requirement is functional or non-functional is a contextual fact. What may be a functional requirement for one technical concept or product, might be non-functional for another, e.g., privacy, delay, and availability, etc.

Prospective candidates for a future internet architecture

The US National Science Foundation (NSF) sponsored the following four internet architectures under the Future Internet Architectures (FIA) program:

1. XIA
2. MobilityFirst
3. Information Centric Networking (ICN)/ Content Centric Networking (CCN)/ Named Data Networking (NDN)
4. Nebula

European research initiatives for potential future internet architectures are:

1. NetInf
2. PSIRP/Pursuit
3. COMET
4. GreenICN

   Moreover, there are some other prospective future internet architecture proposals such as the Accountable Internet [28] and I3 [114], etc., which have recently been gaining the attention of researchers globally.

1.3 Security by design in future internet architectures

Driven by the challenges faced by the current IP Internet architecture, the increasing significance of internet connectivity in financial transactions, and the growing threat of new sophisticated attacks, "security by design" has rightfully been among the main goals of most future internet architecture projects. Based on the learning experiences from the current Internet architecture, it seems imperative that we amalgamate necessary security provisions in the nascent stages of a future internet architecture design.

There is an old saying among security experts [43]: “A system without a specification cannot fail; it can only present surprises”. Just like the architectural design of the current Internet came into being without defining its exact requirements or utility, the security of a future internet architecture must be designed prior to knowing about the security threats that the future internet utilization may present. In other words, we do not only need a *futuristic* but a future-proof internet architecture.

In order to design a a future-proof and secure future internet architecture, information security can no longer be considered in isolation. It overlaps with various social, political, demographic, economic, and legal/regulatory aspects of internet usage. Availability, integrity, and confidentiality of data require input not only from technology, but more importantly from people and processes. Chapter 5 of this thesis presents some of the non-functional requirements to be considered while designing a future internet architecture. Security is a significant one among those. Ambrosin et al. provide a detailed analysis and comparison of security and privacy features and concerns in the aforementioned NSF-funded future internet architectures [26].

1.4 Content-Centric and Named Data Networking overview

Information Centric Networking (ICN) emphasizes on efficient and scalable content distribution. Named Data Networking (NDN) [2], a fork from PARC's Content-Centric Networking (CCNx) architecture [1], is one such research effort. Content-Centric Networking (CCN) is a notable Information-Centric Networking (ICN) architecture. Named Data Networking (NDN) exemplifies CCN and is one of the five NSF-sponsored Future Internet Architectures (FIA) [3]. Most of the work done in this thesis is based on NDN. However, it can be applied to any CCN internet architecture. Hence, in this thesis the names NDN and CCN have been used interchangeably. One of the main principles of NDN is named content. NDN also stipulates in-network content caching, by routers. To secure each content, NDN requires it to be cryptographically signed by its producer. This way, globally addressable and routable content can be authenticated by anyone, which allows NDN to decouple trust in content from trust in entities that store and disseminate it. NDN entities that request content are called consumers.

Unlike the IP based Internet that relies upon the end-points of communication and their names/addresses, NDN [80] [2] focuses on content which is named, addressable, and routable at the network layer. Each NDN content object is assigned a unique name. A content name is hierarchical and is composed of one or more variable-length components opaque to the network. Component boundaries are explicitly delimited by "/" in the usual path-like representation. For example, the name of BBC News web page content for May 28, 2019 might be: `/ndn/BBC/news/28May2019/index.html`. Large content can be split into segments with different names, e.g., segment number 9 of Bob's YouTube video could be named: `/ndn/youtube/bob/video.avi/9`.

By explicit naming of the data and binding of this name with a cryptographic signature [21], NDN provides a number of benefits including data-centric security, support for universal in-network caching, built-in multicast delivery, better alignment between the desired application usages, and the underlying data delivery model in general.

NDN communication uses the *pull* model and content is delivered to consumers only following an explicit request. There are two types of packets in NDN namely **interest** and **content**. A consumer requests content by issuing an *interest* packet for a given name. This interest can be satisfied from a producer or router. If an entity (an edge router or producer, whichever is nearer in the network) can "satisfy" a given interest, it returns the corresponding *content* packet. Content delivery must be preceded by an interest. If content C with name N is received by a router with no pending interest for N, C is considered unsolicited and is discarded. Name matching in NDN is prefix-based. For example, an interest for `/ndn/youtube/george/video2.avi` can be satisfied by content named `/ndn/youtube/george/video2.avi/19`; the reverse of this would not work.

NDN content includes several fields. A content message includes a name, a payload, and a digital signature computed by the content producer. Unlike content, interests are not signed. An interest message must include the name of the requested content. In case of multiple pieces of content sharing a given name, additional control information may be held within the interest to specify the desired content or to restrict the undesired content. Content signatures provide data origin authentication.

Some of the important NDN content fields are described below:

- `Signature` - a public key signature, generated by the content producer, covering the entire content, including all explicit components of the name and a reference to the public key needed to verify it.
- `Name` - a sequence of explicit name components followed by an implicit digest (cryptographic hash) component of the content that is recomputed at every hop. This effectively provides each content with a unique name and guarantees a match with a name provided in an interest. However, in most cases, the digest

component is not present in interest packets since NDN does not provide any secure mechanism for a consumer to learn a content hash prior to requesting it.

- `PublisherPublicKeyDigest (PPKD)` - $SHA256$ digest of the public key needed to verify the content signature.
- `Type` - content type, e.g., data, encrypted content, key, etc.
- `Freshness` - recommended content lifetime (after being cached) set by the producer.
- `KeyLocator` - reference to the public key required to verify the signature. This field has three options: (1) verification key, (2) certificate containing the verification key, or (3) NDN name referencing the content that contains the verification key.

Each content producer must have at least one public key, represented as a bona fide named content of *Type* = *key*, signed by its issuer, e.g., a certification authority (CA)[2]. The naming convention for a public key content object is to contain "key" as its last explicit component, e.g., /ndn/uk/london-airport/transit/lounge/key. An NDN interest includes the following fields:

- `Name` - NDN name of the requested content.
- `Exclude` - contains information about name components that must not occur in the name of returned content. This field can also be used to exclude certain content by referring to its digest, which, as noted above, is included in the content as an implicit last component of each content name, or in a separate field.
- `PublisherPublicKeyDigest (PPKD)` - the SHA-256 digest of the publisher public key. If this field is present in the interest, a matching content object must have the same digest in its `PPKD`.

There are three types of NDN node entities:

(a) consumer[3] - an entity that issues an interest for content.

(b) producer - an entity that produces and publishes (as well as signs) content.

(c) router - an entity that routes interest packets and forwards corresponding content packets.

Each node entity maintains the following three components:

[2] NDN is agnostic to trust management, aiming to accommodate peer-based, hierarchical, and hybrid PKI approaches.

[3] A consumer can also be a producer of the content.

(a) Content Store (CS) - cache used for content caching and retrieval. From here on, we use the terms CS and cache interchangeably.

(b) Forwarding Interest Base (FIB) - routing table of name prefixes and corresponding outgoing interfaces used to route interests. NDN does not specify or mandate any routing protocol. Forwarding is done via longest-prefix match on names.

(c) Pending Interest Table (PIT) - table of outstanding (pending) interests and a set of corresponding incoming and outgoing interfaces.

When a router receives an interest for the content name which is not in its cache and there are no pending interests for the same in its PIT, it forwards the interest to the next hop(s) according to its FIB. For each forwarded interest, a router stores some amount of state information, including the name in the interest and the interface on which it arrived. However, if an interest for content C_n arrives while there is a pending entry for the same content name in the PIT, the router collapses the present interest (and any subsequent interests for C_n) storing only the interface upon which it was received. If and when the required content is returned, the router forwards it out on all incoming interest interfaces and flushes the corresponding PIT entry. Since no additional information is needed to deliver the content, an interest does not carry any source address. If a content fails to arrive before some router-determined expiration time, the router can either flush the PIT entry or attempt interest re-transmission over the same or different interfaces.

An NDN router's cache size is determined by the local resource availability. Each router unilaterally determines which content to cache and for how long, though lifetime (as mentioned above) can be recommended by the producer. Upon receiving an interest, a router first checks its cache to see if it already has the requested content in its cache. Signed producer-originated content allows consumers and routers to authenticate it upon reception regardless of the entity serving it.

1.5 Availability, Integrity, and Confidentiality in CCN

Security issues are broadly concerned with availability, integrity, and/or confidentiality of information or data involved. This thesis presents three different security threats and their mitigation, each belonging to these three distinct areas of security and their mitigation. It can safely be said that for any security risk, threat, and vulnerability, the availability, integrity, and confidentiality of information/data are closely linked, impacting each other directly or indirectly.

The **CIA** (Confidentiality, Integrity, and Availability) triad is the most popular reference model for information security and information assurance, sometimes affectionately referred to as the Holy Trinity of Data Security [95]. The CIA Triad is also called the **AIC** (Availability, Integrity, and Confidentiality) triad to avoid confusion with a well-known three-letter American intelligence services' agency. In this AIC model [72], availability refers to a state where authorized people are guaranteed to have reliable access to the information, integrity is the preservation of trustworthiness and healthiness of data and prevention of its tampering by unauthorized users, and confidentiality stands for a set of directives that prevent the exposure of data to unauthorized parties by governing and limiting access to it.

In this section we provide a high-level overview of some well-known security issues in CCN.

Consumer security

A consumer which does not produce any content, is not a traceable nor addressable host as it has no assigned namespace and no corresponding public key that could be used to verify its content. As a result, routers shall not be forwarding any interests to that consumer. Also, the CCN design implies that routers only forward content towards a consumer if the consumer has specifically requested it through an interest. Hence a consumer will not receive unwanted traffic unless sent maliciously by a router directly connected to it. This is a distinct security advantage of CCN over IP.

Router security

With the exception of FIB, which is influenced exclusively by control traffic, a regular IP router is stateless with respect to data traffic [62]. The CCN router performs more complex functions as it needs to maintain a Pending Interest Table (PIT) and may or may not maintain a cache. PIT and cache depend on correspondence with consumers and producers, requiring processing ability that is not needed in an IP router. Also, additional functionality is required of a CCN router to be able to verify content signature. These additional features make a CCN router more susceptible to availability attacks such as Denial of Service through interest flooding as discussed in Chapter 2.

Cache and content security

Cache and/or content poisoning attacks target the availability of the network and hence the availability of information. In a cache poisoning attack, an adversary injects corrupted or fake content into router caches. A content can be termed as fake if it has a valid signature, but is generated with a wrong private key for the name under which it is published, i.e., by an incorrect producer [62] [63]. A corrupted content is one carrying an invalid signature. A content poisoning attack involves injecting fake or corrupted content into the network [66]. Content poisoning and a proposed mechanism for its mitigation is discussed in Chapter 3 of this thesis.

Since each NDN content is signed, a consumer can perform **signature verification** on all received content and can request a different copy of the content using the `Exclude` field in the interest. Moreover, any NDN router can perform signature verification for any content to be forwarded or cached. Theoretically, content signatures provide an effective defence against content poisoning attacks since the fake or corrupted content can be easily detected and discarded before being forwarded to the consumers. However, signature verification as a process faces two major challenges. The first challenge is router overhead and hence efficiency problems. The second challenge is trust management which includes obtaining the right key to verify a content signature.

1.6 Thesis road map

This thesis is divided into six chapters.

(a) The first chapter describes the definition of an internet architecture and the need for a new one, examples for a few prospective future internet architectures, an introduction to CCN and Named-Data Networking NDN, security challenges from the AIC triad, thesis road map, list of contributions, and the research methodologies used in this thesis.

(b) The second chapter presents a solution to mitigate Distributed Denial of Service (DDoS) attacks to improve the availability of both the CCN network and the information/data being transported over it.

(c) The third chapter addresses the second component of the AIC triad i.e., integrity of content/data/information in CCN.

(d) The fourth chapter addresses the third and final component of the AIC triad i.e., confidentiality of content/data/information in CCN by presenting a content name privacy protection approach using 1) name obfuscation and 2) gateway routing.

(e) The fifth chapter bridges the technical and business evaluations through examples of three real-life case studies, translating some of the qualitative requirements into quantitative parameters using system dynamics modelling. This chapter also discusses the difference between and examples of some functional and non-functional requirements, and illustrates a few socio-economic modelling examples for a future internet architecture using system dynamics.

(f) The sixth and final chapter concludes by summarizing the work presented in this thesis and prospective future work in this domain.

1.7 Methodologies

For the technical contributions in Chapters 2, 3, and 4, we used ndnSIM [22] simulations and also considered some rudimentary data input from the real world test beds such as guifi.net [13] and TakNet [6] for ICN. For the socio-economic analysis we used data from the technical evaluations, case studies, and interviews for data collection and parameter identification; and Vensim [15] software for system dynamics [5] modelling simulations and mathematical computations. Section 5.2 in Chapter 5 of this thesis introduces basic concepts used in system dynamics, and Section 5.3 in Chapter 5 presents a modelling example using real life case studies.

1.8 List of contributions

This thesis presents two major categories of contributions. Chapters 2, 3, and 4 discuss technical challenges in availability, integrity, and confidentiality for CCN/NDN, whereas Chapter 5 presents the socio-economic influences on the design decisions for a future internet architecture such as CCN.

Technical contributions

(a) Availability in CCN - Kiram and WOE: is discussed in Chapter 2. We address the Distributed Denial of Service (DDoS) challenge in CCN and propose a novel approach to mitigate it.

(b) Integrity in CCN - Content poisoning and its mitigation: is presented in Chapter 3. We address the issue of content poisoning in CCN caused by fake interests, content, and signatures and its mitigation using a proposed solution that we named Iris. We amalgamate and improvise upon the honeypot and exclusion techniques and introduce the reverse MA-ABE technique in Iris. Using these techniques as an intelligent framework, Iris detects the fake content objects, identifies, and isolates the Compromised Consumers, and eventually, the Adversarial Producers.

(c) Confidentiality in CCN - Name privacy protection: is addressed in Chapter 4 by introducing a unique solution to offer user-specific privacy protection. User's trade-off between privacy and utility is analyzed using game theory based algorithms. Privacy protection is enhanced using two distinct layers using a) partial or full name obfuscation and b) onion routing through gateways.

System dynamics modelling and its link with technical contributions

The term architecture usually refers to a concrete and stable design. However, if there is one lesson to be learnt from the current Internet evolution, it is the same as what Heraclitus, a Greek philosopher, has been quoted as saying "change is the only constant in life". In other words, a future-proof internet architecture would be one that passes the test of time and changing user needs. Another important fact to consider is that Internet connectivity has strongly impacted the social, industrial, agricultural, economic, educational, medical, and political aspects of human life. As the internet itself evolves, it must also take into account the ever-changing dynamics from all the relevant domains of life. This phenomenon can alternatively be termed as the socio-economic aspect of a future internet design. These non-technical aspects strongly influence the requirements that a future internet architecture must fulfill. Some of these requirements may be functional and others non-functional; the distinction between the two is purely contextual depending upon the application or user requirement. Section 5.1 in Chapter 5 of this thesis provides further insight into this topic and Table 5.1 enlists some examples. Chapter 5 introduces system dynamics modelling to quantify the qualitative parameters that must be considered while designing a future internet architecture. Although, it would not be completely fair to label these contributions as non-technical because they directly take input from and then inform the technical design via feedback: however, for the ease of understanding we can categorize these contributions as the socio-economic evaluation for a future internet architecture.

As described in the previous section, Chapter 2 focuses on Availability in CCN. We address the Distributed Denial of Service (DDoS) challenge in CCN and propose

Kiram and WOE as a novel approach to mitigate it. In Chapter 3, we address the issue of Integrity by mitigating content poisoning in CCN caused by fake interests, content, and signatures using a proposed solution that we named Iris. Chapter 4 addresses Confidentiality in CCN- Name privacy protection is addressed by introducing a unique solution to offer user-specific privacy protection. User's trade-off between privacy and utility is analyzed using game theory based algorithms. Privacy protection is enhanced using two distinct layers using a) partial or full name obfuscation and b) onion routing through gateways. While a DDoS attack, content poisoning, and name privacy are technical security problems, Availability, Integrity, and Confidentiality may be referred to as three of the most significant non-functional security requirements (some others listed in Table 5.1 Chapter 5) of a future internet architecture. Privacy and utility (trade-offs used in Chapter 4) are also non-functional requirements, directly linked to technical problems and their solution. It is also imperative to consider that in addition to being dependent on their technical aspects, none of the non-functional or functional requirements can be considered in isolation. They have a direct correlation with each other as well as other parameters such as delay, user experience control, collaborative innovation, and perception of intrusiveness as illustrated by the system dynamics models presented in Chapter 5. In this thesis, the system dynamics modelling approach presents a unique perspective to bridge the gap between these technical and non-technical parameters to effectively inform the design and development of future internet architectures.

1.9 Summary

In this chapter we described the future internet architectures, CCN, and the AIC triad, presented the thesis road map, and listed the contributions and research methodologies used for the thesis.

Topic of the next chapter is availability in CCN, which is the first of the three AIC concepts covered in this thesis.

Chapter 2

Availability in CCN- Kiram and WOE

This chapter presents a solution to mitigate Distributed Denial of Service (DDoS) attacks to improve the *availability* of both the CCN network and the information/data being transported over it.

2.1 Introduction

Availability is perhaps the most significant pillar of the AIC triad as it is by definition (in terms of information security) [7] the guarantee of reliable access to the information by authorized people. This definition itself makes it evident that availability would be of utmost importance to every internet designer and user, irrespective of the fact that they care about information security or not. As discussed previously in Chapter 1 Section 1.3, security by design must be the primary consideration while designing a future internet architecture; CCN/NDN is no exception.

As described in the previous chapter in Section 1.4, the NDN messages are classified into two main categories namely *interest* and *content* [105]. A consumer or information subscriber's request is represented by an interest that specifies the desired content by a name. The content includes name, required data object, and a digital signature of the content producer. Names are hierarchical structures composed of one or two components. Content is delivered to consumers only upon explicit request. Each request corresponds to an interest message and causes NDN routers to store a small amount of transient state in a structure called Pending Interest Table (PIT). This information is used to route content back to consumers. Forward Information Base (FIB) is analogous to a routing table and maps the content name and the network interface to be used to direct the interest message towards the content serving node (producer or cache). Content Store (CS) is the router cache and is the first place the router checks for content availability upon the arrival of an interest message. If the content is not found in cache, the FIB is checked. Each time an interest message cannot be satisfied from the cache, a record is generated in the PIT. PIT is then checked upon arrival of a content object and the content will follow the reverse route of the interest message. We use the term *honest interest* for a normal/non-adversarial interest generated by a genuine consumer.

2.2 Denial of Service attacks in IP Based vs CCN internet architectures

During recent years, Denial of Service (DoS) attacks have become increasingly effective against the availability of the current IP based internet.

DoS vs DDoS

The flooding traffic of a DoS attack may originate from either a single source or multiple sources. We call the latter case a Distributed Denial of Service (DDoS) attack [101].

Types of DoS/DDoS attacks and their effectiveness in IP vs CCN

DDoS attacks can be classified further into 1) resource exhaustion and 2) timing attacks. Resource exhaustion attacks can be classified further into infrastructure, source, mobile blockade (a wireless node flooding the network with interests and then disconnecting), and flooding attacks [17].

Following are some of the renowned types [63] of DoS/DDoS attacks and their impact on the current IP based Internet is compared with that on CCN:

2.2.1 Bandwidth Depletion attacks

In the current IP-based internet, the Bandwidth Depletion attack is usually carried out via routing protocols such as TCP, UDP, and ICMP, etc. In a Bandwidth Depletion DDoS attack, the adversary controls *zombies* to flood their victims with

IP packets at the highest possible data rate. In case of TCP, the connection-based nature of the protocol implies that each maliciously sent packet tries to open a new connection, requiring the victim to create and store corresponding state, thus resulting in exponential saturation of resources. Due to the caching in CCN, such an attack would have limited impact. An adversary can launch a number of zombies to request existing content from a victim. However, once the content is requested from the producer, CCN routers will cache it and serve the later interests from the caches.

2.2.2 Reflection attacks

In a reflection attack, the adversary uses secondary victims as reflectors to target the primary victim. The adversary sends malicious traffic (packets with the primary victim's address set as the source address). CCN is resilient to such attacks as the content follows the same path in reverse of the interest. The number of content copies a consumer can receive is limited by the number of its interfaces. The adversary can only affect the targeted victim if it is on the same physical network.

2.2.3 Black-holing by prefix-hijacking

Black-holing through prefix-hijacking is an effective attack in IP networks as it involves corrupting the routing information. In a *black-holing* via prefix hijacking [30] attack, a malicious or compromised Autonomous System (AS) advertises invalid routes, misguiding other autonomous systems to route their traffic to itself, acting as a *black-hole*, where all the traffic sent to the malicious autonomous system is discarded. Several mitigation techniques have been proposed [84] [129], but prefix-hijacking still remains a serious security threat in the current internet.

CCN is more resilient to the prefix-hijacking attacks compared to the IP based internet as the routing updates in CCN are signed and can be verified [76] except in compromised routers. Since content follows the same path as an interest in reverse, CCN routers can use information such as the number of unsatisfied interests at any interface to detect if a particular prefix has been black-holed. Furthermore, CCN routers maintain statistics about performance of each interface with respect to a particular prefix. In case of a perceived attack, loop detection and elimination allows redundancy through multi-path forwarding. Denial of Service (DoS) is a routing-related security concern. An adversary could launch a DoS attack by sending many requests to a single source for available content or sending multiple requests for non-existent content, also termed as *fake interests.* A basic illustration of a DoS attack in NDN is demonstrated in Fig. 2.1.

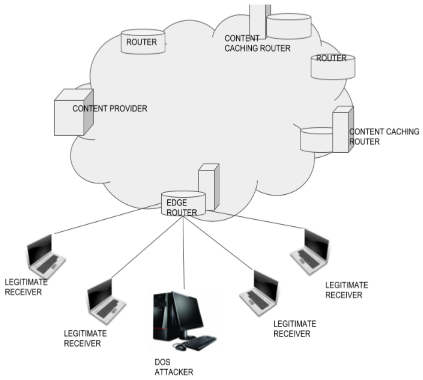


Figure 2.1: Conceptual illustration of a DoS attack in NDN

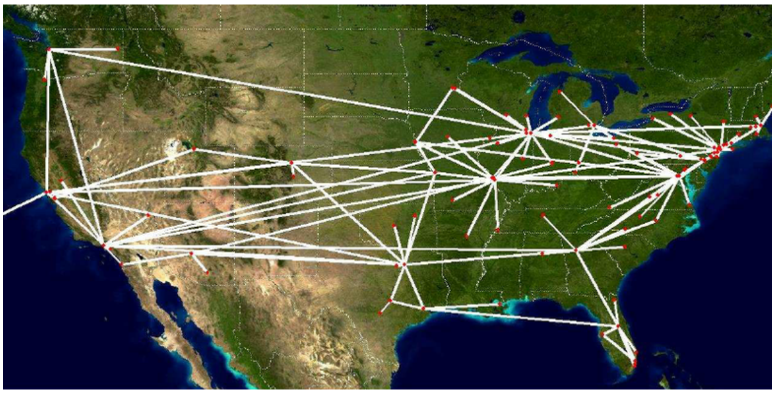


Figure 2.2: AT&T Network Topology (AS 7118) from the Rocketfuel data bank for the continental US

2.2.4 Interest Flooding Attack (IFA)

Flooding a router with fake interests allows the adversary to saturate the PIT. This has been identified in previous work under the name of Interest Flooding Attack (IFA) [61]. In this thesis, we focus on IFA DDoS attacks only (using fake interests). An adversary sends a large number of *fake interests*, i.e., requests for non-existent/unavailable content. The CCN/NDN architecture is designed to find the closest copy from the best available location, therefore the interests take different routes to the content source/producer or router cache/CS, resulting in an overload of the PIT table. If the PIT is completely full, new interests are dropped.

2.3 Related work on DDoS defence

While DDoS is a relatively new area of interest in NDN, there has been no dearth of DDoS mitigation research for the current Internet architecture, specially since the first

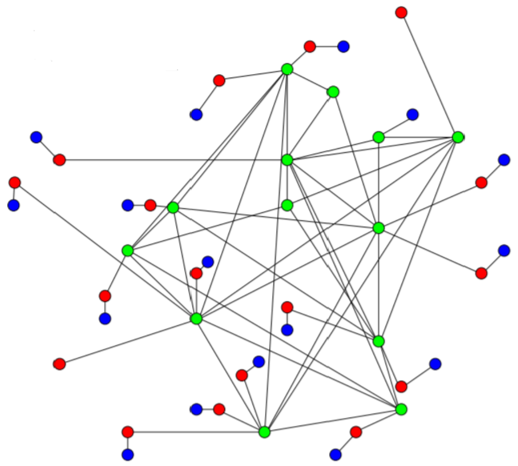


Figure 2.3: DFN Network topology with core routers (green), edge routers (red), and consumers (blue)

DDoS attack in 1974 [11] and the large scale DDoS attacks [10] that gained attention during the early 2000s. Mahajan et al. [91] introduced a network-based solution, called Pushback, as an inside-the-network defence against DDoS attacks. Ioannidis and Bellovin [79] explored this idea further in traditional Internet infrastructure. Afanasyev et al. [20] have proposed DDoS mitigation in NDN through rate-limiting, per-face fairness, per-face statistical analysis, and priority. It requires PIT's extension and storing statistics by the router, implying that the scope is individual (per router node) as well as collaborative (network-based). Compagno et al. [45] also address interest flooding and DDoS in NDN by proposing a mechanism named Poseidon for detecting and mitigating interest flooding. Gasti et al. [61] and Compagno et al. [46] proposed mitigation of interest flooding attacks in NDN by periodic monitoring of PIT usage and interest rates. Dai et al. [50] presented a collaborative technique between routers and producers through interest trace-back. To loosen the stress of PIT attacked by IFA, Wang et al. [121] proposed an approach called Disabling PIT Exhaustion (DPE) to divert all the malicious interests out of PIT by directly recording their state information (e.g., incoming interface) in the name of each malicious interest rather than PIT, as well as introducing a packet marking scheme to enable data packet forwarding without the help of PIT. Wählisch et al. [119] analysed resource exhaustion, mobile blockade, state de-correlation attacks (where adversary compromises the content or cache by updating it at a frequency exceeding the content request consolidation), and usage of data-driven state to launch DoS and DDoS attacks.

The concept of intelligent learning for DDoS defence in the current Internet infrastructure is not new to the industrial and academic worlds. Cisco [8], Fortinet [12],

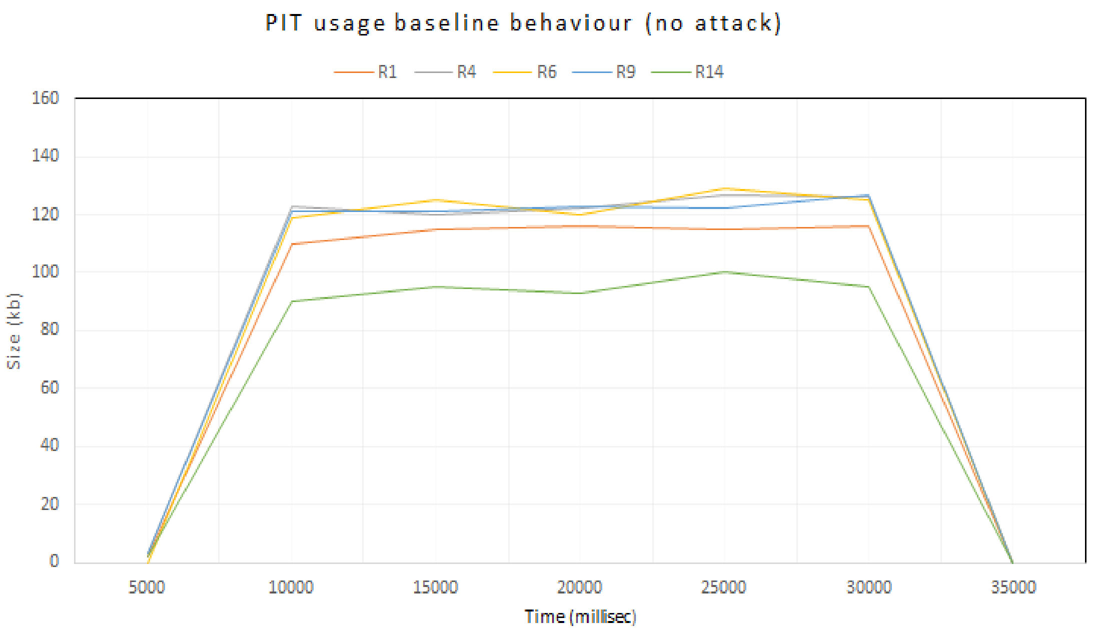


Figure 2.4: PIT usage in the absence of an IFA

CloudFlare [9] and Akamai [24], etc., have all been using intelligent learning and traffic pattern analysis mechanisms for anomaly detection to improve network performance in general, and to compute DDoS defence strategies in particular, for a while. Yuan et al. [128] presented DeepDefense, which is a recurrent deep neural network to learn patterns from sequences of network traffic and trace network attack activities. However most of these solutions involve large scale independent systems which 1) first segregate the good traffic from the bad, 2) then sink-hole [100] or black-hole [25] the suspicious traffic[1] and finally, 3) execute high performance resource consuming computations on the segregated or sink-holed traffic.

Our work compliments and builds upon some of the above mentioned DDoS mitigation strategies by combining the traditional anti-IFA techniques with intelligent temporal learning for anomaly detection and novel computation for alert generation and feedback.

Table 2.1: Kiram computational parameters

Parameter	Description
ρ_{ht}^{x}	PIT space utilization for normal traffic during time interval t
ρ_{at}^{x}	PIT space utilization for abnormal traffic during time interval t
δ^{x}	threshold discerning between normal vs abnormal PIT size for interface x
μ_{h}^{x}	rate of outgoing content objects corresponding to honest interests for interface x
μ_{a}^{x}	rate of outgoing content objects corresponding to satisfied interests for interface x during an adversarial attack
Γ^{x}	interest rate-limiting threshold
ω_{t}^{x}	WOE alert (with variables frequency, timestamp, namespace and optional description link) received from interface x during time interval t
η^{x_ω}	namespace associated with WOE alert ω on interface x
τ^{x_ω}	time-stamp associated with WOE alert ω on interface x
$\daleth^{x_\omega}$	frequency associated with WOE alert ω on interface x
ζ^{x_ω}	description link associated with WOE alert ω on interface x

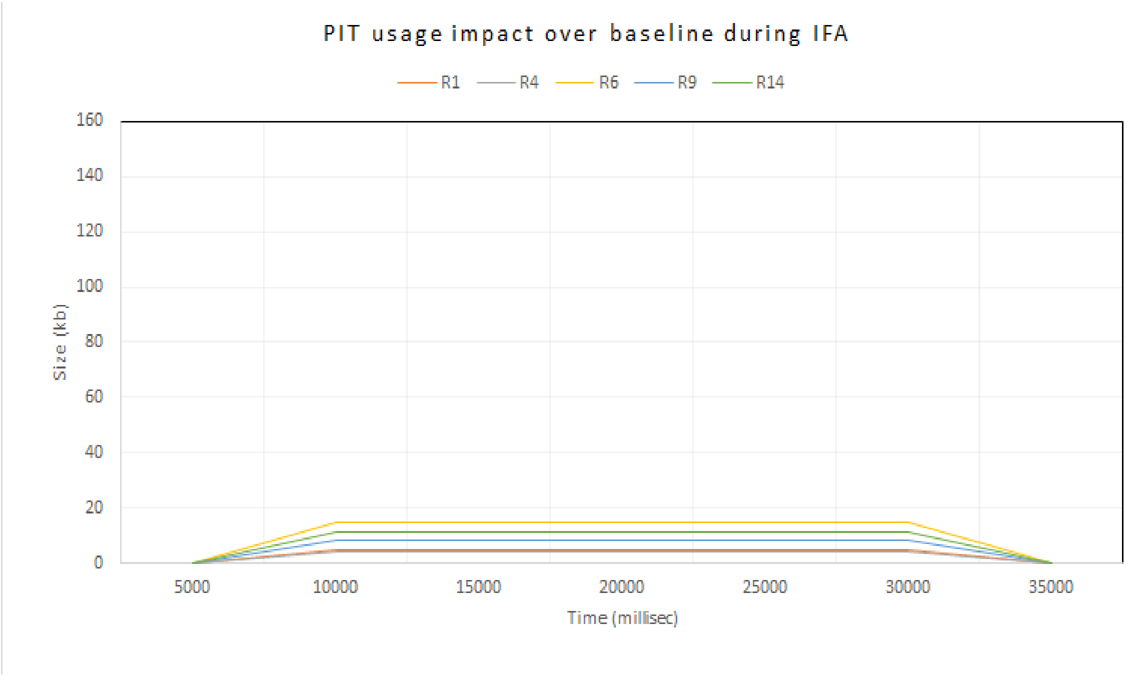


Figure 2.5: IFA impact on PIT usage

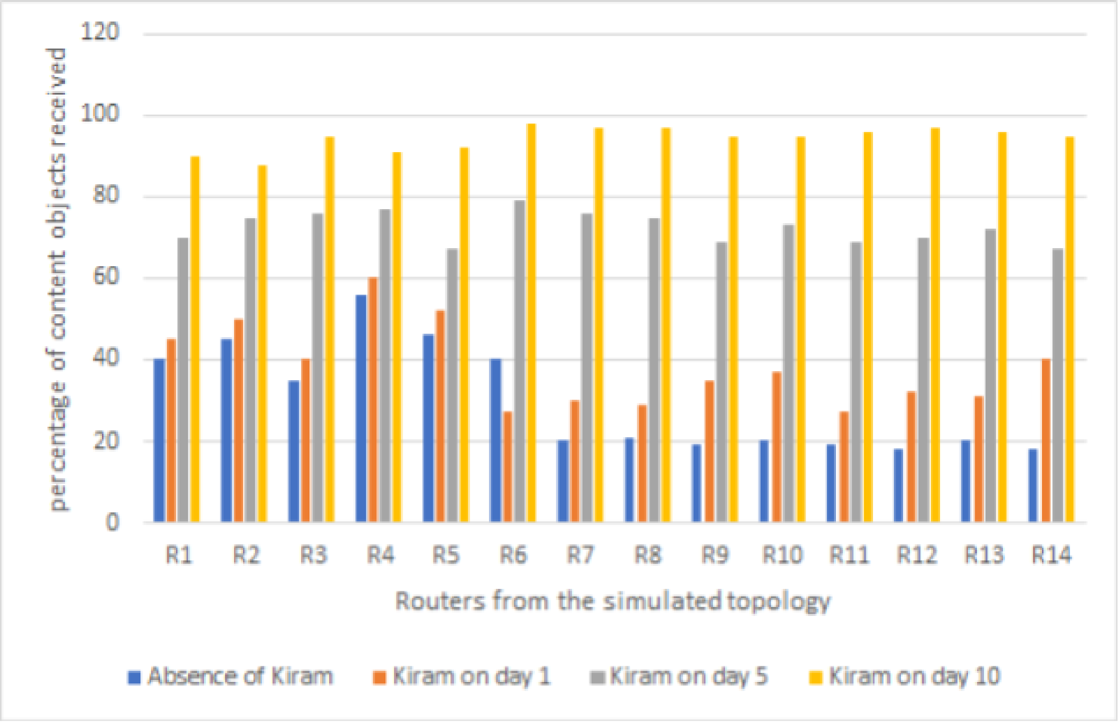


Figure 2.6: Kiram performance over time

2.4 The DDoS defence duo: Kiram and WOE

2.4.1 Kiram: An intelligent interest flooding detection, mitigation, and prevention mechanism

Kiram is our proposed framework consisting of algorithms that utilize the fundamental NDN principles, as well as intelligent learning mechanisms, and improvised computations for anomaly detection. The distinguishing feature of Kiram is that in addition to the time-interval based interest accumulation and previously introduced Pushback [61] techniques, it also utilizes intelligent learning and computation. The unique anomaly detection mechanism distinguishes Kiram from the previously proposed anti-DDoS solutions for CCN. This mechanism enables the passive monitoring of all traffic over time to first establish a normal (baseline) network behaviour/traffic pattern and then compare the ongoing traffic with it.

Kiram utilizes individual (node) and cumulative (network) knowledge-base as well as collaborative learning to prevent unknown/zero-day attacks. The normal traffic baseline is updated incrementally using individual and collaborative router statistics. According to the intrinsic NDN functionality, a content object follows the reverse path of an honest interest. Following this principle, an honest interest will result in the corresponding returned content. Kiram maintains the interest satisfaction portfolio for each incoming interface, outgoing interface, and per-name prefix and then compares it to previously generated baselines (from honest interest traffic patterns).

Following anomaly detection, Kiram mitigates the effects of the attack by limiting the interest rates on the affected interfaces. It then generates WOE (Warding Off Evil) alerts at the first layer of defence, i.e., the first router that experiences a flooding of the PIT. WOE also provides a feedback loop into Kiram's intelligent learning mechanism resulting in a collaborative and proactive defence system.

Kiram is a set of algorithms running on routers. It identifies an anomaly using an established normal traffic pattern baseline. It then compares the baselines statistics to the statistics recorded during the onset of an adversarial attack including expired interests, their corresponding namespaces, and their in and out interfaces.

The next logical step after anomaly detection is to limit the interest acceptance at the affected interface(s) as proposed in previous research works [22] [61] [79]. However, Kiram does not stop at this step. It also generates WOE alerts as described next.

[1] The sink-holed traffic is usually used for analytical learning and the black-holed traffic is discarded.

2.4.2 WOE (Warding Off Evil) real-time alerts

The second step is the WOE alert dissemination in the form of a content message. Content Centric Networks are intrinsically characterized by the information exchange principle of one request per packet. It has been argued by Tsilopoulos et al., that for diverse types of traffic such as real-time streaming, one request per packet can neither be adequate nor efficient [118]. Analyzing diverse traffic types is beyond the scope of this thesis. However, it is noteworthy that to enable the efficient dissemination of information for optimum CCN performance, different mechanisms must be employed for different scenarios. An adversarial DDoS attack through interest flooding is one such scenario.

We augmented upon the concepts of *Reliable Notifications* and *Persistent Interests* presented by Tsilopoulos et al. [118] for the use-case of real time documents. Instead of using these concepts for the regular content objects, we used them for the WOE alert which is disseminated as a content packet. As argued by Compagno et al., it is recommended to send WOE as a content packet belonging to a reserved namespace [45]. First of the three logical reasons for sending WOE as a content message is the full PIT in the next hop router which may result in discarding of WOE alert, preventing it from reaching the intended and affected victims. Secondly, the content message is signed by the producer and hence is a more reliable source of sending an alarm compared to an interest message. Thirdly, the alert message may be cloned by the adversary as a fake interest and used as an additional weapon during an ongoing DDoS attack.

Based on the idea of "self-certifying alerts" for malware detection and containment introduced by Costa et al. [49], we can sign the WOE alert content message with a link to a description of the warning or alert. This tactic is aligned with our strategy of intelligent anomaly detection in which WOE acts as a real time warning, as well as a future prevention tool by contributing back to the Kiram knowledge-base.

Router r_x (where r denotes the router and x denotes the particular interface of that router for routing of the interest or content message under observation), receives a packet ($cont1$) and processes it as detailed in Algorithm 1. A persistent interest flooding attack on router r_x causes it to send multiple alert messages towards the source(s) of the attack. Such sources will decrease their thresholds Γ^x and δ^x until they detect the attack and implement rate limiting on the malicious interests. If no attack is reported for a predefined amount of time, thresholds are restored to their original values.

This push-back mechanism allows routers that are not the target of the attack, but are unwittingly forwarding malicious interests, to detect interest flooding early. In particular, alert messages allow routers to detect interest flooding even when they are far away from the intended victim, i.e., close to nodes controlled by the adversary, where countermeasures are most effective.

Algorithm 1 Processing data message and WOE alert ω_t^x

Input : Incoming packet cont1 from r_x, waittime, Γ^x (interest rate-limiting threshold), δ^x (threshold discerning between normal vs abnormal PIT size for interface x), Alert message ω_t^x from interface x.

```
if cont1 is ContentObject then
    process cont1 as ContentObject and return
if cont1 is $\omega_t^x$ then
    Verify (cont1.signature)
      if IsFresh (cont1) and time from last Alert received from $r_x$ > waittime then
          Decrease $\Gamma^x$
          Decrease $\delta^x$
else   drop message (cont1)
if cont1 is interest then
      if $\mu_a^x$ is > $\Gamma^x$ and $\rho_{at}^x$ is > $\delta^x$  then
          drop message
      if time from last Alert sent on interface x > waittime then
          send alert $\omega_t^x$ to $r_x$
else process cont1 as interest
```

2.5 Evaluation

We used ndnSIM [22], the open source NS-3 based NDN simulator for simulations to evaluate the effectiveness of our proposed framework. While in the future, NDN may lead to different topology networks, it is hard to predict what those would look like. So for now using standard baseline comparison networks such as the AT&T and DFN (German Research Network) [75] could safely be assumed as the best practice. AT&T and DFN network topology networks were chosen for keeping the simulations realistic.

2.5.1 Assumptions

The following assumptions are used in our evaluation:

(a) Kiram is implemented on all NDN routers in the system under evaluation for both AT&T and DFN topologies used for simulations.

(b) The NDN routers are not compromised by the adversary during the Interest Flooding DDoS attack.

(c) In our simulations we assumed that all users send their Interest packets at constant average rates with randomized time gap between two consecutive Interests, because this traffic pattern provides a reasonable approximation of traffic mix from all users without excessive buffering. The content distributions of each legitimate user and attacker follow Zipf-Mandelbrot distribution [92] and uniform distribution respectively, which have been implemented in the latest ndnSIM module.

(d) All NDN routing features are functional on the routers, implying that the NDN routers can easily keep track of unsatisfied (expired) interests and use this information to limit the following:

   i. The number of pending interests per outgoing interface: NDN keeps flow balance between interests and content. For each interest sent through a particular path, at most one content satisfying that interest can flow in the opposite direction on the exact reverse (return) path. Based on that property, each router can compute the maximum number of pending interests per outgoing interface that the return connection can satisfy before they time out. Thus, a router should never send more interests than an interface can satisfy, based on average content package size, timeout for interests and bandwidth-delay product for the corresponding link.

   ii. The number of interests per incoming interface: Using the same flow balance principle, a router can easily detect when a consumer is sending too many interests that cannot be satisfied due to the physical limitations of the link.

   iii. The number of pending interests per namespace: When a certain prefix is under attack, intervening routers can easily detect out-of-proportion numbers of unsatisfied interests in their PIT for that prefix. Thus, routers can limit the total number of pending interests for that prefix and block the incoming interface(s) which has sent too many unsatisfied interests for that same prefix.

(e) In a real life Interest Flooding DDoS attack, the adversary may be able to poison the cache contents of routers, thus launching a simultaneous content poisoning attack, which is also discussed in the next chapter. Additionally, in a real life scenario, various types of DDoS attacks mentioned earlier in Section 2.2 may be launched alongside an IFA. However, we are only simulating Interest Flooding DDoS attacks in isolation to ensure a thorough evaluation of the proposed mitigation technique. The assumption that only the interest and not the content messages can be tampered with by the adversary, also allows us to share the WOE alert as a content message, ensuring that it is signed and cannot be compromised unlike the fake interest messages.

2.5.2 Simulations

The DFN topology as depicted in Fig. 2.3 had 16 Consumers and 30 NDN routers. To check the sensitivity and accuracy of the results, we varied the number of Producers from 1 to 5, number of Consumers and observed routers from 10 to 20, and the number of adversaries from 1 to 5. The sensitivity analysis showed that 5 Producers, 14 honest routers, 14 honest consumers and 3 Adversaries was the optimum number to effectively showcase the successful results of the experiments. Therefore, these were the selected numbers finally used and reported in the results. Based on the same practise of showcasing the results in the most optimum way, the simulation system for the AT&T set up included 5 Producers, 14 Honest Consumers and 3 Adversaries. Results in Fig. 2.6 are displayed using an average from the AT&T and DFN topology network simulations. The producers are denoted by P_n. The honest routers are denoted by R_h and the honest consumers are denoted by C_h. The adversaries are A_1, A_2 and A_3.

The first set of simulations was used to verify the effects of an adversarial attack. For this purpose the initial simulations were run on the AT&T and DFN network topologies separately using ndnSIM with no adversarial activity. In the next set of simulations for both AT&T and DFN network topologies, the adversaries A_1, A_2 and A_3 start generating fake interests. The initial set of experiments endorsed the idea that successful IFA DDoS attacks can be easily carried out using very small amounts of bandwidth. PIT usage was significantly affected during an IFA attack as illustrated in Fig. 2.4 and Fig. 2.5. During the attack, several routers were impacted significantly depicting an average of 27% (ranging from 18% to 64% depending on the routing distance from adversarial activity) of the regular routed traffic throughput.

The parameters were varied based on the **sensitivity analysis** carried out during each set of simulations. Each variable was varied independently (one variable changed while others remained constant) in ascending order. For example, to evaluate the Γ^x rate-limiting threshold calculated by $\mu_h^x : \mu_a^x$ was varied from 0.1 to 0.2, 0.3,0.4,...up to 1.0 as the DDoS attack becomes aggressive and then the mitigation through Kiram becomes effective overtime. We argue that neither increasing Γ^x, nor computing μ_h^x or μ_a^x over longer intervals, produces the indented effects. In fact, in the first case the bound must be set high enough to avoid classification of short burst of interests as attacks; however this could inevitably lead to late or non-detection of actual attacks. Increasing the size of the interval over which Γ^x is computed may reduce the sensitivity of Kiram to short burst of interests. An interval length similar or longer than the average round-trip time of interest/content packet, in-fact, may allow (part of) the content requested by the burst to be forwarded back, reducing μ_a^x to a value closer to 1. However, this could significantly increase the detection time. Instead, to improve detection accuracy (distinguishing naturally occurring burst of interests from attacks), Kiram also takes into account δ^x. This value measures the PIT space used by interests coming from a particular interface x. This allows Kiram to maintain the number of false positives low – when compared to considering solely μ_a^x, while allowing it to detect low-rate interest flooding. In a low-rate interest flooding attack, the adversary limits the rate of fake interests to keep μ_a^x below its thresholds. Monitoring the content of the PIT allows Kiram to observe the effects of the attack, rather than just its causes, allowing for early detection.

To sum up, different parameters monitored by Kiram act as weights and counter-weights for interest flooding detection. When a router is unable to satisfy incoming interests over a relatively short period, ρ_{at}^x may exceed the detection threshold but μ_a^x will not; when the router receives a short bursts of interests, μ_a^x may become larger than Γ^x but the PIT usage will likely be within normal values. To stay undetected, an adversary willing to perform interest flooding must therefore: (1) reduce the rate at which it sends interests, which limits the effects of the attack; and/or (2) restrict the attack to short burst, which makes the attack ineffective. Thresholds ρ_{at}^x and Γ^x are not constant and may change over time to accommodate different conditions of the network. The time interval and the results which showed maximum variation in the results were reported. Each simulation was carried out 20 times initially, and after calculating averages for regular intervals of simulation repeats i.e. 5, 10, 15, and 20 times, it was observed that 15 was an optimum number of simulations to report consistent results effectively. Hence for all experiments, each simulation was carried out 15 times and the average results are represented in Fig. 2.6.

All routers used in the evaluation implement Kiram. Once a router detected an adversarial IFA from one or more interfaces using baseline comparison, the interest acceptance from the suspicious interface(s) was restricted. Kiram's ability to learn the normal traffic patterns over time is directly proportional to the extent of learning time. This hypothesis is proven by extensive simulations of an adversarial attack first in the absence and then in the presence of Kiram, on day 1, day 5, and day 10. For evaluation, the adversarial interference was only carried out on days 1, 5, and 10. The time period in between was used by Kiram on an average of twelve hours per day for ten days to build up the intelligent learning information. Kiram utilizes the normal/honest interest rates, interface, and namespace information to establish the normal baseline. Baseline comparison is carried out in addition to the per incident and per interface parameters such as size of PIT, rate of interests (for a given time interval), and variation of interest magnitude during two time intervals, etc. Kiram improved the throughput during an effective DDoS attack to an average of 38.2% on day 1, 72.5% on day 5 and 94.4% on day 10. These results clearly show that the Kiram and WOE duo provides a solid defence against DDoS attacks in NDN and improve the network availability substantially.

Additionally, the temporal learning capability reduces the probability of false positives by recognizing the common network occurrences such as packet loss, non-adversarial congestion, and hardware and software errors. Kiram detects attacks by using the parameters listed in Table 2.1. All of the parameters (except thresholds which are calculated based on the comparison between honest/normal and adversarial/abnormal traffic data) have two sets of values for any interface at any given time. One is the honest traffic behaviour representation (depicted by subscript `h`) and the other is the adversarial or fake interest representation (depicted by subscript `a`).

2.6 Conclusion

Kiram offers intelligent anomaly detection by learning normal traffic patterns to establish a baseline. In the advent of an adversarial interest flooding DDoS attack, it mitigates the effects by limiting interest rates on affected interfaces and generates WOE alerts to neighbouring routers as a collaborative countermeasure. Kiram amalgamates a novel intelligent temporal learning capability with traditional DDoS mitigation techniques such as PIT saturation monitoring, interface rate-limiting, namespace book-keeping and alert generation. WOE alerts from neighbouring routers also provide feedback loops into Kiram. Extensive simulations show significant improvement in Kiram's effectiveness over time. Kiram and WOE could prove to be front-runners in future work to mitigate DDoS attacks in CCN/NDN.

In this chapter the focus was on IFA DDoS attacks. Some other DDoS attacks such as Bandwidth Depletion attack, Reflection attack and Black-holing prefix-hijacking are mentioned in Section 2.2. For future work we can run ndnSIM simulations for these attacks as well as do real life testing for Kiram for IFA DDoS attacks. Since Kiram is a temporal learning mechanism, a larger network and longer learning time may reveal further benefits of this approach. Further work can also be done to equip the alert message called WOE with more effective and meaningful information.

In this chapter we discussed the DDoS attacks in CCN as a threat to availability of content/data and presented Kiram as a defence mechanism. The next chapter addresses the second component of the AIC triad i.e., integrity of content/data/information in CCN.

Chapter 3

Integrity in CCN- Content poisoning and its mitigation

The previous chapter discussed the availability in CCN and presented Kiram as a defence mechanism against DDoS attacks. This chapter considers the second component of the AIC triad, i.e., integrity of content/data/information in CCN, by addressing the challenge of content poisoning and proposing its mitigation through a novel solution named Iris.

As discussed previously in Chapter 1 Section 1.5, integrity [7] is the assurance that the information is trustworthy and accurate. This definition also clearly shows the strong interdependence of availability, integrity, and confidentiality of information upon each other. When an adversary attempts to compromise the integrity of data, she tampers with the data to corrupt it enough to either make it useless for the user or useful to herself for malicious purposes such as injecting a worm or trojan or providing false information for social/political gains such as propaganda.

3.1 Content poisoning

As previously discussed in Section 1.4 of Chapter 1, NDN routers maintain Content Stores (CS)s to enable efficient distribution of popular content through caching. This caching is a key CCN feature that reduces latency, improves bandwidth utilization, and ensures swift content delivery. However, content caching is susceptible to content pollution, content poisoning, and content snooping attacks [96]. *Locality disruption* [52] attacks continuously generate requests for new unpopular files, thus ruining the cache file locality. *False locality* attacks [52] repeatedly request the same set of files, thus creating a false file locality at proxy caches. It is noteworthy that through the injection of fake content, the adversary can achieve much more: the adversary may inject fake content to build a false locality as a large storage network to store junk and malicious content such as malware and trojans, etc.

3.2 Related work

A big share of CCN security research done so far has focused on Denial-of-Service attacks [63] [45]. However, cache poisoning also known as cache pollution attacks pose an equal, if not a greater challenge for the NDN architectures. Content poisoning is an attack during which an adversary injects *fake* (junk or planted on purpose) content into the NDN network with the intent of polluting the router caches. First, such attacks are stealth in nature, i.e., they are capable of degrading overall network performance without flooding network resources. Second, they possess a dangerous level of indirection, i.e., while both consumers and CS are affected by the attack, neither consumers nor CS are directly attacked. Third, they pollute the cache with unwanted content, which appears to be harmless as it is either simply useless or is skilfully hiding malware, making these attacks much harder to detect. Finally, no counter-poisoning mechanisms exist in internet caches; thus, even simple, brute-force poisoning attacks can be quite successful.

While some caching systems do apply simple mechanisms to mitigate the effects of unintentional cache poisoning, such mechanisms are fundamentally limited in their ability to thwart systematic, and intentional poisoning attacks. While being much more effective, such attacks are much harder to detect. CCN Cache poisoning/pollution attacks are investigated by Xie et al. [127] and CacheShield is proposed as a proactive mechanism. Conti et al.'s work [48] proves the inefficacy of CacheShield against realistic adversaries. Our work addresses the limitations of CacheShield by proposing a realistic defence mechanism that identifies and mitigates a systematic content poisoning attack from a realistic adversary in a fairly realistic topology. Moreover, in contrast with Ghali et al. [66] using a ranking system for unsatisfied or rejected content for exclusion, and Mauri et al. [94] proposing a honeypot mechanism for blacklisting fake content, we propose a more evolved, improvised, and intelligent framework called *Iris* that uses the concept of reverse attribute based encryption in addition to the traditional exclusion and honeypot techniques.

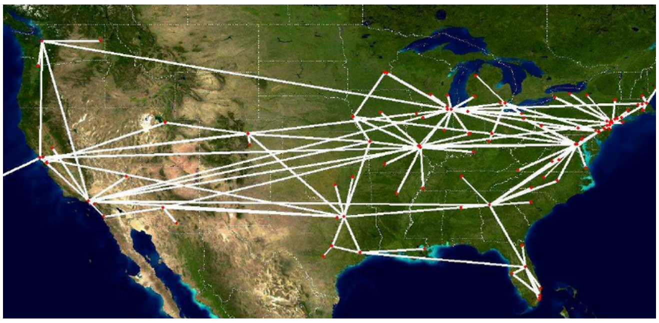


Figure 3.1: AT&T Network Topology (AS 7118) from the Rocketfuel data bank for the continental US.

3.2.1 Fake content and fake signatures

A *fake* content is a content injected by an adversary with malicious intention. Ghali [66] identifies a fake content as one having a fake signature. A **fake signature** is a content signature with any one of the following characteristics:

(a) It maybe an invalid signature.

(b) It maybe a valid signature with a key not belonging to the producer.

(c) It maybe an ill-formatted signature.

3.3 Evaluation

For this thesis, we examined a planned content poisoning attack in which an adversary infers the interests for content names and injects fake content of the same name in the cache.

To quantify the effectiveness of our proposed framework named Iris, ndnSIM [22], the open source NS-3 based NDN simulator was used for simulations.

3.3.1 Network topologies

We used the AT&T (AS 7118) [37] from the Rocketfuel data bank and DFN topologies for the ndnSIM simulations. One of the reasons for choosing AT&T and DFN topologies was that whereas NDN may lead to different topology networks in future, it is hard to predict what those would look like. Hence, using standard baseline comparison networks such as the AT&T and DFN can be safely assumed as the best practice for now. Secondly, we chose these topologies to keep the simulations realistic. Following are some definitions of the entities used in our experiments:

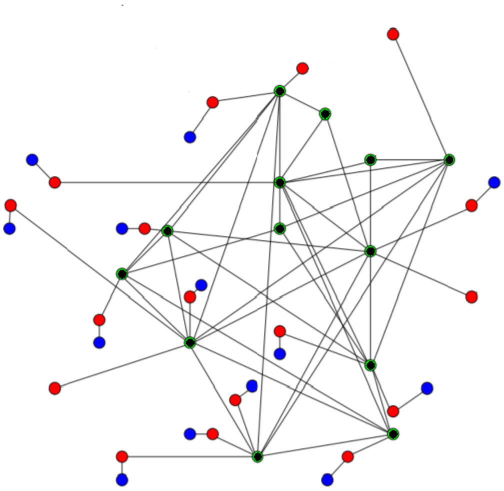


Figure 3.2: DFN Network Topology. Red dots depict edge routers, blue are consumers, and green are core routers

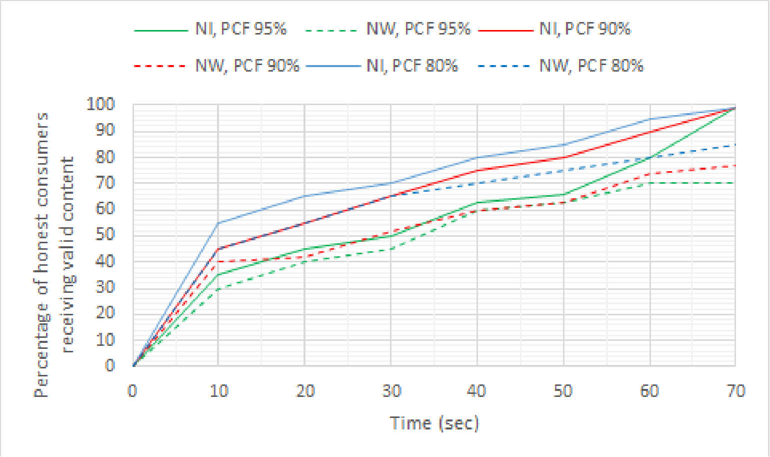


Figure 3.3: DFN Topology results with different rates of pre-populated fake content objects (NW: NDN without Iris, NI: NDN with Iris, PCF: % of pre-populated fake content objects)

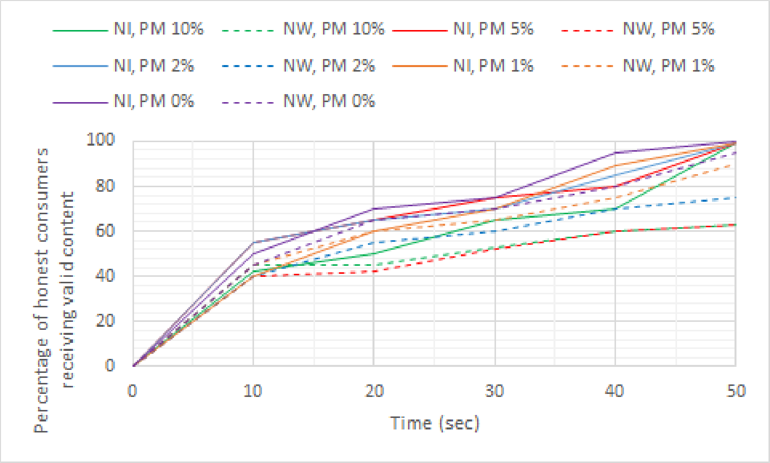


Figure 3.4: DFN topology results with different rates of malicious consumers and 99% pre-populated fake content objects (NW: NDN without Iris, NI: NDN with Iris, PM: percentage of malicious nodes in the consumer population)

(a) An adversarial producer is a producer that generates fake content and injects it in the NDN network. For our experiments, we consider an adversary which is capable of creating a false locality with an ultimate goal to poison the end user storage. The adversary has the capability to compromise a number of consumer nodes and use them to request the fake content objects.

(b) An honest consumer is not satisfied with the fake content object. An honest consumer would exclude the name of the fake content and Iris keeps the log for this exclusion. Also, an honest consumer stops sending the relevant interest messages once the required valid content is received.

(c) A compromised consumer acts on behalf of the adversary. The compromised consumer would exclude the interests returning valid content and would request fake content.

The DFN topology as depicted in Fig.3.2 had 16 consumers and 30 NDN routers. To check the sensitivity and accuracy of results, we varied the number of observed producers from 1 to 5, number of observed honest consumers and observed routers from 10 to 20, number of compromised consumers from 1 to 10, and the number of adversaries from 1 to 5. The sensitivity analysis' showed that 5 honest producers, 14 honest consumers and 6 compromised consumers controlled by one adversarial producer were the optimum system parameters to effectively showcase the successful results of the experiments. Hence, these were the selected numbers finally used and reported in the results. The one adversarial producer is denoted by P_A. The honest producers are denoted by P_x, where x varies from 1 to 5. The routers in the AT&T and DFN topologies are denoted by R_n where n varies from 1 to 132 for AT&T and 1 to 30 for DFN.

The honest consumers are denoted by C_{hm} where m varies from 1 to 14. We use C_{h5} and C_{h12} as Monitored Consumers (MCs) to observe network behaviour through the experiments. Compromised consumers controlled by the P_A are denoted by C_{A1}, C_{A2}, C_{A3}, C_{A4}, C_{A5}, and C_{A6}.

F is a set of fake content objects that is injected in the network by P_A.

In a real-life content poisoning attack, the fake content may originate from multiple sources. However, for the sake of experimental simplicity, we simulated an attack using only one adversary.

3.3.2 Sensitivity analysis

Since there are various variables involved in our evaluations, we used a sensitivity analysis technique. This technique was based on keeping all variables except one constant at any given time to determine the impact of changing values of that specific variable over a range of values. This variation allowed us to determine the optimal value range that best demonstrated the impact of changing values of one specific variable. This process was repeated for every variable that we have evaluated.

For example, in the simulations discussed in this chapter, the percentage of prepopulated fake content objects, number of honest consumers, percentage of malicious nodes in consumer population, the number of routers to be monitored, and the number of adversarial producers, etc., were all subjected to this sensitivity analysis to determine the optimum range of variation in values to be reported.

3.3.3 Simulations

The first set of simulations was used to verify the effects of an adversarial attack. For this purpose, the simulation was initially run on the AT&T and DFN topologies using ndnSIM with no adversarial activity. In the next set of simulations, P_A generated fake content. Initially the simulations were carried out 10 times (as that has traditionally been the minimum number of simulation sets in ndnSIM experiments). From 10 to 20 simulation sets, it was observed through sensitivity analysis that 14 simulations were the optimum number of simulations to report the results most effectively. Hence, each simulation was ultimately carried out 14 times and the average results were obtained by monitoring C_{h5} and C_{h12}. Table 3.1 shows the topology parameters, whereas the simulation results are depicted in Fig. 3.2, Fig. 3.3, Fig. 3.4 for DFN topology and in Fig. 3.5 for AT&T topology.

3.3.4 Iris: Cure for content poisoning

Iris helps classify a content as fake by utilizing an attribute based classification. This attribute of a content being **fake** is determined using the following four thresholds with priority high to low, with (a) being the highest and (d) being the lowest:

(a) A content is most likely to be classified as *fake* if it has fake signatures. A signature can be declared fake based on the criteria described earlier in Section 3.2.1, i.e., it may be 1) an invalid signature, 2) a valid signature with a key not belonging to the producer, and/or 3) an ill-formatted signature.

(b) A content can be declared *fake* if it has a high dissatisfied interest count. (In this evaluation we varied the dissatisfied interest counter from 5 to 13).

(c) A *fake* content object may also be identified by the idle time it spends in the cache.

(d) Once a fake content is identified along with its corresponding adversarial producer P_A, the content's reappearance from P_A can also be used to establish the attribute again after some time has lapsed. This is the lowest priority criterion, as it would only be evident once the content poisoning attack has been detected and monitored to be effective for some time. Moreover, detecting the original adversarial producer and retaining that information over time requires greater router overhead.

3.3.5 Multi-Authority Attribute Based Encryption (MA-ABE)

Based on the nature of most NDN architectures, it is difficult to agree on a single trusted authority that issues attributes for all the users. Therefore, Iris' second level of defence against content poisoning attacks is based on multi-authority attribute based encryption (MA-ABE) [87]. MA-ABE decentralizes the trust by allowing several independent authorities to issue decryption keys corresponding to different attributes. This allows maximum flexibility as required by the NDN architecture. The reason we applied the MA-ABE concept in reverse for Iris is because every node in the network chooses its trusted authorities before it joins the network. The initial trust relationship between a node and its authorities is established by default. We can assume two scenarios:

(a) In the first scenario, MA-ABE is already in place, i.e., the nodes initially establish an out-of-band trust by exchanging secret keys. In this scenario, Iris can revoke the key of identified adversarial producers or compromised consumers.

(b) In the second scenario, where the trust relationship is not established, Iris can perform the identification and exclusion based on the criteria listed above. Once a producer and compromised nodes are identified, access to content can be restricted by using the attribute qualifying the producers and consumers as honest by virtue of lack of the *fake* attribute.

3.3.6 Iris in action

(a) The first step in content poisoning mitigation is to evaluate the content and classify it as fake based on the criteria mentioned in Section 3.2.1 and specified in the below mentioned Algorithm 2 as Conditions 1 to 4.

Conditions for adding attribute *f* (fake) to content c_x and corresponding interest i_x are the following:

Condition 1: Content has an invalid signature, a valid signature with a key not belonging to the producer, and/or an ill-formatted signature.
Condition 2: Content's dissatisfied interest count $\geqslant 5$.
Condition 3: Content's idle time $\geqslant 15$ sec.
Condition 4: Content's reappearance from P_A within 10 sec of being dropped as idle from PIT.

Algorithm 2 Attribute addition and response for fake content

Input : Condition 1 *or* Condition 2, Condition 3 *and* Condition 2
Output : forward message or drop message and log P_A, interface and δ

```
if Condition 1 =true $\vee$ Condition 2 =true
 then
    check for Condition 3 and Condition 4
    if Condition 3 $\wedge$ Condition 4 = true then
        $c_x = c_h$ and $i_x = i_h$
        forward message
else
    if $c_x = c_f$ and $i_x = i_f$ then
        drop message return log $P_A$,
    update interface and $\delta$
```

(b) The second step is to mitigate the ongoing compromise by adding the attribute *fake* to the corresponding relaying interface(s).

(c) The third step is to identify the compromised consumers, and eventually the adversarial producer, and revoke the access keys for these nodes.

Table 3.1: ndnSIM AT&T and DFN Topology Parameters

Parameter	AT&T simulations	DFN simulations
No. of C_h	14	16
No. of R_n	132	30
No. of P_A	1	1
No. of P_x	5	5
No. of simulations	14	14
Simulation time [sec]	300	300
Fake content rate injection	0% to 70% in 5% intervals	0% to 70% in 5% intervals
No. of C_A	6	6
No. of MCs	2	2
C_A rate	0%, to 30% in 5% intervals	0%, to 30% in 5% intervals
Interest interval [millisec]	[100,300]	[100,300]

It is noteworthy that until a content poisoning attack is detected (based on the presence of fake content identified using the criteria mentioned earlier), the content producers determine the access control policy. Once a content poisoning attack is detected, Iris acts as a function that accepts a consumer identity and the associated attribute and outputs *honest* denoted by h if the consumer satisfies the input attribute (i.e., absence of the attribute *fake* denoted by f). The presence of attribute f confirms that the customer is requesting fake content and/or the producer is relaying fake content. In other words, Iris starts functioning as the access control provider by managing and relaying the access control policy.

Iris was implemented on all nodes used in the evaluation for both AT&T and DFN topologies. Once a node detected the existence of a content poisoning attack based on the relaying of fake content objects from one or more interfaces, the countermeasure Iris is activated as depicted by Algorithm 2, mitigating further propagation of fake content.

3.3.7 Significance of the results

As described in the earlier Section 3.3.3, the initial set of simulations was run to establish the impact of an active content poisoning adversarial attack. These initial simulations proved that a successful content poisoning attack, if left unchecked, results in a significant increase in the adversarial producer's activity and the percentage of fake contents received by the honest consumers, as depicted in Fig. 3.5 for AT&T topology and Fig. 3.3 and Fig. 3.4 for DFN toplogy.

After establishing the impact of the adversarial content poisoning attack without any mitigation, the next set of simulations was carried out by implementing the

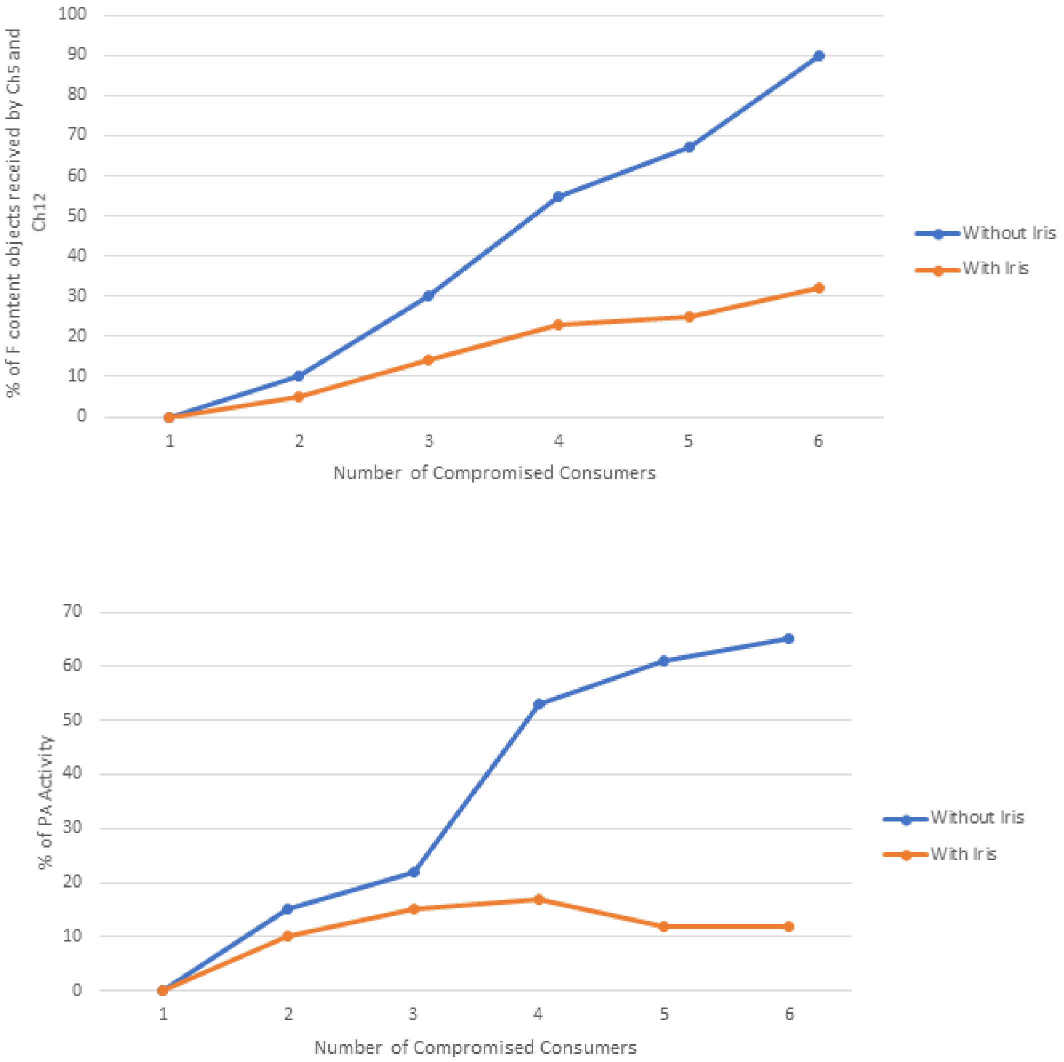


Figure 3.5: Evaluation results for Iris simulations on AT&T topology

proposed solution, i.e., Iris. Both AT&T and DFN topologies were again used for these simulations.

As depicted in Fig. 3.3, once Iris was implemented on all nodes in the simulations for the DFN topology, the fake content objects were detected as soon as the percentage of compromised consumers increased beyond 30% on average, while percentage of pre-populated fake content objects (denoted by PCF) was varied from 80% to 95% with increments of 5% each time (a difference determined by the sensitivity analysis as mentioned in Section 3.3.2).

In another set of simulations depicted in Fig. 3.4 for DFN topolgy, the percentage of malicious nodes (denoted by PM) was varied from 0% to 10%, with and without Iris, which showed significant mitigation of fake content object propagation by Iris, specifically when percentage of fake content received by honest consumers rose above 20%. The maximum mitigation is seen when the fake content objects' percentage rose above 40% (on average) depending on the varying percentage of malicious consumers and a 99% injection rate of pre-populated fake content objects As depicted in the Fig. 3.5, NW denotes NDN without Iris, NI denotes NDN with Iris, and PM denotes the percentage of malicious nodes in the consumer population.

Once Iris was implemented on all nodes in the simulations for the AT&T topology, the fake content objects were detected as soon as the number of compromised consumers increased beyond 3 and fake content objects' percentage rose above 20% as illustrated in Fig. 3.5.

These numerical results from simulations run on both AT&T and DFN topologies clearly demonstrate that the proposed framework Iris provides a solid defence mechanism against systematic adversarial content poisoning attacks in NDN and substantially improves the network availability.

3.4 Summary

In this chapter we explored the content poisoning attack in NDN and its mitigation through a proposed framework named Iris. We amalgamated and improvised upon the honeypot and exclusion techniques and introduced the reverse MA-ABE technique in Iris. Using these techniques in an intelligent framework, Iris detects the fake content objects, identifies, and isolates the compromised consumers, and eventually, the adversarial producers. We used AT&T and DFN topology simulations over ndnSIM and demonstrated the effectiveness of Iris through extensive simulations.

Future work in this area includes extension of trust federations in Iris and its implementation in other CCN networks. Moreover, we continue to pursue the scalability of Iris through large scale deployments.

Integrity preservation of content in CCN (through mitigation of adversarial content poisoning) was explored in this chapter. The next chapter presents a solution to ensure data confidentiality from a content name privacy perspective.

Chapter 4

Confidentiality in CCN- Name privacy protection

The previous two chapters presented potential solutions to 1) ensure availability and 2) protect the integrity of information in CCN. This chapter addresses the third and final component of the AIC triad, i.e., confidentiality of content/data/information in CCN.

Based on the"*security by design*" principle and our learning experiences from the current Internet architecture, it seems imperative that we amalgamate necessary security provisions in the nascent stages of the CCN architecture development. Undoubtedly, confidentiality has always been the most researched field of the AIC triad. As described earlier in Chapter 1 Section 1.5, confidentiality [7] stands for a set of directives that prevent the exposure of data to unauthorized parties by governing and limiting access to it. The core idea that makes confidentiality exciting and relevant to a wide variety of audience ranging from a computer scientist to a common internet user is "privacy". Privacy is an integral aspect of confidentiality.

Privacy by design [85] is a technological design framework [74] and is a natural extension of security by design. Privacy by design ensures that the internet architecture is designed and developed with built-in privacy considerations, instead of privacy being an afterthought.

As discussed in the previous chapters, CCN/NDN's named-content based design makes it vulnerable to threats such as DDoS [20, 88], cache poisoning [83, 67, 106], cache pollution [102, 94], timing-based side channel [40, 18, 47], censorship, and anonymity attacks [29, 56, 60, 53, 40, 86]. In spite of the remedies such as secure naming, routing, and forwarding [125, 23, 107], privacy vulnerabilities caused by the name-to-content binding and pervasive caching features of NDN are still a massive challenge [69, 68, 19].

In NDN, name privacy is an important issue since the default structure of NDN works based on content names which are human readable and reveal plenty of information about the requested content and users' interests. The name of a content can be used as a highly acclaimed piece of sensitive information (of political, religious, and social interest) by an adversary. This information can also be exploited for user profiling to enforce censorship or pursue advertisement objectives.

Encrypting each NDN message is a promising approach for preserving name privacy in NDN. However, a naive adaptation of encryption obviates the benefit of caching. Although several previous studies [33, 126, 40] addressed the problem, they suffer from either information leakage because of weak privacy protection or inefficient routing and inability to use pervasive caching features because of strong privacy protection. To overcome these contradictory problems, we introduced a new two-layer privacy protection mechanism which is based on the users' choice of privacy level. In the first layer of protection, names are encrypted using Message-locked encryption (MLE) [32], which obfuscates sensitive and human readable names from NDN messages. However, simple adaptation of MLE may enable adversaries to link identical obfuscated names to a specific user or group of users by side-channel attack (because encrypted names would be the same if the original names are the same). To overcome this problem, the encrypted name from the first privacy protection layer is re-encrypted and delivered using onion routing [116]/ gateways in the second layer. Thus, adversaries are prevented from linking the requests (names) to the specific users.

However, the encryption layers may impose extra burden on the users and networks especially for data that is not sensitive for the users. It must be noted that there is a certain cost associated with obfuscation, encryption, decryption, and routing etc., as with any privacy protection technique. Therefore, the user must be able to decide to accept this cost depending upon the sensitivity level of information (e.g., the risk posed by the discovery of her potential association with the desired content by an adversary). User's selected privacy protection level(s) may or may not include the first and/or second layers of encryption. The user's choice is based on sensitivity of data and determined by game theory application. Using game theory, the user determines the optimum level of privacy by balancing/trading off the desired level of privacy with the utility cost.

The main contributions described in this chapter are summarized below:

(a) The proposed protection method considers information leakage for a name as well as correlation between two similar names.

(b) We considered two layers of privacy protection to provide granular and bespoke name privacy for NDN users. The first layer of protection prevents information leakage (deducible from the content name) using MLE based name obfuscation. The second layer of protection avoids linkage between two similar names and users by using gateways and onion routing.

(c) The hierarchical structure of the name is preserved and the ubiquitous in-network caching is used along with the proposed privacy protection.

(d) User controlled privacy protection is determined based on game theory to optimize utility cost against privacy.

(e) Scalability is duly considered to ensure that the proposed approach works equally well on real-world large scale network topologies.

4.1 Related work

With pervasive eavesdropping and monitoring now being considered a serious threat [58] and the growing increase in large-scale network packet interception by unauthorized entities, privacy must be a necessary feature for emerging protocols. To counter such privacy threats, ubiquitous and opportunistic encryption protocols are being standardized for IP-based protocols such as TCP and DNS, etc. [34] [130] [35]. However, there are few works aimed towards this goal in NDN. NDN privacy concerns can be broadly categorized into three domains, namely 1) user/consumer privacy, 2) producer privacy, and 3) content cache privacy. Different kind of attacks such as naming, monitoring, censorship, and timing attacks can endanger the privacy of users and providers [117]. The name of the requested messages (interest messages) can itself reveal ample information about the content that a user has requested and hence endanger users' privacy. Therefore, in this thesis, we concentrate on users' privacy with the perspective of content name privacy which is a significant issue in NDN. Since the proposed name privacy protection is based on convergent encryption, we review the previous name privacy methods in NDN and then discuss the convergent encryption based methods, which are used in cloud database.

4.1.1 Name privacy in NDN

Using obfuscation [74] as a privacy mechanism, the privacy and utility experience of a user are at odds with each other. Utility loss due to obfuscation can be termed as the degradation of the user's service-quality expectation resulting from sharing obscured data which needs processing time to reveal the actual data.

There are two noteworthy metrics proposed in privacy literature. **Differential privacy** limits the information leakage through observation. However, it does not reflect the absolute privacy level of the user, i.e., what actually is learned about the user’s secret. **Distortion privacy** (inference error) metric overcomes this issue and measures the error of inferring user's secret from observation. This requires assumption of a prior knowledge which enables quantification of absolute privacy, but is not robust to adversaries with arbitrary knowledge. Hence, neither of these metrics alone is capable of providing adequate privacy.

As pointed by Ghodsi et al. [70], although there has been ample discussion about how ICN changes the security model from securing the communication path to securing the content, there has not been enough focus on the challenges that ICN privacy model presents due to the intrinsic name-based identification of content. Arianfar presented an initial design [29] where users and providers collude to prevent detection of access to “forbidden” content. Since the ICN approach results in content arriving from network elements other than the originating server, the security model cannot be based on the source or destination; instead, ICN designs must secure the content rather than the path, as suggested by Walfish et al. [120] and Wendland et al. [122]. Even the critics of ICN designs, showing less faith in ICN's ability to improve network performance [70] have pointed out that ICN designs might bring benefits such as more secure network configuration, intrinsic routing stability, and protection against denial-of-service.

Systems such as Tor [116] and Freenet [44] provide anonymity for users. However, they require substantial infrastructure investment. In addition, they do not prevent *watchlist* attacks: they prevent the adversary from knowing who asked for a given object, not which object was requested. Approaches such as broadcast encryption [59] effectively preserve the privacy of content, but they require information to be shared between publishers/producers and end users/consumers.

Bernardini et al. proposed a scheme named PrivICN which protects name and content confidentiality and also preserves in-network caching [33]. This method is based on the proxy encryption scheme and the Key Management Server (KMS) which is the fully trusted party and generates one master key and multiple pairs of client/proxy key for each client. However, in this method if a client colludes with the proxy, she can access the master key and decode all the messages. Based on a centralized key management system, this method also presents the risk of a single point of failure. Moreover, this method is primarily for the intra-domain; for it to work between two domains, the message needs to be decrypted and re-encrypted with the master key of the new domain. However, in this case, the junction node accesses the real name and data.

Chaabane et al. discuss various privacy threats and some potential countermeasures for Content-Oriented Networking (CON) [40]; they also discussed the name privacy issues raised by the human readable feature of a CON name and correlation between the name and its corresponding content. Broder et al. introduced the bloom-filter based scheme using a hierarchical bloom-filter as the router storage and the routing table [36]. In this method, the client computes the hierarchical bloom-filter of the name, and her request in the obfuscated form. When a router receives the request, it checks the last filter containing an exact match with the stored name in its cache. If the router finds the exact match, it will return the corresponding data to the user. Although this method also uses name obfuscation to provide privacy, the bloom-filter scheme suffers from high false positive error rate and needs frequently resetting.

Wood and Christopher introduced TRAPS [126] which is an application-transport protocol and provides opportunistic encryption for all data in NDN. TRAPS is built based on knowing the name to access data and relies on the establishment of a secure session between users and producers. However, since TRAPS is based on MLE, it is only secure for unpredictable names. Therefore, an attacker who can predict or estimate commonly used names can compromise users' privacy. Although the author uses the salt generation mechanism to prevent dictionary attacks, it is not clear how the attacker cannot access the mechanism already accessible by all other authorized users.

4.1.2 Convergent encryption based method

The default architecture of NDN uses application name to transfer interest and data messages. However, application names reveal information about requested data and users' interest which endanger users' privacy. Therefore, to provide some level of privacy, we should convert human readable application names to random strings which are still routable through NDN.

The method that seems compatible with NDN features is MLE based on Convergent Encryption (CE) which uses the message itself to generate the key, therefore, the same messages have the same key and the same ciphertext [32]. MLE is used in the cloud storage to save space by reducing redundant data and providing deduplication. Since in NDN, the same request (including the same name) should look the same after encryption, to fetch the same data in NDN caches, MLE seems to compliment NDN and to be suitable for obfuscating names with considering NDN features. However, in MLE method, the attackers who can access the name (data) can generate the key related to that name. Moreover, MLE is susceptible to brute force attacks (dictionary attacks). Keelveedhi et al. introduced DupLESS to improve the MLE method with the aid of the key server to generate key from the message and the secret key which belongs to the server [82]. DupLESS uses oblivious transfer to transfer the message between a user and the server to prevent the key server from obtaining information about data, and provides users with encrypted messages without knowing any information about the secret key of the server. As long as the server is not accessible by an attacker, the system will be secure. However, this method suffers from single point of failure, and since DupLESS needs one server to generate the same key, it suffers from scalability problem, showing that it is not suitable for large networks such as P2P and NDN.

Liu et al. introduced a method for providing de-duplication in cloud storage and remove the additional server by using client-side encryption and PAKE (Password Authentication Key Exchange) [90]. In this method, the users first send a short hash of the file to server and the server determines if any other users sent the same file. If any other users send the same file, the server lets them run a single round PAKE protocol. If the users have the same file, the uploader will receive the same key as the previous user, otherwise, it will receive a random key. This method is not suitable for NDN because the encryption is based on the users' secret keys and not on data; while in NDN the content (data) is distributed in the network. Moreover, in NDN, the providers are the first entities that inject data to networks so the key would need to be exchanged between the user and the provider which would be similar to exchanging a secret key between them. Therefore, this method does not provide an efficient way for generating random string names in NDN.

Duan and Yitao used group signature as encryption to improve the DupLESS method [55]. In this method, the users encrypt data using t+1 servers. Therefore, in this method the signature is distributed among several servers which is more suitable for P2P networks as well as for NDN. Moreover, the system is secure against up to t corrupted users and servers. However, in this method there is a need of the trusted entity to distribute group signature among servers which can be considered honest but curious. However, the equality of messages may reveal some information to attackers in methods based on MLE.

Our proposed method for obfuscating names in NDN is based on the obfuscation technique proposed by Duan and Yitao [55]. However, we introduce an additional level of privacy protection using gateways.

4.2 Problem statement and potential attacks

In this chapter, we focus on privacy of users and try to mitigate name-monitoring attacks that can endanger users' privacy. In NDN architecture, the hierarchical naming technique and un-encrypted names are used to reap benefits of easier routing and in-network caching, respectively. However, hierarchical and un-encrypted names can reveal information of content that can endanger users' privacy.

NDN names are potentially meaningful to humans. The more granular and well defined the structure, the more specific they are. Secondly, while content names are "metadata" in the normal communications sense (just like IP addresses or telephone numbers are metadata), it is widely accepted that metadata associated with communications sessions is as valuable, sensitive, and private as content/data. In the case of addresses, the threat is of traffic analysis (who talks to whom); in the case of name-spaces, it is who is interested in what.

The attacks relevant to the threat in consideration can be internal or external. The active or passive attacks performed by the compromised internal nodes by tracking its neighbors, flooding the wrong false message on routing and so on are called *insider attacks* [64]. Such attacks are also known as Byzantine attacks. In Byzantine attacks, a set of intermediate nodes working individually within the network carry out attacks like forming routing loops, consuming time and bandwidth by forwarding packet from non-optimal paths, and selectively dropping packets to disrupt the network.

Following are some of the most well known node-oriented byzantine attacks:

(a) Selfish node attack

(b) Black hole attack

(c) Worm hole attack

(d) Grey hole attack

4.2.1 Selfish node attack

During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find new path to destination. In a Selfish node attack, a faulty node corrupts the route discovery packets to advertise itself as having the shortest path to the node whose packets it wants to compromise. The attacker aims at modifying the information so that they can control the traffic flow of the network.

Malicious nodes quickly respond to the source node as these nodes do not refer to the routing table and drop all the routing packets and also flood false information of the shortest route in network. The source node assumes that the route discovery process is complete and ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets.

4.2.2 Black hole attack

In this attack, when a vicious node senses some route request packet in the network, it responds to the legitimate node by pretending it has the shortest and original route to the destination node even if no such route exists. Subsequently, the vicious node easily drops the packet and/or introduces misleading routing information in the network.

4.2.3 Grey hole attack

Grey hole attack is a denial of service attack in which routers in a mesh topology forward a subset of packets which are handled by the targeted receiver but left by others.

4.2.4 Worm hole attack

Worm hole connects two different points in space through shortcut path. In this attack, a pair of attacking nodes can intercept the route by short circuiting the network. Worm hole attack can be performed with single node too but is generally carried out by worm hole link.

4.3 Determining privacy-sensitivity

Privacy-sensitivity is obviously a contextual phenomenon [86], including but not limited to the time and geographical location of the interest. What may be termed as an intellectual debate in one part of the world may be considered an execution-able offense in another. What may be termed as personal liberation in one community, could be termed as an unspeakable act of shame in another. Personal data, e.g., health data could have severe economic or political implications on personnel, countries, and organizations depending upon the content and location of the data being considered. Problems may arise with such data when it is associated with a) countries where this content is considered politically sensitive or b) sharing more information than necessary by the “need to know” access control principles in information security [108].

In monitoring attacks, an attacker can access the same router that a user can fetch data from, and the attacker tries to identify users and recognizes users' requested content. The attacker may know victims' habits such as language and region.

4.4 System description and threat models

The system consists of three entities namely: 1) consumer (user), 2) router, and 3) content provider.

In this work, we attempt to mitigate name and monitoring attacks that can endanger users' privacy. In NDN architecture, 1) hierarchical and 2) un-encrypted names are used to allow benefits of easier routing and in-network caching, respectively. However, they can reveal private information regarding content that can invade users' privacy.

To protect users's privacy and to prevent an attacker from finding out users's interest, we consider the following threat models:

- Attacker may be an eavesdropper who can probe the traffic transferred between a user and a provider.
- Attacker may be any router or can compromise a set of routers.
- Attacker may be a user who can monitor the traffic, generate an interest message and receive the corresponding data packet, or can compromise a set of users.
- Attacker may compromise a set of routers and users and/or facilitate collusion among them.
- Attacker can correlate corresponding data for each interest that returns to the users. Therefore, although the users may use different formats of interest (different encryption for the same interest message), the attackers can perceive that the two interests generated by two different users are the same if these users receive the same corresponding data.

Moreover, we consider the frequency attack which is the well-known inference attack used to break deterministic encryption [69] [99]. In our case, the adversary can eavesdrop on the request (interest) and see the cached contents of each edge router. Therefore, with accessing some auxiliary information about the popularity distribution of contents, the adversary can perform the frequency attack on the encrypted interests.

Let N_o be the set of obfuscated name (ciphertext) o observed by an attacker, and N_p be the set of name (plaintext) N in a local area at a specific time. Given a deterministic obfuscated name o over N_o, and auxiliary information about popularity distribution of local content (name) N over N_p, the attack performs by assigning the ith most frequent o to the ith most popular N. Then, the attacker can understand the user's interest by mapping obfuscated interest o to real name N. Let Hist() is a function to return the number of times each item in a given set is requested, and sort() is a function to sort the result of Hist() in descending order. Let for all items in the set, ρ be the sort of Hist(N_o), and π be the sort of Hist(N_p). Moreover, we denote the rank of o which is the position of the occurrence of o in sorted set ρ by $Rank_\rho(o)$. Formally, the attack performs as follows:

- $\rho \longleftarrow$ sort(Hist(N_o))
- $\pi \longleftarrow$ sort(Hist(N_p))
- calculate $\alpha : N_o \longrightarrow N_p$ such that

$$\alpha(o) = \begin{cases} \pi[\, Rank_\rho(o)] & \text{if } o \in N_o \\ \perp & \text{if } o \notin N_o, \end{cases}$$

  where α defines the guessed mapping between encrypted names and plain-text names. Moreover, the accuracy of the attack is estimated based on the total number of attacker's correct guesses.

4.5 Assumptions

Following are the assumptions used in this evaluation:

- Since we are focusing on name privacy, we assume that the content is encrypted by the provider. The encryption key may be generated and shared by various methods. One of these methods is to generate the key from the obfuscated name.
- It is noteworthy that we are not including cryptography or code vulnerabilities as threats in the scope of this thesis.
- We assume that if there are different ways to obfuscate a name, the producer shall provide for the corresponding/salient encryption technique for the linked data accordingly.
- We assume that the content is encrypted by the provider in order to preserve name privacy using MLE. The encryption key is derived from the service name in an obfuscated way with the help of key servers as in a server-aided MLE scheme [55]. Therefore, if the users are allowed to obfuscate content names partially or fully, there will be different keys for each type of obfuscation. So

the producer would need to provide different encryptions of corresponding data respectively.

- We assume that there is a fully trusted dealer who generates secret shared keys used to obfuscate names in the first layer of privacy protection. The dealer distributes the keys to the key servers securely.
- We assume that the gateways used in the second layer of privacy protection are honest but curious.
- Since two different layers of privacy protection utilize two independent mechanisms (key servers and gateways), we assume that the adversary's capacity to collude with or compromise both the key servers and gateways is not beyond a reasonable limit. In other words, we are assuming that both the privacy protection layers cannot be fully compromised simultaneously.

4.6 Preliminaries and Definitions

4.6.1 Encryption techniques

Oblivious Pseudo Random Function(OPRF)

A verifiable oblivious PRF scheme [98] consists of five algorithms OPRF = (Kg, EvC, EvS, Vf, Ev), the last two being deterministic. Verifiable OPRF schemes can be built from deterministic blind signatures [38]. Therefore, we use RSA-OPRF[G,H] scheme based on the RSA blind signature [31] [41]. The RSA blind signature scheme includes fixed public RSA exponent e. The key generation takes e as an input to generate M, d such that $ed \equiv 1 \bmod \Phi(n)$, where $n < e$ and modulus M is the product of two distinct prime numbers with approximately equal lengths. The output of this scheme is $(n, (n, d))$ as the public key and private key respectively. At the client side, the user uses hash of the name as $H : \{0, 1\}^* \to \mathbb{Z}_n$, and then multiplies the hash with the blinding element r^e where r^e is a random group element and sends the resulting blinded hash x to the Key Server. The Key Server encrypts x with secret key d to generate y and sends back to the consumer. The consumer removes the blinding from y to generate z. For verification, the consumer computes $(z^e modn)$ and checks if it equals $H(N)$. Finally, if the verification is confirmed, the consumer will generate final output $G(z)$ where G is another collision-resistance hash function.

Threshold Signature

In the threshold scheme [55] used for name obfuscation, parameter l depicting the number of players (key servers) and parameter t<l define a (t+1,l) threshold signature where a subset of t+1 players can generate a signature, but a subset of t or less players cannot generate a valid signature. To provide convergent, non-interactive, and efficient properties, the threshold scheme used by Duan and Yitao [55] is based on Shoup's RSA-based scheme [110].

In the RSA threshold signature scheme, the trusted entity which we call dealer, chooses two random large prime numbers of equal length (e.g., 512 bit) p and q, where

$$p = 2p^{'} + 1, q = 2q^{'} + 1$$

where $p^{'}$, and $q^{'}$ are also prime. The RSA modulus is $n = pq$. Let us assume that $m = p^{'}q^{'}$. The dealer selects the RSA public exponent e where e > 1 and prime. The public key is PK = (n,e)

In the dealing phase, the dealer generates a public key PK, secret key shares $SK_1, ..., SK_l$, and verification keys $VK, VK_1, ...VK_l$. let $\mathbb{Z}$ be the set of integers, and for positive integer n, let $\mathbb{Z}_n = \{0, 1, .., n-1\}$ and $\mathbb{Z}_n^* = \{i \in \mathbb{Z} : 1 \leq i \leq n-1\}$. The dealer determines $d \in \mathbb{Z}$ such that $de \equiv 1 \bmod m$. The dealer sets $a_0 = d$ and selects a random a_i from $\{0, ..., m-1\}$ for $1 \leq i \leq t$. The polynomial $f(X) = \sum_{i=0}^{t} a_i X^i \in \mathbb{Z}[X]$ is defined by numbers $a_0, ..., a_t$. For $1 \leq i \leq t$, the dealer computes $d_i = f(i) \bmod m$, where d_i is the secret key share SK_i of player i. Let Q_n (which is in cyclic of order m) be the subgroup of squares in $\mathbb{Z}_n^*$. The dealer randomly selects $v \in Q_n$ and for $1 \leq i \leq l$ calculates $v_i = v^{S_i} \in Q_n$. These elements define the verification keys: $VK = v$ and $VK_i = v_i$.

Let $\Delta = l!$. For any subset S of $t+1$ points in $\{1, ..., l\}$ and for any $i \in \{1, ..., l\} \backslash S$ and $j \in S$, we can define (4.1).

$$\lambda_{i,j}^{S} = \Delta \frac{\Pi_{j^{'} \in S \backslash \{j\}} (i - j^{'})}{\Pi_{j^{'} \in S \backslash \{j\}} (j - j^{'})} \in Z \tag{4.1}$$

For the NDN name N, let $x = H(N)$, where H is a hash function defined as $H : \{0, 1\}^* \rightarrow \mathbb{Z}_n$. The signature share of key server i consists of ($x_i = x^{2\Delta s_i} \in Q_n$) along with a proof of correctness that is the log of x_i^2 to the base of $\widetilde{x} = x^{4\Delta}$ which is the same as the log of v_i to the base v.

To combine the valid shares from a set $S = \{i_1, ..., i_{t+1}\} \subset \{1, ..., l\}$ of players, we assume $x = H(N) \in \mathbb{Z}_n^*$ and $x_{i_j}^2 = x^{4\Delta s_{i_j}}$ and compute

$$w = x_{i_1}^{2\lambda_{0,i_1}^S} ... x_{i_{(t+1)}}^{2\lambda_{0,i_{(t+1)}}^S} \tag{4.2}$$

where λ is defined in (4.1) and we can calculate $w^e = x^{e^{'}}$ where $e^{'} = 4\Delta^2$. Because $gcd(e, e^{'}) = 1$, we can compute y such that $y^e = x$. Moreover, according to a standard algorithm $y = w^a x^b$ where a and b are integers and $e^{'} a + eb = 1$ that can be attained from the extended Euclidean algorithm on $e^{'}$ and e.

4.6.2 Game theory model

In this section, we explain the use of the game theory model based on Shokri and Reza's method [109] to select the optimum name privacy protection level to meet the user's need. We assume that a user shares the name of the requested data with the network to receive the corresponding data. However, the user wants to protect her sensitive information from untrustworthy entities. According to her desired privacy level, the user must make a trade-off between efficiency and privacy. Following are some noteworthy considerations to guide the user's decision.

(a) Name obfuscation involves overheads caused by:

  i. Crypto-computation

  ii. Key distribution

(b) The gateway system has potential latency overhead and may also cause some reduction in bandwidth.

(c) Together, the combination of the two privacy protection approaches might reduce the effectiveness of NDN caching algorithms. Hence, there is a compromise in efficiency.

In short, the stronger the privacy, the more the network delay and the higher the cost (resulting from procedures such as name obfuscation and routing through gateways). The flow of sharing name data is shown in Fig. 4.3.

Protection mechanism

We assume that a user wants to protect her privacy by keeping the content name $N \in N_s$ as confidential as possible, where N_s is a set of all possible names. According to her required privacy protection level, the user chooses different ways of encryption including various levels of name obfuscation and gateway routing. In name obfuscation, a part or whole of the name may be encrypted. Thereon, it may be routed through different number of gateways. We assume that this encrypted information (name) $o \in O$ is observable through the network. We consider that the observable name is sampled according to distribution (4.3).

$$p(o|N) = Pr(O = o|N_s = N) \tag{4.3}$$

Generally, the members of observable O can be a subset of the different ways that a name can be encrypted.

Utility cost function

Our work is based on the premise that the user is willing to accept the cost of her desired level of privacy. For NDN name privacy, this is the cost of name obfuscation and the cost of introducing gateways, both processes involving computational overhead as well as causing delay.

Let us assume that the difference between the cost of retrieving an obfuscated/encrypted name versus an non-obfuscated or un-encrypted name (plain text), added to the difference between the cost of retrieving an obfuscated or non-obfuscated name from a (number of) gateway(s) versus without any gateway, equals the Utility Cost $c(o, N)$. Although the exact delay cost (diffidence delay) cannot be calculated since data can be retrieved from any cache of intermediate routers in the network, we can definitely estimate the delay cost by considering the cost difference in data retrieval for an encrypted name and an un-encrypted name, with or without gateways. This is due to the fact that more encryption can impose limitation on routing and retrieving data from nearby a user. Therefore, the Utility Cost $c(o, N)$ is a summation of the costs of applying obfuscation and using number of gateways. We use a **Hamming distortion function** for the obfuscation cost (i.e., the obfuscation cost is 0 if no obfuscation is carried out on the interest name, otherwise it is 1 for partial or full name obfuscation). Moreover, the cost includes number of gateways as more gateways can impose more delay to retrieve data from the nearby user. Therefore, the expected utility cost can be computed as (4.4).

$$\sum_{o} p(o|N).c(o, N) \tag{4.4}$$

The utility cost function can be based on applications or users' preferences.

Inference Attack

We assume that adversary wants to get users' sensitive information by observing a name sent to the network. Therefore, the attacker tries to estimate the real name $\widehat{N} \in N_s$ from the observed name $o \in O$. The probability distribution for estimating a real name from an observed name can be shown as (4.5).

$$q(\widehat{N}|o) = Pr(N_s = \widehat{N}|O = o) \tag{4.5}$$

In other words, inference algorithm q tries to invert the effect of privacy protection p. Moreover, the error of the inference algorithm to estimate the real name of the message can be estimated by the distortion privacy metric.

Distortion Privacy Metric

To calculate the privacy distortion metric, $d(\widehat{N}, N)$ is considered as the difference between the name $\widehat{N}$ (estimated by the attacker) and real name N. The distortion privacy metric is determined by the user depending on her sensitivity about the real name N being revealed to an attacker (when the attacker estimates the name $\widehat{N}$ based on the information available to him). Therefore, the higher the value of $d(\widehat{N}, N)$ the lesser the user's concern about the observed name o. The user's expected distortion privacy is computed in (4.6).

$$\sum_{o} p(o|N) \sum_{\widehat{N}} q(\widehat{N}|o).d(\widehat{N}, N) \tag{4.6}$$

It is noteworthy that just as a specific interest message containing name and the corresponding data message would hold a certain level of privacy sensitivity to the user, they would also hold a value for the adversary. In this work, the specific value of a certain piece of information/interest/content to the adversary is termed as *advantage*. The adversary also incurs a cost of resources to carry out an attack which is denoted by c_a. Hence, an attack would only be feasible to an adversary if:

$$advantage > c_a \tag{4.7}$$

This implies that the attack has a threshold point and once the adversary reaches the limit where c_a is approaching a value equal to the *advantage*, the attack would need to be stopped whether successful or not. In other words, by that point the attacker/adversary would have exhausted the allocated resources for the particular value of a successful attack. Hence the value of c_a may be used to select d function,

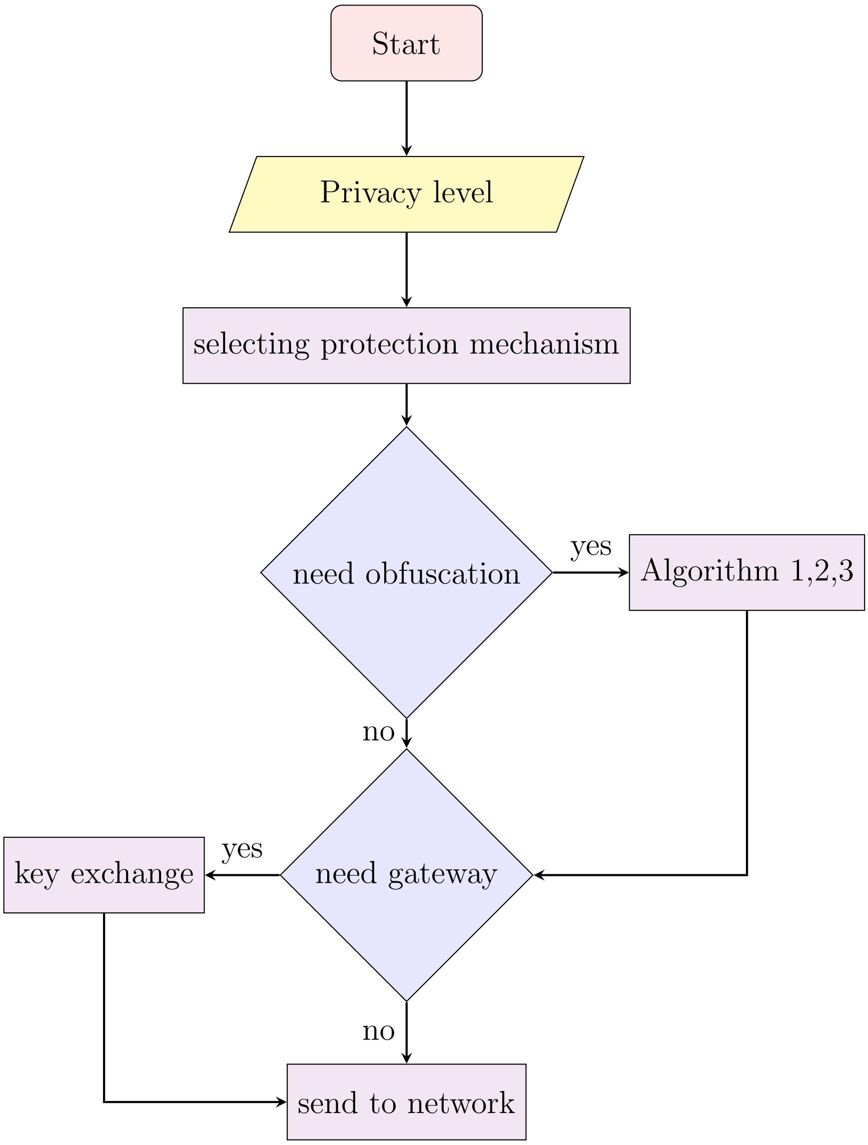


Figure 4.1: The flowchart of the proposed method for selecting the proper mechanism based on the privacy level given by a user.

i.e., if the cost for an attacker is more than the value of the stolen information, then $d(\widehat{N}, N)$ has a higher value and it is harder for an attacker to estimate the real name from an encrypted/obfuscated name.

4.7 The proposed approach

In this section we describe the outline of the proposed method and details of the two privacy layers.

As described (with examples) earlier in Chapter 1 Section 1.4, NDN content names are hierarchical and include different levels. In this work, two different privacy protection processes are proposed. The first process is the name obfuscation to ensure name privacy. The Convergent Encryption (CE) method [55] used in this work implies that any two names that are identical should still appear identical in the network after encryption. This poses a privacy leakage risk. To mitigate this risk, we used an additional layer of security which separates the interest for named data from the user requesting it. A user's interest is hidden from the neighboring routers/network by using gateways in between. The proposed method is further explained below:

(a) As shown in Fig. 4.1, based on the user's privacy requirements, firstly she chooses whether to use name obfuscation or not and then the required extent of name obfuscation (full or partial).

(b) Secondly, she chooses whether or not to use gateways and the required number of gateways.

(c) If the user decides to obfuscate the name, she uses the following process: Each user has her own key and uses it to send the encrypted name to $t+1$ servers with oblivious transfer as shown in Algorithm 3. In the algorithms and rest of this chapter when we use k indexed to any variable, it depicts the level of sections in a hierarchical name, e.g., if N is a name cnn/eng/news, N_k is cnn/eng/news when $k = 3$, N_k is cnn/eng when $k = 2$, and N_k is cnn when $k = 1$.

(d) Each server signs the message (encrypted name) transferred by the user. In other words, the server uses signature as encryption for the encrypted name. Since users use oblivious transfer to send the message to each server, the servers cannot gain any information about the message and users cannot get any information about servers' secret keys, as illustrated in Algorithm 4.

(e) After receiving the signed interest messages, the user removes the blinding r from the encrypted name. The encryption of this interest message is based on convergent encryption and includes the interest message and group signature (the secret keys of $t+1$ servers). This process is depicted in Algorithm 5.

(f) For the second layer of privacy, based on the required privacy level the user decides the number of gateways and encrypts the message with (suitable number of) secret shared keys to transfer it to the proper gateway. Onion encryption is used for encrypting the message between the user and gateways.

(g) When the message reaches the final gateway, this gateway can decrypt the CE based encrypted message. Therefore, it can send this message to the network.

(h) The data message corresponding to the interest message can be fetched from the cached router if the corresponding data message is saved in an intervening router, otherwise the data message can be fetched from the original server (content provider).

Algorithm 3 Consumer to Key server

```
    Input:  Key registration $n$, RSA public exponent $e$, and real name $N$
    Output:  Hierarchical blinded name $x$

if $e \leq n$ then return false
$r \xleftarrow{\$} \mathbb{Z}_n$
for $k = 1 \rightarrow |N|$ do
    $h = H_1(N_1 \| N_2 .. \| N_k)$
     $x =$ Append $(x, h \cdot r^e) = (x || h \cdot r^e)$
return $x$
```

Algorithm 4 Key server i to Consumer

```
    Input :  Name $x$ and secret server key $d_i$
    Output :  Hierarchical encrypted and blinded name $y_i$

for $k = 1 \rightarrow |x|$ do
    $y_i =$ Append $(y, x_k^{d_i}$ mod $n)$
return $y_i$
```

Algorithm 5 Consumer to Gateway/Network

```
    Input :  Hierarchical encrypted and blinded name $y_i$ and Key registration $n$
    Output :  Hierarchical encrypted name $G$

for $i = 1 \rightarrow t + 1$ do
    if proof of Key server i for $y_i$ fail then return false
combine t+1 signature $y_i \rightarrow y$
for $k = 1 \rightarrow |N|$ do
    $z =$ Append $(z, y_k.r^{-1}$ mod $n)$
    if $z^e$ mod $n \neq h_k$ then return false
     $G =$ Append $(G, G(z))$
return $G$
```

4.7.1 First privacy layer: name obfuscation

As it was mentioned before, the default name used in NDN reveals a lot of information that can show consumers' interests. Therefore, in the first privacy layer of the proposed method, we obfuscate the name to transfer meaningful names to random string names. To retain the NDN in-networking caching feature, name obfuscation is based on Credential Encryption (CE) implying that two identical names are obfuscated to the identical random strings. Moreover, the proposed method keeps the hierarchical structure of the names that is useful for efficient routing. As shown in Algorithm 3, the consumer selects a random number as blinding r. Next, the consumer sends the product of r with the hash of the name h to $t+1$ key servers.

Therefore, as depicted in Algorithm 4, the consumer uses oblivious transfer to send the name x to key servers, and the key server signs (encrypts) the blinded name x with its secret key d_i without any knowledge of N. In this case, the encrypted name y_i is generated from the server key d_i and the blinded name x, and key server i returns hierarchical encrypted name y_i including blinding r to the consumer. By using shared signatures and oblivious transfer, the proposed method mitigates the effect of the dictionary attacks. Oblivious transfer ensures that the consumers do not access secret keys and the key servers encrypt (sign) the names without knowing the users' requested name (interest). Moreover, by using shared signatures, encryption is distributed among $t+1$ servers, thus reducing the possibility of a single point of failure.

After the consumer receives the encrypted name y_i, first she checks the proof of correctness by calculating (4.1) and (4.2) and comparing it with the log of the server verification key v_i to base of v shown in Algorithm 5. After receiving the encrypted name from the $t+1$ key servers, the consumer verifies and combines the signatures using (4.2). After computing (4.2) the consumer can calculate y, remove the blinding r to get z. Moreover, the consumer verifies that z^e is same as the hash of the name h. If this verification is confirmed, the consumer returns the hash of encrypted name G which is the obfuscated name.

4.7.2 Second privacy layer: gateways

The first privacy protection layer of our proposed method implies that two identical names would yield identical obfuscated names. This could cause a privacy vulnerability susceptible to inference, which is addressed by introducing the second privacy protection layer. The second privacy protection layer uses gateways, i.e., routers capable of encrypting as well as routing interest messages. The user can send the name to a gateway that can uniquely encrypt the message and also hide the link between the user and the requested message. According to the consumers' privacy level and sensitivity of data, the consumers may choose to uniquely encrypt the message to one or more gateways. Therefore, according to the privacy level, the consumers decide how far the uniquely encrypted message should be sent, i.e., how many gateways it should be routed through. We used the Onion routing method [115] for this purpose. The process is described below:

(a) The user first selects the number of gateways she wants to use based on the desired level of privacy protection.

(b) The user exchanges the session key (symmetric key) with the gateway using the gateway's public key (asymmetric key).

(c) The interest message is then encrypted with layers of different session keys corresponding to the gateways.

(d) Each gateway decrypts its layer and forwards the message to the next gateway.

(e) The last gateway removes the last layer of the encryption and then forwards the interest message according to the default NDN rules to fetch date from the cache or forward the interest further.

(f) According to NDN routing rules, the content message follows the interest's reverse path.

(g) When the content message is returned from the network to the last gateway (which is also the first gateway on the reverse path), it is again encrypted with the shared key of the gateway.

(h) From one gateway to the next, the data message is encrypted in layers.

(i) Once the user receives the data message, she decrypts it.

4.7.3 Privacy level determination using game theory

Privacy preservation mandates that minimum information should be revealed to any adversary. For NDN, this would include the content's name and how much it reveals about the content as well. Additionally, the correlation between the interest/content and the user could be exploited by an adversary. However, there is a trade-off between providing name privacy and using benefits of NDN. Therefore, name privacy preservation should provide the optimal level of privacy that does not spoil NDN features such as decreasing delay and pervasive caching (content distribution).

We define a method based on Game theory [73], wherein a user can determine the level of privacy which fulfills her requirements. We can set the level of privacy based on first and second layers of privacy as discussed in the previous subsection, to achieve the user's requirements for providing optimum privacy and efficiency in receiving data. Fig. 4.2 shows the problem of choosing a trade-off between user privacy and utility in NDN with the game model in the extensive form (i.e, as a tree diagram), and the normal form (i.e, in tabular form) of this problem statement is shown in Table 4.1. As shown in Fig. 4.2, we assume that a user according to sensitivity of her information makes a decision to either choose the strongest level, medium level

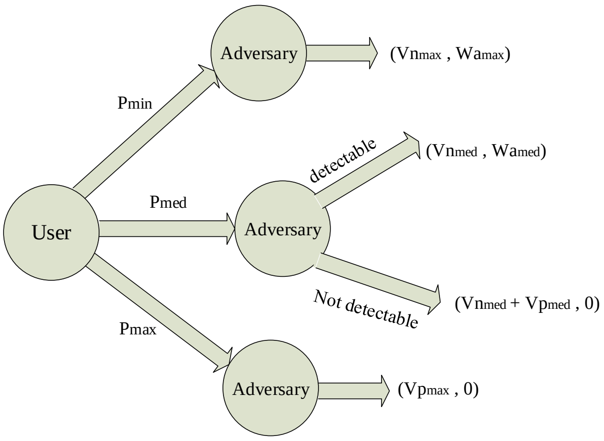


Figure 4.2: The tree diagram of the named privacy game model (V_p and V_n are the user's privacy and network utility payoffs respectively. W_a is the adversary's payoff)

or weakest level of privacy. It is noteworthy that the privacy levels can vary to more than one value/level in between the maximum and minimum privacy levels. However in this thesis, for the ease of discussion, we have only shown three privacy levels. We depict the privacy level as $P_{o,g}$ where o represents level of name obfuscation as described in the first layer of privacy and g represents number of gateways utilized as described in the second layer of privacy. When a user chooses maximum privacy level i.e., P_{max}, then $P_{max} = (P_{o_{max}}, P_{g_{max}})$. A medium level privacy level can be depicted by P_{med} which may equal $(P_{o_{max}}, P_{g_{min}})$, or $(P_{o_{min}}, P_{g_{max}})$, or $(P_{o_{med}}, P_{g_{med}})$. A minimum or weakest privacy level can be depicted as $P_{min} = (P_{o_{min}}, P_{g_{min}})$. Both name obfuscation and gateway utilization include encryption, decryption, and routing costs. This cost also known as utility cost defined in (4.4) also includes the delay factor. Since utility cost is directly proportional to the privacy levels chosen, it implies that when privacy is maximum, (P_{max}), so is utility cost (C_{max}). V_p is the privacy payoff for the user which is $\propto d$ (defined in (4.6)) and V_n is the network utility payoff for the user which is $\propto$ utility cost. W_a is the payoff for the adversary which is $\propto 1/d$. We have previously defined that for the *advantage* and cost c_a in (4.7) for the adversary and how that impacts d. The game theory payoffs for the user and the adversary are illustrated in Fig. 4.2.

The normal form is also shown in Table 4.1. In this table, the first column corresponds to the potential strategy of the adversary, and the first row corresponds to the potential strategy of the normal user.

Table 4.1: The Normal form of the named privacy game model(V_p and V_n are the user's privacy and network utility payoffs respectively. W_a is the adversary's payoff.)

		user		
		maximum	medium	minimum
adversary	If the user opts for P_{min}, the adversary will detect ;if the user opts for P_{med}, the adversary may detect; if the user opts for P_{max}, an adversary cannot detect	(W_amax, V_nmax)	(W_amed, V_nmed)	$(0, V_pmax)$
	If the user opts for P_{min}, the adversary will detect ;if the user opts for P_{med}, the adversary may not detect; if the user opts for P_{max}, an adversary cannot detect	(W_amax, V_nmax)	$(0, V_nmed + V_pmed)$	$(0, V_pmax)$

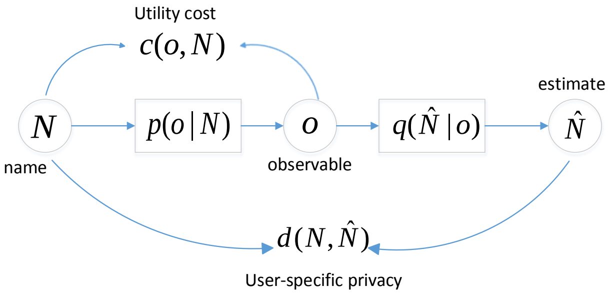


Figure 4.3: The process of sharing a name from a user to an attacker

Game theory problem statement

In this work, we try to balance between user's utility function and privacy. Therefore, the proposed method tries to find an optimal utility function that keeps the user's privacy at a certain level. Generally, the proposed method maximizes the utility function with guaranteed distortion privacy.

Therefore, the problem is to find optimum value p^* for the probability distribution function that minimizes utility cost of the user, on average, as illustrated in (4.8).

$$p^* = \underset{p}{argmin} \sum_{o} p(o|N).c(o, N) \tag{4.8}$$

This optimization should be provided within the user's privacy constraints. We denote the minimum desired distortion privacy level as d_m. If the protection mechanism p^* satisfies the inequality defined in (4.9) below, then the user's average distortion privacy is guaranteed.

$$\sum_{o} p^*(o|N) \sum_{\widehat{N}} q^*(\widehat{N}|o).d(\widehat{N}, N) \geq d_m \tag{4.9}$$

Game theory solution

In the proposed method, the user starts the game by choosing a privacy level as described in Section 4.7.3. Following that, the adversary applies a suitable inference attack. We assume that the privacy protection mechanism is not a secret to the adversary, so she can adapt her attack accordingly.

The best privacy protection mechanism is the one that can anticipate and overcome an adaptive adversarial behavior. The user must anticipate the optimal inference attack by the adversary and optimize her objective (utility and privacy) accordingly. Therefore, we do not model any specific adversary. However, we consider the adversary that minimizes $d(\widehat{N}, N)$ as described in Section 4.6.2 to successfully compromise users' privacy.

It is noteworthy to explain here that the privacy distortion metric, $d(\widehat{N}, N)$ is considered as a difference between the name $\widehat{N}$ (estimated by the attacker) and real name N. The distortion privacy metric is determined by the user based on sensitivity of the user about revealing the real name N when an attacker estimates $\widehat{N}$. Since estimating the real name for an attacker with using obfuscation and more gateways becomes hard, the distortion privacy metric can be defined as shown in (4.10). Where L_O is the length of obfuscation (number of obfuscated levels of the name), L_N is the length of the real name (number of levels the name has), $D(E, G)$ is the distance between edge router and the gateway, and $D(E, P)$ is the distance between the edge router and the producer (maximum distance). Therefore, the value of $d(\widehat{N}, N)$ is between zero and two. While $d(\widehat{N}, N)$ value is zero when there is no protection method, $d(\widehat{N}, N)$ becomes two when there is maximum protection i.e. maximum number of obfuscation levels and maximum number of gateways.

$$d(\widehat{N}, N) = \frac{L_O}{L_N} + \frac{D(E, G)}{D(E, P)} \tag{4.10}$$

As it is impossible to list all user-adversary models, to model the proposed method, we use a Stackelberg (leader-follower) game in which the user selects an optimal protection mechanism p^* and the adversary follows the user by selecting an optimal inference attack q^*. Thus, solutions p^* and q^* are mutually optimal against each other and p^* is optimal against any inference attack.

For any name $N \in N_s$, the user strategy space model is all observable O, and for any observable $o \in O$ an attacker space model is N_s which is set of all possible estimated names $\widehat{N} \in N_s$. Therefore, the mixed strategy for a user can be shown by a vector $p(.|N) = (p(o_1|N), p(o_2|N), ...p(o_m|N))$, where $\{o_1, o_2, ..., o_m\} = O$ and the mixed strategy for an adversary can be shown by a vector $q(.|o) = (q(\widehat{N_1}|o), q(\widehat{N_2}|o), ...q(\widehat{N_j}|o))$, where $\{\widehat{N_1}, \widehat{N_2}..., \widehat{N_j}\} = N_s$. The vectors $p(.|N)$ and $q(.|o)$ are conditional distribution functions with an obfuscated function for name N and an inference algorithm for an observable name o respectively. As shown in (4.11) and (4.12), P and Q are all sets of all mixed strategies for user and adversary respectively.

$$\begin{aligned} P = \{p(.|N) = (p(o_1|N), p(o_2|N), ...p(o_m|N)), \forall N \in N_s : \\ p(o_i|N) \geq 0, \forall o_i \in O, \sum_i p(o_i|N) = 1\} \end{aligned} \tag{4.11}$$

$$\begin{aligned} Q = \{q(.|o) = (q(\widehat{N_1}|o), q(\widehat{N_2}|o), ...q(\widehat{N_j}|o)), \forall o \in O : \\ q(\widehat{N_j}|o) \geq 0, \forall \widehat{N_j} \in N_s, \sum_j q(\widehat{N_j}|o) = 1\} \end{aligned} \tag{4.12}$$

The pure strategy of choosing action k is the member vector of the set P and Q where the kth element of these sets is 1 and other elements are zero.

To consider distortion privacy, the game should be formulated as Baysian Stackelberg [103]. In this game, the optimal values $p^* \in P$ and $q^* \in Q$ to create the equilibrium point will be defined. After that if a user deviates from this value and selects p', there will be an inference attack q'^* against users that decreases the user's privacy than the optimal value p^*. Next we discuss how to obtain the optimal values for this game.

To solve the aforementioned Bayesian Stackelberg game [103] and find the equilibrium point (p^*, q^*), first we assume that an adversary finds the optimal inference attack q^* against any user's protection mechanism. Therefore, the user's protection mechanism shall be defined according to her object function and privacy constraint (d_m) as mentioned in this section earlier. This solution will maximize the user's utility function and provide the protection level that a user needs in anticipation of the adversary's best response.

Optimal inference attack

The adversary tries to minimize the error of the inference algorithm. If function $d(\widehat{N}, N)$ determines the error in estimating real name N by the adversary, she will try to minimize the error function $d(\widehat{N}, N)$ to optimize the inference attack. However, a user tries to maximize function $d(\widehat{N}, N)$ to protect his privacy. The adversary's expected error function can be computed as mentioned in (4.13).

$$\sum_{N,o,\widehat{N}} p(o|N).q(\widehat{N}|o).d(\widehat{N}, N) \tag{4.13}$$

To optimize the inference attack, the adversary minimizes the expected error function as illustrated in (4.14).

$$q^* = \underset{q}{argmin} \sum_{N,o,\widehat{N}} p(o|N).q(\widehat{N}|o).d(\widehat{N}, N) \tag{4.14}$$

Optimal utility function

To optimize the utility function, the user needs to minimize the utility cost of name encryption. However, the optimal utility function should consider the privacy constraint corresponding to the user's chosen privacy level. Therefore, the problem can be formulated as mentioned in (4.15).

$$\begin{aligned} p^* = \underset{p}{argmin} \sum_{N,o} p(o|N).c(o|N) \\ s.t. \sum_{N,o,\widehat{N}} p(o|N).q^*(\widehat{N}|o).d(\widehat{N}, N) \geq d_m \end{aligned} \tag{4.15}$$

However, to solve (4.15), we need to know q^*, and to get q^* from (4.14), we need to know p^*. Therefore, the solution of one equation is required for another equation. This problem reflects the concept of the best response of two players in game theory model. To break this loop, we use the game theory model, and since the optimization formula for an adversary and a user is different, we model this problem as a nonzero-sum Stacklberg game. We can prove that the best strategy for the user can be achieved by using the linear programming mentioned as (4.16).

$$\begin{aligned} p^* = \underset{p}{argmin} \sum_{N,o} p(o|N).c(o|N) \\ s.t. \sum_{N} p(o|N).d(\widehat{N}, N) \geq x(o), \forall o, \widehat{N} \\ \sum_{o} x(o) \geq d_m \end{aligned} \tag{4.16}$$

Where $x(o)$ can be calculated as (4.17).

$$\begin{aligned} x(o) = \underset{\widehat{N}}{argmin} \sum_{N} p(o|N).d(\widehat{N}, N) \\ or \\ x(o) \leq \sum_{N} p(o|N).d(\widehat{N}, N) \end{aligned} \tag{4.17}$$

4.8 Security analysis

In NDN, name is a common identifier used for both interest and content messages, and the name can reveal substantial information that can endanger users' privacy. We assume that the data (content) is encrypted with the provider's key or using the obfuscated name as key so only legitimate users or the users who know the name can decrypt it. As mentioned earlier, we assume that the adversary can access traffic channel between users and providers (act as an eavesdropper).

We also consider an adversary who can access users, routers, and can compromise multiple routers and users. However, we assume a reasonable level of privacy protection using our two-layer privacy protection mechanism. In this section, we discuss how each layer of privacy protection can combat different kinds of attacks separately and then jointly.

4.8.1 Name obfuscation

In the first layer of privacy protection, the name is obfuscated either partially or fully. The user may also have the option of not obfuscating the name at all.

lemma 1

First layer of privacy protection can mitigate the dictionary attacks or brute force attacks.

proof 1

The proposed name obfuscation method is inspired by MLE encryption. However, this encryption technique can still be vulnerable to a brute force attack. The reason behind this is that any one can generate the key from the name. To address this vulnerability, we use multiple key servers to generate keys using the name and a secret key. Moreover, the encryption process is via oblivious transfer, implying that 1) the key servers are not privy to any information about the name and 2) the user is not privy to any information about the secret key. Therefore, the adversary would need to compromise the key-generating servers; knowing the content name alone would not serve the purpose.

corollary a

Utilizing MLE principles, the proposed name obfuscation method is secure for unpredictable names.

lemma 2

The proposed method offers resistance to the compromise of upto t number of nodes. t may be the total number of users, key servers, or both.

proof 2

As described earlier in Section 4.6, since we use shared signatures of $t+1$ servers, the method is effective for up to t servers. This is because any subset of $t+1$ servers can generate valid signatures but the subset of t or less key servers cannot. However, we assume that the dealer generating public keys, shared keys, and verification keys is the "trusted party". If the dealer gets compromised, the security of the obfuscation layer degrades to the general security level of MLE which is secure for unpredictable names.

It must be noted that the first privacy layer, i.e., the name obfuscation privacy protection does not offer secrecy against inference of similar names, as the obfuscated versions of two identical names shall be identical.

lemma 3

The proposed method prevents an attacker to correlate different obfuscated versions of the specific interest message (including interests with partially and/or fully obfuscated names) with the corresponding data message.

proof 3

In the proposed method, the provider can provision different obfuscation formats for the interest name and the corresponding content. In other words, different obfuscated versions of one specific interest message correspond to different encrypted versions of the same content. Therefore, an adversary cannot link different interest versions with the same data. However, if the provider uses only one obfuscated version of the name for a specific content, e.g., if it is a fully obfuscated name, then the consumer must also use the fully obfuscated name to express their interest for that content.

4.8.2 Gateway routing

In the second layer of privacy, gateways are used between the user and the edge router to prevent the linkage between the interest (specifying the content name) and the user.

lemma 4

An adversary can link a name with a user if they are able to compromise the name obfuscation, and are either able to eavesdrop on the interest in transit or compromise the edge router. The second layer of privacy protection can prevent such inferences.

proof 4

The number of gateways is directly proportional to an adversary's error of estimation of the above mentioned "link" between a user and her interest.

The last gateway may be able to see the name, but is unable to link it with the user who requested it, as the gateway routing is based on onion routing.

lemma 5

The second layer of privacy protection can mitigate frequency attacks where an attacker can understand the user's interest by eavesdropping on the user's encrypted request and accessing the cache of routers.

proof 5

We assume that attackers know the popularity distribution of the content in the local area and can access the cache of the edge router to map encrypted data to the corresponding plaintext. The attacker can estimate ρ by sorting encrypted contents based on their popularity distribution which is the total number of requests for a given content. Also, with auxiliary information about the popularity of contents in the local area, the attacker can compute π and calculate α to map the encrypted content to the corresponding plaintext form. However, the proposed method can create mismatching between π and α. This is due to the fact that users can hide a request for the specific content from the local cache by applying the second layer of protection. Therefore, the attackers see the different request distribution of contents from the real one that makes unlinkability between π and α.

In order to demonstrate Lemma 5 in practice, we measure unlinkability with different number of users who adopt additional privacy protection mechanism in Fig. 4.4. In the simulation, we assumed that the local cache includes 100 encrypted contents, and these contents are sorted based on the maximum request that they have received which is randomly distributed between one and the maximum request rate. As shown in Fig. 4.4, in our proposed method, once the concerned users decide to use a privacy level, they can mitigate the frequency attack significantly by disordering the frequency distribution of encrypted cached content. We change the maximum number of users adopting privacy-preserving mechanism from 20% to 60%, and show the proposed method can create unlinkability and mismatching between encrypted data and plaintext data from 80% to 93% respectively. It is noticeable that even with only maximum 20% of the total number of users, the proposed method can gain 80% unlinkability between ρ and π that an inference attacker can compute. Furthermore, as illustrated in Fig. 4.4, the percent of unlinkability increases as the maximum number of requests decreases. This is due to the fact that when the differences between the number of requests of the cached contents are reduced by only a few numbers of users who are more concerned about privacy and apply the second privacy layer, the probability of mismatching between ρ and π will rise.

corollary b

If the final gateway also happens to be the producer of the requested content, then the proposed method can provide strong privacy, as the final gateway (producer) would be the only one to see the name.

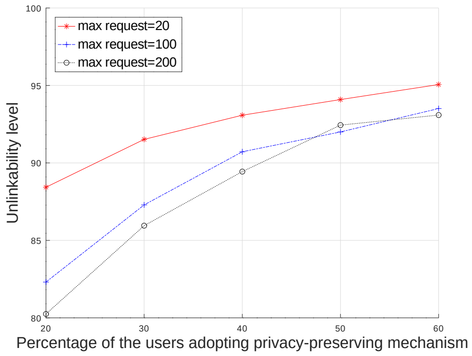


Figure 4.4: Percentage of unlinkability between ρ and π with changing maximum privacy concerned users.

Table 4.2: Simulation Parameters

Parameter	Scenario I	Scenario II
Network access layer protocol	Point to Point	Point to Point
Traffic type	CBR, Zipf	CBR, Zipf
Zipf:α	0.9	0.9
Zipf: total number of content	100	100
Request rate (Interest packets/second)	100	100
Number of consumers	4	10
Number of providers	1	1
Data size (byte)	1024	1024
Simulation time (sec)	20	20

4.9 Evaluation

This section covers the network simulations performed using the ndnSIM package [93] which implements the basic component of NDN in a modular way. We used the RocketFuel topology which is a well known topology widely used in previous works [112][77]. As shown in Fig. 4.5, the topology includes 169 leaf nodes (red circle), 45 routers (green circle), and 65 backbone nodes (blue circle). We selected a backbone node as a producer and leaf nodes as consumers. We used Cisco 4000 family Integrated Service Routers (ISRs) which run multiple concurrent services including encryption and traffic management in addition to the traditional routing services such as computing, forwarding, and caching. The ISR 4461 model includes 10 Gbps performance and 7 Gbps encrypted throughput. Therefore, the AES encryption and decryption delay for onion based routing are negligible against network packet

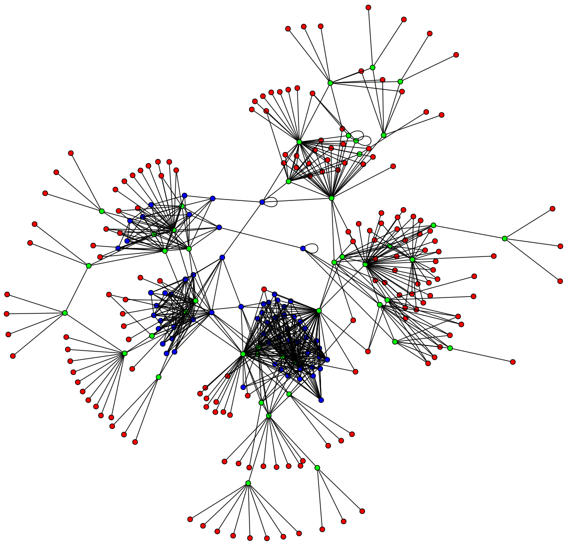


Figure 4.5: Rocketfuel topology with 169 leaf nodes (red), 45 routers (green), and 65 backbone nodes (blue).

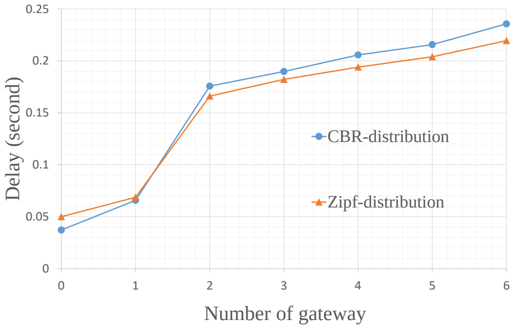


Figure 4.6: Average end-to-end delay for a consumer with changing privacy levels

forwarding delay. Moreover, we consider the fact that in onion routing, the delay caused by threshold signature computation and sharing keys with gateways are dependent on consumer system’s capabilities and is independent of the routing delay caused by message forwarding. Hence, we only evaluate the routing delay, i.e., the delay caused by forwarding of messages in the network, ignoring the cryptographical computation time.

The simulation parameters are listed in Table 4.2. The consumer's traffic follows two distributions namely Constant Bit Rate (CBR) and Zipf. While in the CBR distribution, a consumer requests data and sends interest message with constant rate, in Zipf distribution, the consumer sends request with rate that follows Zipf's law (based on related discrete power law probability distributions). Also, it is

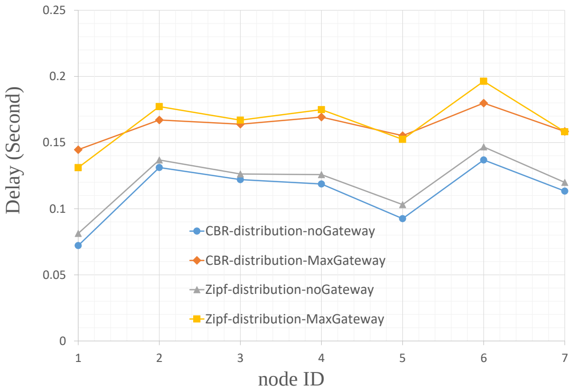


Figure 4.7: Average end-to-end delay for seven nodes with the maximum and minimum privacy levels using gateways

assumed that every router in the network can act as a gateway. In other words, each intermediate router in the Rocketfuel topology can act as:

(a) a normal router using its cache to fetch data for encrypted messages (which does not use unique encryption)

or

(b) a gateway which cannot use its cache for encrypted messages and merely forwards an encrypted requested message to the next hop.

The following two scenarios were used for evaluation:

Scenario I: In this scenario, we considered one producer and four consumers that sent similar requests with two distributions: CBR and Zipf. The delay metric (representing delay between sending first interest message and receiving corresponding data message) is evaluated for a consumer by changing her security level. As shown in Fig. 4.6, the delay is directly proportional to the security level. Since the distance between the consumer and the producer was seven hops in this experiment, the maximum security level could include six gateways. It is noteworthy that in the absence of any privacy consideration, the consumer could get data from the producer directly. However, for any security level less than the maximum of six hops, the data can be fetched from intermediate routers to minimize the delay.

Scenario II: In this scenario, we considered one producer and ten consumers that sent similar requests with two distributions: CBR and Zipf. In this scenario, we evaluated delay for seven consumers with node ID from one to seven for minimum and maximum security levels. While the minimum privacy level for all consumers implied that number of gateways was constant i.e., zero, the maximum level varied with the maximum number of hops available between a user and the producer. When the

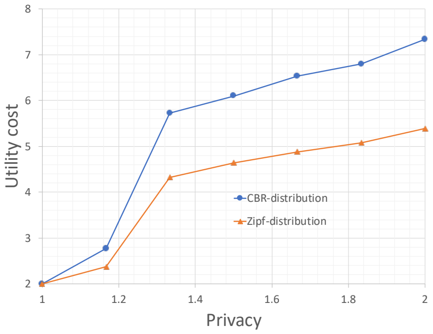


Figure 4.8: Utility cost vs privacy for a consumer in *Scenario I*

maximum level of privacy was selected, data was fetched directly from the producer (not intermediate caches). As illustrated in Fig. 4.7, the average delay in receiving data packets for the maximum privacy level (for all consumers) is higher than that for the minimum privacy level. It is assumed that in the scenarios under consideration, data had been cached in intermediate routers to cater for the consumers who did not use the gateways. However, when a consumer with the maximum level of privacy requested a content for the very first time in the network, she had to experience higher computational delays (compared to what she would with lower privacy levels). This is due to the fact that in such a case, the consumer had no option but to fetch data directly from the producer (irrespective of the minimum or maximum privacy level selection). Moreover, as shown in Fig. 4.7, although both distributions depict similar behaviour, for most consumers Zipf has a higher average delay compared to CBR. This is because in the CBR distribution, evaluated consumers always requested data which had been previously requested by other consumers. In the Zipf distribution, the evaluated consumers requested data that was not requested and hence not cached earlier.

4.10 Conclusion

In this chapter, we explored name privacy in NDN through name obfuscation and gateway-oriented onion routing. Privacy and utility are optimally chosen by the user (or application) using the utility function.

User privacy is a critical aspect of NDN confidentiality and the users may have variable needs of privacy based on the nature of content they intend to access. Based on this premise we enable the user to choose from different levels of privacy related to two aspects, i.e., the name itself and its correlation with the user. The hierarchy of the name is maintained in the proposed mechanism. We used Rocketfuel topology in ndnSIM to measure the privacy protection level and the consequential network delay. For future work, other simulation topologies as well as real life test beds of these simulations can help us verify the effectiveness of our solution with the required trade-off between user's utility and privacy. Further work may also identify the impact of different users choosing different levels of privacy (name obfuscation and gateways) upon the delay and hence utility function, for the same name and content.

The next chapter bridges the gap between technology and business. We transition to the quantitative measurement of qualitative variables affecting the choice of a possible future internet architecture.

Chapter 5

Design inputs for a future internet architecture

In the previous chapters of this thesis, we presented specific technical problems related to availability, integrity, and confidentiality (privacy) in CCN and their respective proposed solutions. In this chapter, we transition from the technical evaluation to the translation of some qualitative non-functional and functional requirements into quantitative parameters so that their impact can be measured as precisely as possible to factor into the design of a future internet architecture.

5.1 Functional and non-functional requirements

As previously mentioned in Section 1.2 of Chapter 1, the constantly evolving diversity of modern-day content and of the devices accessing it and the dynamically evolving needs of scalability, accessibility, affordability, security, and privacy etc., have been indicating the need for a future Internet architecture for quite some time.

It is also worthwhile to mention here that whether a requirement is functional or non-functional is essentially a contextual fact. What may be a functional requirement for one technical concept or product, might be non-functional for another, e.g., privacy, delay, and availability, etc. In the software language some may argue [14] that "A functional requirement describes what a software system should do, while non-functional requirements place constraints on how the system will do so". However, in an architectural design phase, the *how* and *what* are interdependent. The design through all its stages, must be informed by the functionality and vice versa. Moreover, internal factors such as delay and external factors whether quantitative (such as cost of raw materials to build a 5G tower) or qualitative (such as ease of usage generating value for the end user) are equally salient and must be considered in any architectural design. These considerations are undoubtedly logical for the design of a future internet architecture for reasons mentioned earlier in

Section 1.2 of Chapter 1.

Non-functional requirements cover a wide variety of issues and have been traditionally mentioned in terms of software quality [42]. They are sometimes referred to as “ilities or -ities”. Table 5.1 enlists some of the non-functional requirements salient to a future internet architecture, including a few from previous works such as by Gomes et al. [71] and by Chung et al. [42].

acceptability	accessibility	accountability
accuracy	adaptability	additivity
adjustability	affordability	agility
auditability	availability	capability
capacity	clarity	commonality
compatibility	composability	comprehensibility
conceptuality	confidentiality	controllability
dependability	disposability	distributivity
enhanceability	extensibility	feasibility
flexibility	generality	inspect-ability
integrity	inter-operability	learnability
longevity	modifiability	nomadicity
operability	productivity	profitability
promptness	reconfigurability	re-engineering ability
replaceability	responsiveness	safety
scalability	security	simplicity
stability	supportability	susceptibility
sustainability	timeliness	trainability
usability	variability	visibility

Table 5.1: Some *ilities*

5.2 System Dynamics

To incorporate the quantitative and qualitative, functional, and non-functional parameters and to measure their time-sensitive impact on any system simultaneously, business System Dynamics (SD) [5] modelling is the most appropriate tool available: SD can be used to understand the nonlinear behaviour of complex systems over time using stocks, flows, internal feedback loops, table functions, and time delays.

System Dynamics is a methodology and mathematical modeling technique to frame, understand, and discuss complex issues and problems. Originally developed in the 1950s to help corporate managers improve their understanding of industrial processes, SD is currently being used throughout the public and private sector for policy analysis and design.

Convenient graphical user interface (GUI) System Dynamics software developed into user friendly versions by the 1990s and have been applied to diverse systems. SD models solve the problem of simultaneity (mutual causation) by updating all variables in small time increments with positive and negative feedbacks and time delays structuring the interactions and control. The best known SD model is probably the 1972 *The Limits to Growth*. This model forecast that exponential growth of population and capital, with finite resource sources and sinks and perception delays, would lead to economic collapse during the 21st century under a wide variety of growth scenarios.

System dynamics is an aspect of systems theory as a method to understand the dynamic behavior of complex systems. The basis of the method is the recognition that the structure of any system, the many circular, interlocking, sometimes time-delayed relationships among its components, is often just as important in determining its behavior as the individual components themselves. Examples are *chaos theory* and *social dynamics*. It is also claimed that because there are often properties-of-the-whole which cannot be found among the properties-of-the-elements, in some cases the behavior of the whole cannot be explained in terms of the behavior of the parts.

5.3 An example of System Dynamics modelling

Earlier in this chapter Section 5.1 enlisted some of the non-functional requirements for a prospective future internet architecture. The previous Section 5.2 described system dynamics modelling. The following sections of this chapter present an example for the evaluation of these non-functional requirements using system dynamics modelling. System Dynamics [5] is a computer-aided approach to policy analysis and design. It applies to dynamic problems arising in complex social, managerial, economic, and ecological systems—literally any dynamic systems characterized by interdependence, mutual interaction, information feedback, and circular causality.

Coopetition: The new-age panacea for enabling service provider sustainability and profitability

The marvels of fascinating technological advancements in the telecommunications industry are shaping the human social fabric, politics, economics, and national and global development. The telecommunications industry has been the most dynamic and volatile during the last three decades. Evolution of mobile technology has revolutionized human communication across the world. The access of Internet through mobile phones has raised the usage and reach of Internet to a colossal scale.

The wireless ecosystem is more complex than the wired Internet. All of the key players in the ecosystem such as service providers or bit-pipe providers, end-user device manufacturers, core equipment providers, content providers, and application developers, as well as the end users are all interdependent. This diverse ecosystem encourages new technological and business joint ventures; collaborative innovations to enable new service offerings resulting in platform enrichment, and in turn delivering more value to the consumers. This complexity presents new challenges, effects, and remunerations. It also demands revision of business models, identification of collaborative innovation/coopetition opportunities, and strategic evolution of the value chain players.

The SD analysis presented in this chapter is conceived and presented in layers. The background layer is the analysis and study of the existing and evolving value chain of the telecommunications industry which includes device manufacturers, content developers and providers, fixed line and wireless communication providers. Three case studies were evaluated to extract lessons about *collaborative innovation* and *user experience control* as the front layers, later superimposed in the aggregated model to draw conclusions. It is essential to note that the inferences from this work are takeaways for any player in the value chain of the telecommunications industry. The rest of this chapter is organized as follows:

Section 5.4 describes the research methodology. Three case studies are evaluated in Sections 5.5, 5.6, and 5.7. Section 5.8 presents the aggregated model combining the overlapping and unique parameters identified in the three cases studies. Section 5.9 sums up the inferences derived from the work presented on these case studies. Section 5.10 describes the significance of socio-economic modelling for the design of a future internet architecture. Section 5.11 describes an initiative aimed at providing affordable Internet connectivity for the masses. Sections 5.12, 5.13, 5.14, and 5.15 showcase causal loop diagrams for the system dynamics modelling of the parameters salient to the new-age technology stakeholders, and Section 5.16 points towards the possible future extensions of this research.

5.4 Research methodology

Interviews

Around two hundred and fifty formal and informal interviews were conducted with representatives of various key players and stakeholders across the telecommunications value chain from USA and Europe. The work focusing on the three case studies presented in this builds on and extends the work submitted for my M.Sc. dissertation [78]. However, it is imperative to clarify the substantial differences. Although the case studies are the same as in the M.Sc thesis, and some of the data (from 50 interviews) was re-used, extra data (from 200 interviews) was further collected and re-analysed. The interviewees included chief operating officers, strategy heads, managers, research lab personnel, operational engineers and application developers from service providers, wireless and wireline telecom operators, content developers, infrastructure providers, and device manufacturers. As the majority of the interviewees did not consent to publishing their names and company affiliations for considerations of privacy and following professional ethics to respect the confidentiality of their companies' information, their names and affiliations are not explicitly mentioned in the thesis. Moreover, although the same basic method (i.e., system dynamics modelling) is applied, it is to a different problem and data, so produces different knowledge, specially in correlation to the technical work presented in the rest of this thesis. While the MSc. thesis [78] discussed the strategies for monetization of Quality of Service of data by cellular operators, the current thesis has a completely different context, i.e., to analyze the availability, integrity, and confidentiality in CCN internet architectures.

We formulated the interview questions to gauge the direction and trends of the telecommunications industry in general and the experimentation and innovation in the mobile technology and services in particular. Some of the questions were designed to determine the trends of the telecommunications value chain. For example, 80% of the stakeholders agreed that voice was becoming a commodity. Research and development teams of 90% of the service providers were working on value added services, which required relaxation from the regulatory authorities.

Case Studies

Three case studies were used to analyse the common parameters listed in section in general and the "User Experience Control" and "Collaborative Innovation" in particular. These case studies are:

1. Zero.facebook.com, where Facebook collaborated with Mobile Network Operators (MNOs) around the world to bundle a stripped down Facebook application version with a mobile connection.

2. Collaboration between Google Voice and Sprint where Sprint added OTT Google Voice minutes to its mobile plans.

3. NTT DoCoMo's i-mode, which served as a revolutionary concept in mobile services, as a traditional mobile operator reshaped the consumer experience through customized service offerings and by getting involved in almost all sectors of the telecommunication value chain.

Though individually unique and mutually disparate, the above listed three case studies have been chosen as premises of this research work in an attempt to represent the diverse issues salient to *coopetition*.

Modelling

We used SD modelling to evaluate the three case studies (mentioned in the previous section) and then combined the salient variables together in the aggregated model. The causal loop diagrams that have been simplified and trimmed to capture significant aspects of the three individual cases studies are presented in upcoming sections of this chapter. The aggregated model as presented in Section 5.8 was simulated to test the inferences and endorse or dismiss the intuitions governed by the common parameters extracted from the three case studies.

5.5 Zero.facebook.com

The zero.facebook.com initiative is Facebook's attempt to replicate the initial viral effect success story of Facebook.

The original reason for Facebook's quick success at Harvard [124] was that it provided the students a platform to interact and connect with new people at school, filling the void of being away from their families. A Facebook user could easily acquire a substantial amount of information about a potential friend (another Facebook user) through the Internet. Soon after Facebook's inception, it faced the decision of ending the exclusivity of the social network by providing access to everyone; a decision that could make or break the new enterprise due to issues of brand dilution, server space, and soaring costs associated with the expansion. Existing advertising revenue was insufficient to cover the substantial costs of expanding the network, so Facebook allowed access to anyone over thirteen years of age who wanted to join the popular social network. Soon after, Facebook allowed anyone to write programmes to run on it. There was no fee or permission required to write and run these applications on Facebook. Thousands of applications thus developed kept pace with the expanding network. This decision added an extra dimension to ways in which a Facebook profile could be utilized [81], thus providing a vast and inexpensive gateway to business users, who could now use the online social networking world to advertise and expand their businesses.

Zero.facebook.com and Mobile Network Operators (MNOs)

In emerging Internet markets, Facebook collaborated with MNOs in a quest to associate a new mobile internet user's first encounter with mobile data connectivity exclusively with her first Facebook experience. The case study of zero.facebook.com is a clear example of application-specific mobile Internet traffic discrimination, and a subtle example of traffic prioritization. In this case, Facebook, an application provider, collaborated with the existing and emerging mobile operators, to help them expand their subscriber base. Primarily, this is an initiative taken by Facebook as an idea sold to mobile operators. The idea stems out of Facebook's intention to become the symbol of Internet for the new social networking application users as they join the mobile Internet experience. Two of the significant challenges associated with the mobile Internet usage are slow data transfers and costly and complex data plans. These factors can deter the users from using the mobile Internet frequently and seamlessly. Facebook designed zero.facebook.com to help solve these two barriers with the hope that even more people will discover the mobile Internet lured by Facebook's brand appeal, recognition, and the need of association with it. Zero.facebook.com is the stripped down version of the social networking application. It is Wireless Application Protocol (WAP) based, hence lightweight and does not consume a large amount of data bandwidth. The access to zero.facebook.com is free, i.e., it does not get charged against the mobile Internet data traffic quota.

The incentive for Facebook is that the users bond with Facebook in a unique way, as they associate the Internet experience through Facebook. The incentive for the mobile operators is to get new subscriptions and introduce the mobile data services to these new users or the existing customers. In exchange, the mobile operator charges the user for data connectivity required to access and upload pictures, and non-Facebook Internet access requirements.

The zero.facebook.com site was launched in 2010 in collaboration with 50 operators that Facebook partnered with. People could still access Facebook from the standard mobile site m.facebook.com or Facebook mobile site for touch screen mobile devices, touch.facebook.com, under their operator's standard data charges.

Causal loop diagram for zero.facebook.com

The causal loop diagram in Fig. 5.1 primarily depicts reinforcing loops, which show benefit for both MNO and Facebook.

Basics of the SD causal loop diagrams

The arrows represent the causal relationship between two variables. The arrow points from the cause towards the effect. The +ve sign shows that there is a positive correlation or a reinforcing correlation between the two variables. For example, there is a +ve arrow connecting the new mobile subscriptions to the MNO profitability. This positive correlation implies that when the new mobile subscriptions increase, the MNO profitability

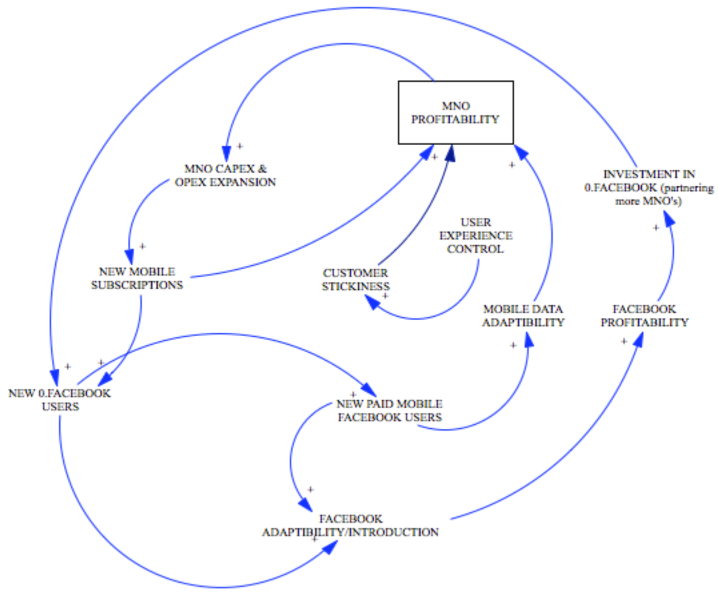


Figure 5.1: Causal loop diagram for zero.facebook.com

increases. We use a rectangular box for MNO because it is a *stock* variable in our model. In SD [113] terminology, a variable is called a *stock*, when it has a fixed value at one point in time, the inflows coming into it increase its value and the outflows leaving it decrease its value. There are two primary loops in this diagram; the exterior loop representing the Facebook profitability and the interior loop representing the MNO's profitability. Facebook's profitability is dependent upon the number of connected Facebook users. MNO's profitability is dependent on the number of subscribers as well as the subscribers who are paying for the mobile data connectivity. Hence, the common profit driving variable for both Facebook and MNO profitability is *new paid Facebook mobile users*. This means that as the number of *new paid Facebook mobile users* increases, both the Facebook and MNO *profitability* increase.

This case study exemplifies collaborative innovation between two incumbents namely Facebook and MNOs. User experience control and customer stickiness (also termed as customer loyalty in this thesis), are the significant links of this causal loop diagram.

Lessons learned from zero.facebook.com

Application alacrity

Zero.facebook.com included all the key features of the standard mobile site m.facebook.com. Users could update their status, view their News Feed, like or comment on posts, send and reply to messages, or write on their friends' Facebook page/wall just as they would on Facebook.com. Zero.facebook was Wireless Application Protocol (WAP) based, hence it was lightweight and efficient. Instead of making the photos viewable on zero.facebook.com, they were kept one click away so they do not slow down the experience. Users could still view any photos on Facebook if they wanted but in that case their regular mobile data fees were applicable.

Zero cost

Facebook collaborated with MNOs to ensure that people can access zero.facebook.com without any data charges. Using zero.facebook.com was completely free. Users only paid for data charges when they viewed photos or when they left zero.facebook.com to browse other mobile sites. When they clicked to view a photo or browse another mobile site, a notification page would appear to forewarn of an associated charge.

User experience control

The number of Facebook users has been astronomical. In April 2016 [123], Facebook was the most popular social networking site in the world, based on the number of active user accounts. Facebook had more than two billion monthly active users in June 2017 [123] and 2.41 billion [57] monthly active users on Facebook on 30th June 2019.

As evident from the above numbers social media led by Facebook has drastically affected the way humans communicate. Users' personal and professional lives have been reshaped to the extent that even brain activity is being fundamentally altered [39]. Sparrow et al. [111] observed that "we are becoming symbiotic with our computer tools, growing into interconnected systems that remember less by knowing information than by knowing where the information can be found". Kirkpatrick [51] labels Facebook as "a technological powerhouse with unprecedented influence across modern life, both public and private". He notes that in conjunction with other social media vehicles spawned in Facebook's aftermath, it offers individual liberation as well as a "safety in numbers" aspect that can potentially affect social change in a variety of ways, ranging from organizing political movements and protests in Columbia [51], to connecting the separated family members and loved ones in a variety of ways; one such example being the aftermath of the Japanese earthquake and tsunami [104]. Zero.facebook.com used the same idea of shaping the user experience in emerging mobile markets by associating itself with the mobile user's first Internet experience. It is noteworthy that this was only accomplished through collaborative innovation with MNOs.

5.6 Google Voice and Sprint

This case study is an example of coopetition enabling value chain evolution, where an Over the Top (OTT) application is embraced by a MNO to create a mutually beneficial

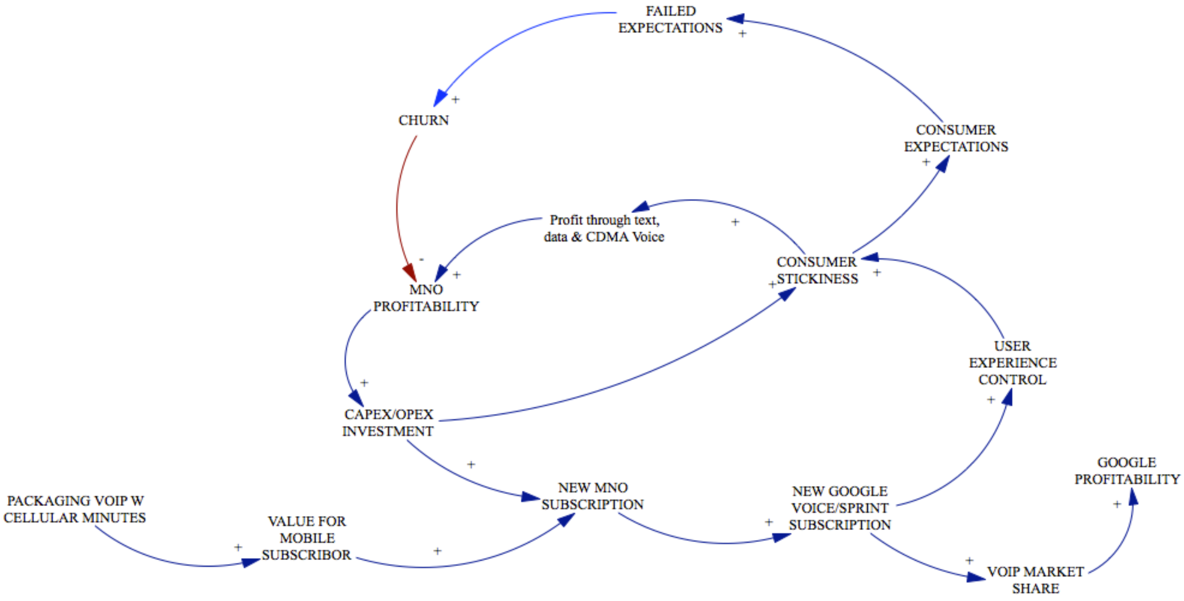


Figure 5.2: Causal loop diagram for Google Voice and Sprint

value added service to attract more customers.

Google Voice took the innovative route and encroached on U.S. mobile operators' turf, even offering to port a user's carrier assigned mobile number for a $20 fee for use with Google Voice service. But for one carrier, i.e. Sprint, the potential friction turned into a partnership. On 20th March 2011, Sprint and Google announced deep integration with Google Voice that allowed subscribers to use their Sprint phone number as a Google Voice number to access the service features. Features offered included transcribed visual voice mail (manage voice messages similar to e-mails), call forwarding (calls ring through on subscribers' cell phone, home phone, office phone, Gmail inbox and so on), custom voice mail greetings, and competitive international calling rates, among other additional offerings. Anyone could sign up for the free Google Voice service before, but Sprint-Google Voice agreement brought forth a few notable exclusive benefits. First, Sprint simplified getting on board with Google Voice. Previously, Google Voice users on any carrier needed to walk through a number of steps to either get a new Google Voice number, port their existing mobile number, or let Google handle just the voice mail. The results could be confusing and cumbersome, with friends often collecting multiple phone numbers for a contact, depending on several factors, including if the Google Voice user had a feature phone, or used a Google Voice mobile application or website from a smart phone. As a second benefit, all Google Voice calls originate from the same single number; the one first issued by Sprint. Third, if you enable Google Voice, the service replaced Sprint's voice mailbox on your phone, so dialling “1” from the handset dialled up your Google Voice message inbox. No additional set up on the Internet VoIP (Voice over IP) application would be required. Fourth, Sprint smart phones get most Google Voice features without requiring a mobile app. Mobile texting is one exception to this last point, however, Sprint's rates and plans still apply for messages sent from the phone's default texting program. Google Voice texts remain free to the United States and Canada if sent from the Web or from a Google Voice smartphone application.

5.6.1 Causal loop diagram for Google-Voice and Sprint

The −ve polarity arrow shown with red color in the Fig. 5.2 originating from *churn* and leading to MNO profitability shows the simple negative causal relationship between these two variables; as *churn* increases the MNO profitability decreases. Packaging VoIP with cellular minutes increases the Value for Mobile Subscriber, which in turn increases the *new MNO subscription.* As the *consumer stickiness* increased in this case, so did the *consumer expectations* from the service offering. The *integration failure issues* led to a rise in *failed expectations*, which increased the *churn.*

5.6.2 Lessons learned from Google-Voice and Sprint case study

Coopetition

This case study is an effective example of coopetition between an OTT VoIP service provider and Mobile Network Operator (MNO). Sprint collaborated with its traditional value chain competitor Google Voice. The ease of integration and price effectiveness provided value for end user and increased subscriptions for both Google Voice and Sprint. Hence, the first lesson to be learned from this case study is that competitors using different technologies can actually act as complimenters.

Integration failures

Integration failures observed in this case study present a good example of possible pitfalls in collaborative ventures. Technical interface integration issues between Google Voice and Sprint for the international roaming mobile users, and lack of integration in the texting/Short Messaging Service (SMS), resulted in failure to meet user expectations. The *collaborative failure rate* increased, decreasing the *value for mobile subscriber* and in turn reducing *customer stickiness/loyalty.* It is noteworthy that this setback did not affect Google Voice revenue much because of it being an OTT platform. Internet users and non-Sprint subscribers could still use Google Voice and map the Google Voice number to other mobile carriers. Another significant factor is that Google itself had other service offerings to sustain itself and Google Voice was willing to share similar collaborations with other mobile operators. Sprint, however had a setback since they were already losing

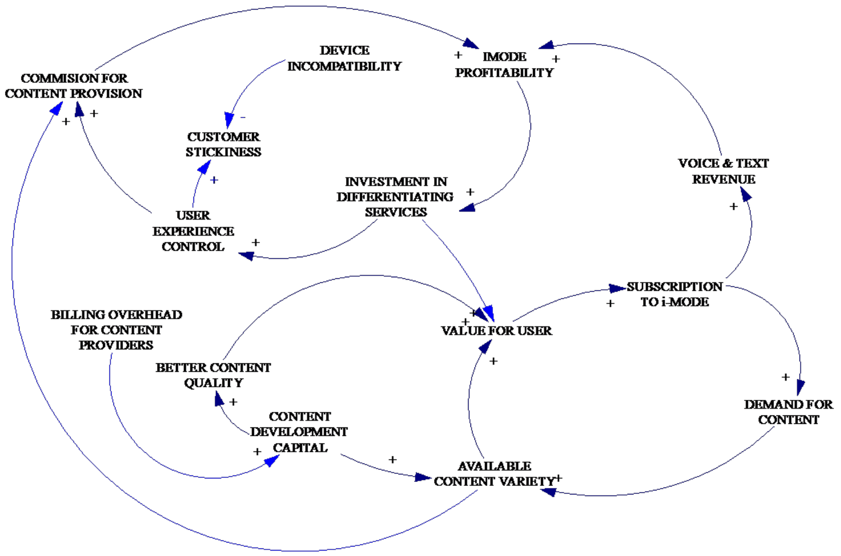


Figure 5.3: Causal loop diagram for NTT DoCoMo's i-mode

revenue on regular mobile subscriptions and voice minutes. The MNOs are expected to provide seamless support over their network including any new value added services. This observation is endorsed by the aggregated model, presented in Section 5.8.

Negative feedback from user experience control

The Google Voice-Sprint venture's most prominent selling point was its low price. The international roaming integration failures caused the consumers to pay more because they were forced to use the Sprint mobile minutes instead of low-priced Google-Voice minutes while travelling overseas. This reduced the value for end user and magnified the *sense of entrapment* that is incorporated in the *perception of intrusiveness* parameter in the final aggregated model presented in Section 5.8. While a platform offers benefits of exclusivity, it can also backfire, if the users are unable to enjoy the benefits of other free services available in the market. A similar setback was witnessed in the next case study of NTT DoCoMo's i-mode.

5.7 NTT DoCoMo i-mode

In this case study, the years under observation are between 1999 and 2007, which were the peak years of NTT DoCoMo i-mode's success and subsequent setbacks. In 1999, the Japanese population numbered 126 million. Of this 126 million, only 12.2 % of the population had Internet access, compared with 39 % of the US population, 21 % of the British population, and 23 % of the Korean population.

Despite the relatively low prevalence and popularity of Internet usage, the mobile handset usage and popularity was far ahead in Japan as compared to other industrially developed countries. At the end of 1999, 44.5% of the Japanese population had mobile phones, compared with 40% in the UK, and 31% in the USA. Dial-up telephone access was expensive in Japan and consumers were obsessed with media and information access; information ranging from daily stock exchange rates to weather updates to latest comic publications. These facts presented Japanese market as an ideal stage [97] to sell a reasonably priced mobile data service targeted towards specified segments of users with the content and information of their choice, available on their mobile handsets round the clock.

Despite the uniqueness of Japanese regulatory controls and the monopolistic situation NTT DoCoMo enjoyed, it improvised as an operator to jump ahead in the value chain by providing content availability and Internet experience to customers in a unique fashion.

By 1990, the Japanese mobile market had enjoyed meteoritic growth at a pace unmatched by any other country in the world. In the latter half of 1990, the Japanese mobile market was on the verge of reaching maturity, even though not complete saturation, when NTT DoCoMo developed a novel service in the form of an innovative mobile Internet platform with the aim of promoting a further evolution in mobile communications. The i-mode service was launched in 1999 attracting overwhelming support from mobile phone users. i-mode not only created new profitability in the mature mobile phone market, but also redefined mobile communications for the new age by providing users with an incomparable service. NTT DoCoMo's i-mode proved to be a revolutionary walled garden mobile Internet service in Japan. It offered the users a wide variety of services, including web access, e-mail and the packet-switched network that delivered the data. i-mode users could access services such as e-mail, sports, weather forecast, games, financial services and ticket booking through a customized interface called i-Menu.

The primary reason for i-mode's soaring initial success was the outstanding convenience it offered to end users and its business model. The business model for i-mode was unique and innovative spanning the entire mobile Internet value chain. It synchronized all value chain aspects related to the user experience control, such as choice and quality of content and Internet subscription. The consolidated billing system allowed DoCoMo to collect information-access fees on behalf of i-Menu-listed content providers. NTT DoCoMo's i-mode collaborated closely with equipment manufacturers, content providers, and other platforms to ensure that wireless technology, content quality, and user experience evolve jointly. This synchronization guaranteed that customers, partners and shareholders shared interests with end-users, thus enabling all parties to maximize value and improve the services.

In contrast with the Wireless Application Protocol (WAP) standard used for the website zero.facebook.com, i-mode utilized fixed Internet data formats such as C-HTML based on

HTML, as well as DoCoMo proprietary protocols ALP (HTTP) and TLP (TCP, UDP). i-mode phones had a special i-mode button for the user to access the start menu. There were more than 12,000 official sites and around 100,000 or more unofficial i-mode sites, which were not linked to DoCoMo's i-mode portal page and DoCoMo's billing services. NTT DoCoMo supervised the content and operations of all official i-mode sites, most of which were commercial. These official sites were accessed through DoCoMo's i-mode menu but in many cases official sites could also be accessed from mobile phones by typing the URL or through the use of QR code (a barcode).

NTT DoCoMo authorized all i-Menu content, while quality was maintained by setting high operability standards and offering quality services. Other content providers complemented these services via their own sites as demand dictated. The i-mode service was thus energized by attracting more subscribers and by adding high-quality content.

The operator NTT DoCoMo controlled the user pricing and billing by collecting monthly information charges for the i-Menu listed content providers via a consolidated bill for all mobile phone activities, thus eliminating the need for provider billing. This arrangement reduced expenses for the content partners and encouraged them to generate high-quality offerings to attract new subscribers, thereby boosting their profits. Additionally, NTT DoCoMo was able to generate incremental revenue by charging a small commission for the billing service. Peak profit years were between 1999 to 2006; with over 22 million subscribers within the first two years. By the middle of 2001, within a short span of two years, i-mode had signed up nearly 20 % of the total Japanese population, or 25% of the population between the ages of 15 and 64, and became the mostly widely used mobile Internet service in the world.

Causal loop diagram for NTT DoCoMo i-mode

In Fig. 5.3 *device incompatibility* has a negative relationship with *customer stickiness*, whereas the user experience control is positively correlated with *customer stickiness. Available content variety* and *better content quality* drive an increase in the *value for user* which in turn increases the *subscription to i-mode.* In Fig. 5.3 the *i-mode profitability* is represented as a variable whereas the content provider is gaining the benefit of collaboration through the increase in *content development capital.*

Lessons Learned from i-mode

Shaping User Experience Control

NTT DoCoMo's i-mode presents an ideally vivid example of shaping and controlling user experience by using technology. NTT DoCoMo had an existing customer base as a traditional MNO, and its content designers were familiar with the demands of Japanese market on a segment-by-segment basis. DoCoMo leveraged the existing customer base and the user profiling advantage to identify potential customers, design targeted services based on customer interests (financial markets, comic strips, and cartoons, etc.), and shape consumer experience. Key to i-mode's success was its collaboration with device manufacturers and content developers.

Value for end user

Characterized by the traditional slow transmission speed of the mobile Internet access in the late '90s, i-mode's successful strategy was to offer more value to the users compared to what they were used to getting from the traditional wireline Internet Service Providers (ISPs). Unlike the ISPs, i-mode charged the users based on the amount of information downloaded and not the connection time. For example, emails cost 1 Japanese Yen per 20 Japanese characters (40 Roman letters), downloading still images cost 7 Yen, checking stock prices cost 26 Yen, and transferring funds from bank accounts cost 60 Yen. While some of i-mode's content providers charged a flat monthly fee, others were free of charge. In 1999, i-mode charged a basic monthly fee of 300 Yen ($3.5) and a packet fee (based on the volume of data sent or received) of 0.3 Yen per 128 bytes of information. i-mode also priced the mobile phone handsets reasonably in comparison to other mobile phones available in the market.

An i-mode user paid for both sent and received data. Unsolicited emails could be avoided through the email service hence making the cost fair. In addition to low price, the billing method was also convenient for users. Instead of paying i-mode for service fees and paying the content providers for subscription fees, i-mode customers received one monthly bill with all of their mobile charges.

Collaborative innovation based on user needs

One target market that intrigued Takeshi Natsuno, Executive Director of NTT DoCoMo [27], included consumers interested in the financial markets and their own personal finances. To appeal to this group, i-mode developed relationships with the banking industry. According to Natsuno, of the more than 700 content partners they had, 320 were banks. Another target market comprised customers with an eye for comics. To serve this segment, i-mode contracted the publishing firm Shueisha to provide weekly comic strips for a monthly fee of 300 Yen (less than $4) for the transmission of a weekly comic strip. The toy company Bandai sold charappa or cartoon characters. For less than $2 a month, subscribers received a different cartoon image on their phone every day. By February 2000, Bandai had 400,000 i-mode subscribers.

As Natsuno said [27], "the success of i-mode is because we adjust our site to Internet users". Furthermore, unlike a dial-up Internet connection, i-mode web access was always on, allowing customers to use the Internet without dialling the phone. Even the phones were appealing to the Japanese market, with color screens, lightweight handsets, multi-link navigation and better graphics capabilities. According to Mullins [97], the only disadvantage of the product was its transmission speed of 9.6 kilobytes per second.

Win-win arrangement with content providers

NTT DoCoMo's insight into the needs of its content providers was an important contributor to its early success. By taking care of the customer billing, i-mode made business easy for content providers, who were hesitant to sell online (because of the expensive and cumbersome billing process). By outsourcing the billing to NTT DoCoMo, content providers were able to concentrate on what they did best i.e., providing content, and still generate earnings. In return for this, i-mode charged its content providers 9% of the revenue.

The company kept a firm grip on its business, controlling all aspects of the i-mode service. Unlike some European promoters of WAP (as used by zero.facebook.com), DoCoMo knew that developing content would be crucial. DoCoMo required its content providers to create entirely new content fit for the mobile phone. DoCoMo's success did not depend on its technology, which actually was not state-of-the-art, but in its ability to bring together and direct all these services shaping and controlling the user experience.

The Achilles heel of a global trendsetter

A few months after DoCoMo launched i-mode in February 1999 [89], DoCoMo's competitors launched very similar mobile data services: KDDI launched EZweb, and J-Phone launched J-Sky. Vodafone later acquired J-Phone including J-Sky, renaming the service Vodafone live!. Seeing the tremendous success of i-mode in Japan, many operators in Europe, Asia and Australia sought to license the service through a partnership with DoCoMo. The quick success encouraged more operators to launch i-mode in their markets [27] and the footprint reached 17 countries by 2017.

While i-mode was an exceptional service that positioned DoCoMo as a global leader in value added services, the real success contributors for i-mode were the Japanese smartphone manufacturers who developed state of the art handsets to support i-mode. As i-mode was exported to the rest of the world, Nokia and other major handset vendors who controlled the markets at the time, refused to manufacture i-mode compatible handsets. The operators who decided to launch i-mode had to rely on Japanese vendors who had no experience in international markets. As i-mode showed success in these markets, a few known vendors started customizing some of their handsets to support i-mode. However, the support was only partial and came much later than required.

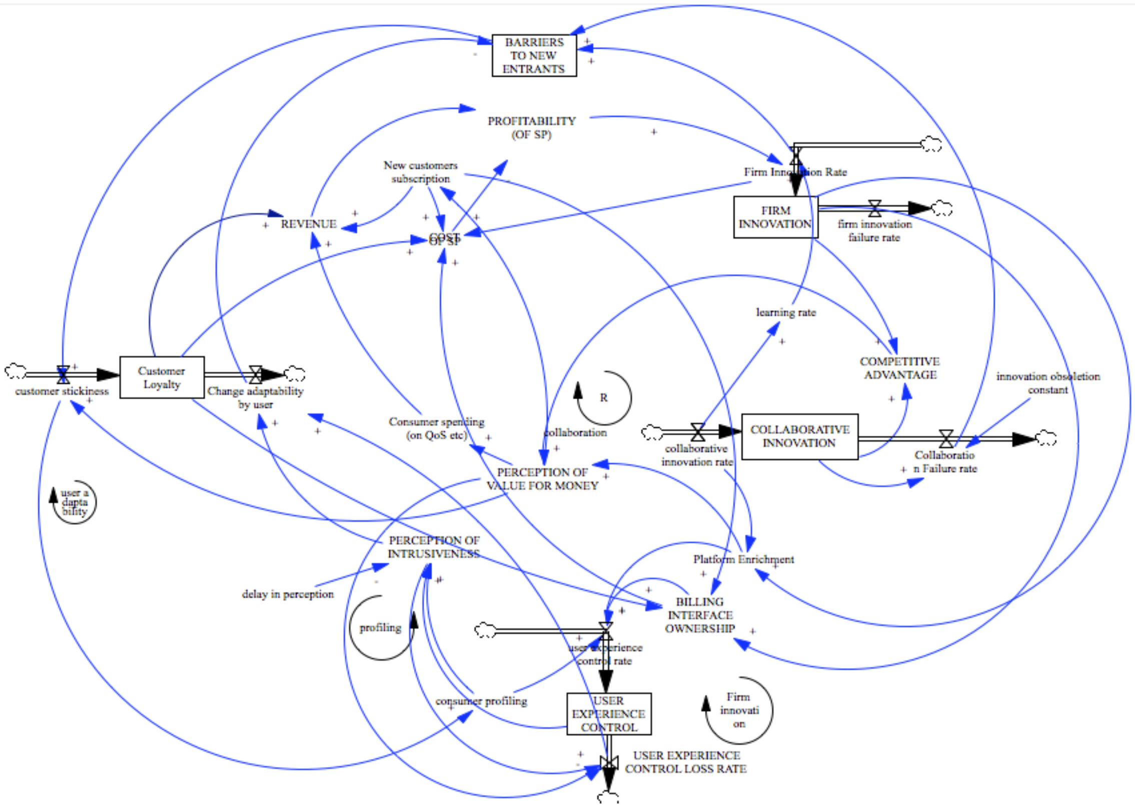

BARRIERS TO NEW ENTRANTS
PROFITABILITY (OF SP)
New customers subscription
REVENUE
COST OF SP
Firm Innovation Rate
FIRM INNOVATION
firm innovation failure rate
learning rate
COMPETITIVE ADVANTAGE
innovation obsoletion constant
customer stickiness
Customer Loyalty
Change adaptability by user
Consumer spending (on QoS etc)
R
collaboration
collaborative innovation rate
COLLABORATIVE INNOVATION
Collaboration Failure rate
PERCEPTION OF VALUE FOR MONEY
user adaptability
PERCEPTION OF INTRUSIVENESS
delay in perception
profiling
Platform Enrichment
BILLING INTERFACE OWNERSHIP
user experience control rate
consumer profiling
USER EXPERIENCE CONTROL
Firm innovation
USER EXPERIENCE CONTROL LOSS RATE

Figure 5.4: The aggregated model with loops

Consequently, the lack of “i-mode compatible handsets” (and the emerging popularity of new handsets [54] most of which did not support i-mode), proved to be i-mode’s Achilles heel and led to its downfall.

5.8 The aggregated model

Based on the lessons learned from the three case studies described in the previous Sections 5.5, 5.6, and 5.7, and the individual causal loop diagrams depicted in Fig. 5.1, 5.2, and 5.3, an aggregated model was developed as illustrated in Fig. 5.4. Fig. 5.4 depicts the causal loop structures while Fig. 5.5 uses Shadow variables for the ease of understanding the parameter interconnections and dependencies. A **Shadow variable** is a copy of a system dynamics variable used to reduce the complexity of the diagram and overlapping of arrows. Following are some of the important parameters used in the aggregated model:

Firm innovation

Firm innovation can be described as the innovation that a firm develops in-house. This could be measured in the number of inventions, patents or even the new products launched by a firm. However in this model, “service features” are used as the units to measure firm

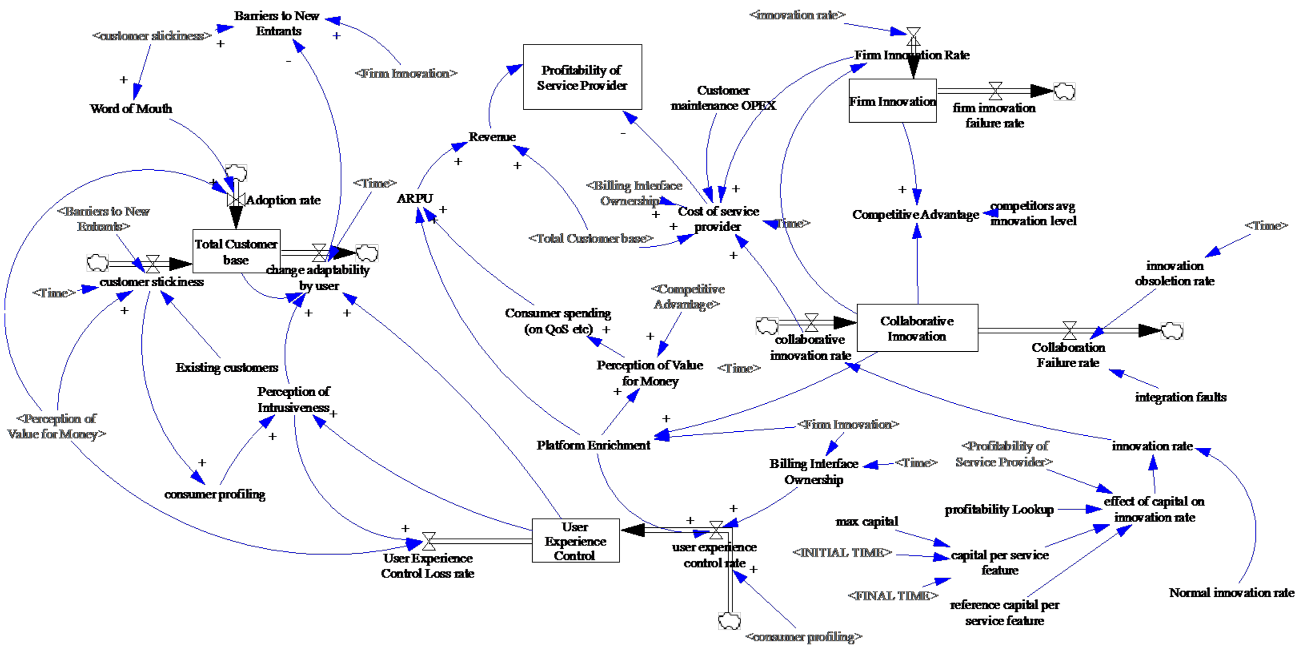
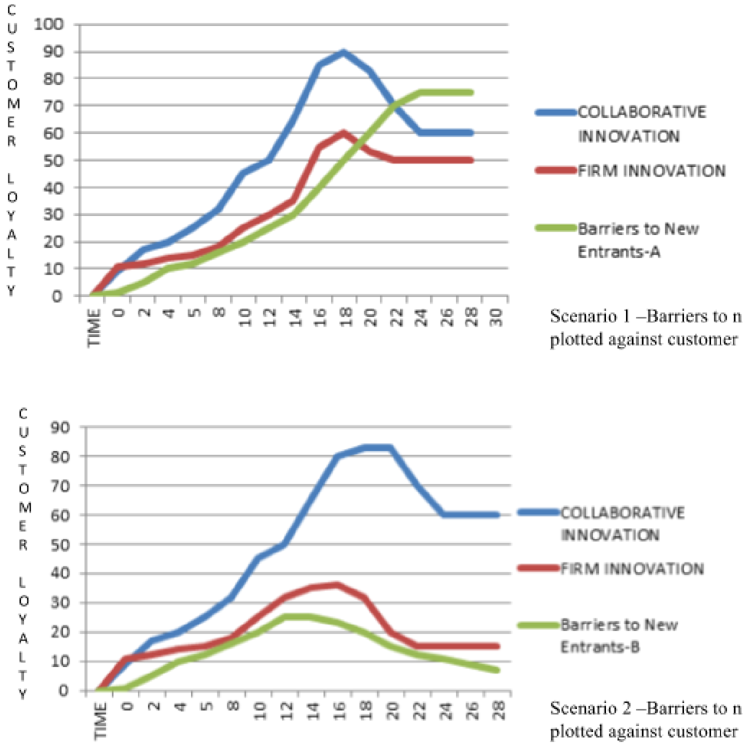

Barriers to New Entrants
<customer stickiness>
<Firm Innovation>
Word of Mouth
Profitability of Service Provider
Customer maintenance OPEX
<innovation rate>
Firm Innovation Rate
Firm Innovation
firm innovation failure rate
Revenue
Adoption rate
<Time>
ARPU
<Billing Interface Ownership>
Cost of service provider
<Barriers to New Entrants>
Total Customer base
change adaptability by user
<Total Customer base>
<Time>
Competitive Advantage
competitors avg innovation level
<Time>
customer stickiness
<Time>
innovation obsoletion rate
<Competitive Advantage>
Consumer spending (on QoS etc)
collaborative innovation rate
Collaborative Innovation
Collaboration Failure rate
Existing customers
Perception of Value for Money
<Time>
integration faults
Perception of Intrusiveness
<Firm Innovation>
<Perception of Value for Money>
Platform Enrichment
<Profitability of Service Provider>
innovation rate
Billing Interface Ownership
<Time>
consumer profiling
profitability Lookup
effect of capital on innovation rate
max capital
User Experience Control
user experience control rate
<INITIAL TIME>
capital per service feature
User Experience Control Loss rate
<FINAL TIME>
reference capital per service feature
Normal innovation rate
<consumer profiling>

Figure 5.5: The aggregated model with Shadow variables (Shadow is a copy of an SD variable used to reduce complexity of the diagram)



Scenario 1 –Barriers to new entrants, firm innovation and collaborative innovation plotted against customer loyalty (customer stickiness) over time

Scenario 2 –Barriers to new entrants, firm innovation and collaborative innovation plotted against customer loyalty (customer stickiness) over time

Figure 5.6: Simulations from the Aggregated Model

innovation.

Collaborative innovation

Collaborative innovation between competitors is coopetition. For this evaluation, we used the parameter of collaborative innovation to measure coopetition. Collaborative innovation is the innovation where two or more organizations combine their resources to either develop a new technology or to launch a new service. Similar to "firm innovation", "collaborative innovation" is measured in units of service features.

User experience control

"User experience control" is a parameter describing the service provider's capability to own and shape a user's experience. Other factors such as consumer profiling and customization of service offerings based on consumer needs, collectively work to enhance user experience control. Traditionally, it was believed that billing interface ownership was the primary criteria for being closely associated with the customer. However, this belief has been challenged repeatedly in the recent years. The results from the model used in our work also endorsed the fact that billing interface ownership might delay the customer churn by some brief time period, but would not ensure customer loyalty by itself in the long run.

Perception of intrusiveness

As obvious from the name, this parameter refers to he consumer's feeling of being intruded upon, which is not only based on the loss of privacy (a possibility in the case of consumer profiling and data mining which probes into the user's consumption of applications and choice of content etc.), but also on the user's perception of confinement or entrapment because of the rigidity of a certain platform or service and the lack of integration opportunities. One such example is the lack of compatibility of i-mode handsets with the open Internet and the non-availability of free content over the i-mode interface.

Additional evaluated parameters

Following is a list of some other parameters used in the aggregated system dynamics model presented in Fig. 5.4 and Fig. 5.5. All functions are mathematical equations governing the relationships between variables used in the model simulations. These equations (available in Appendix A Section A.1 incorporate time delays as integral functions and are formulated based on the data accumulated from interviews, financial records, and market reports related to the case studies.

1. Adoption rate is a function of: Perception of Value for Money as well as Word of Mouth.

2. ARPU (Average Revenue per User) is a function of: Consumer spending as well as Platform Enrichment.
3. Barriers to New Entrants is a function of: Customer stickiness as well as change adaptability by user. This variable can be quantified with considering the other parameters, e.g., the Firm innovation of one player in the value chain.
4. Billing Interface Ownership is a function of: Firm Innovation
5. Capital per service feature is a function of: Maximum capital, which is governed by the profitability of the service provider.
6. Change adaptability by user is a function of: Total Customer base, a positive causal relationship with Perception of Intrusiveness; it has a negative or balancing relationship to User Experience Control.
7. Collaboration Failure rate is a function of: Innovation obsoletion rate as well as integration faults.
8. Collaborative Innovation is a stock or level.
9. Collaborative innovation rate is constant.
10. Competitive Advantage is a function of: Collaborative Innovation as well as Firm Innovation-competitors average innovation level.
11. Consumer profiling is a function of: Customer stickiness.
12. Consumer spending is a function of: Perception of Value for Money.
13. Cost of Service Provider is a function of: Billing Interface Ownership, Total Customer base, Time, Firm Innovation Rate, collaborative innovation rate, Total Customer base and Customer maintenance Operating Expenditure (OPEX).
14. Customer maintenance OPEX is the operational cost of maintaining one customer per month.
15. Customer stickiness is a function of: Barriers to New Entrants, Perception of Value for Money and Existing customers.
16. Effect of capital on innovation rate is a function of: Profitability Lookup, capital per service feature, reference capital per service feature, and Profitability of Service Provider.
17. Existing customers is a constant, which was given values between 1000 to 20 mill]ion for different classes of service providers.
18. FINAL TIME is the final time for the simulation = 2053, Units: year
19. Firm Innovation is a stock with firm innovation rate as inflow and firm innovation failure rate as outflow, Units: service features
20. Firm innovation failure rate is a constant and varying values were utilized for test purposes depending upon the technology and its life-cycle.

5.9 Results

From the case studies described in the earlier sections of this chapter and the related simulations of the aggregated system dynamics model, several results were deduced. Some of these results are listed below:

1. It was concluded that collaborative innovation can improve sustainability and profitability and elevate barriers to new entrants, i.e., deter competition when and if it also contributes to the growth of firm (in-house) innovation.

2. The results from the model used in our work also endorsed the fact that billing interface ownership might delay the customer churn for short time, but would not alone ensure customer loyalty in the long run.

3. Another important conclusion was that platform enrichment (which includes offering new innovative services to customers), increases the perception of value for money, hence increasing user experience control. However, if perception of intrusiveness keeps increasing, then beyond a certain threshold, platform enrichment fails to increase the perception for value for money.

5.10 Socio-economic modelling for a future internet architecture

Socio-economics [65] aims to understand the interplay between the society, economy, markets, institutions, self-interest, and moral commitments. It is a multidisciplinary field using methods from economics, psychology, sociology, history, and even anthropology. Socio-economics of networks have been studied for over 30 years, but mostly in the context of social networks instead of the underlying communication networks. It is imperative to discover, discuss, and evaluate the challenges and perspectives related to "socio-economic" issues to design a well-informed architecture for the future internet. It would lead to new insights on how to structure the architecture and services in the future internet.

As discussed in Chapter 1, the Internet is a remarkable platform enabling creativity, collaboration, and innovation engendering amazing possibilities that would have been impossible to imagine before its advent. If architected proactively with all salient variables duly considered, the future internet could prove to be a source of further advancement in all aspects of human life. One must admit that despite being a "best effort based" and "resource hungry" technological marvel, the Internet has been immensely resilient and dependable. However, the current Internet was never designed to serve massive scale applications with guaranteed quality of service, scalability, and security.

Emerging technologies like high quality video streaming and 3D applications face severe constraints to run seamlessly anytime, everywhere, with good quality of services. In June 2019, out of the approximate 7.7 billion people in the world only 4.5 billion (58.8%) have Internet access [16] implying that global reach is still an ongoing issue. In order to overcome the global digital divide (by providing affordable internet access to the next few billion), new technical and business models must be co-designed to make the future internet more economical, reliable, affordable, sustainable, secure, and hence feasible.

To evaluate the functional and non-functional requirements of a future internet architecture, the qualitative parameters must be quantified in terms of the impact on the dynamics that matter to the service providers who build and manage the infrastructures based on these architectures.

5.11 RIFE

RIFE stands for "architectuRe for an Internet For Everybody (RIFE)" [4]. RIFE was initiated to address the major societal challenge of affordability[1], i.e., providing internet access to those who cannot afford it by solving the technological challenge to increase the efficiency of the underlying transport networks and the involved architectures and protocols. Some of the objectives of RIFE were:

1) to utilize the traditionally unused transmission capacity.

2) to place content caches and service functionality closer to the user.

3) to use heterogeneous transmission opportunities that range from localized mesh and home networks over well-connected ISP backhauls to scarce satellite resources.

RIFE also explored optimized dissemination strategies for ICN/CCN and delay-tolerant networking.

During RIFE's course of three years, RIFE:

1. Deployed an ICN network with 6 super nodes in 6 sites in the Catalonia region of Tarragona, Spain, as illustrated in Fig. 5.7.

2. Advanced insights into the suitability of providing cheaper Internet connectivity through IP-over-ICN given that regular operators are often more expensive in provisioning Internet services in remote locations.

3. Innovated in areas such as surrogate management, multi-casting, and edge caching.

4. Advanced insights into how to stimulate localized service deployments.

5. Advanced insights into the operational complexity of localised service deployments.

[1] one of the non-functional requirements mentioned in Chapter 5

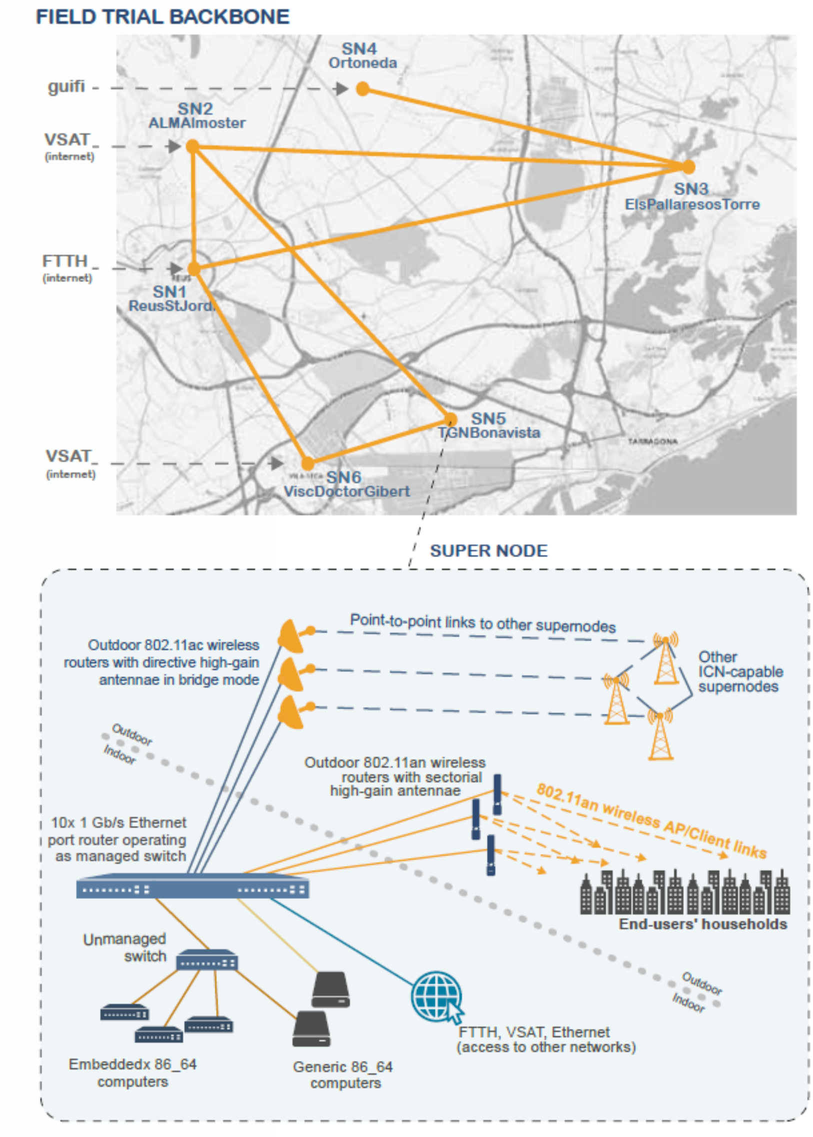

FIELD TRIAL BACKBONE
guifi
VSAT (internet)
FTTH (internet)
VSAT (internet)
SN4 Ortoneda
SN2 ALMAlmoster
SN3 ElsPallaresosTorre
SN1 ReusStJord.
SN5 TGNBonavista
SN6 ViscDoctorGibert
SUPER NODE
Point-to-point links to other supernodes
Outdoor 802.11ac wireless routers with directive high-gain antennae in bridge mode
Other ICN-capable supernodes
Outdoor
Indoor
Outdoor 802.11an wireless routers with sectorial high-gain antennae
802.11an wireless AP/Client links
10x 1 Gb/s Ethernet port router operating as managed switch
End-users' households
Unmanaged switch
Outdoor
Indoor
FTTH, VSAT, Ethernet (access to other networks)
Embeddedx 86_64 computers
Generic 86_64 computers

Figure 5.7: RIFE ICN/CCN Deployment

6. Provided technical guidance to develop the next version of IP-over-ICN

RIFE also developed, deployed, and showcased a real-life setting within a large-scale community network in Spain, demonstrating the technology and economic opportunities provided by the RIFE platform. The real-life test beds were complimented with emulation scenarios to enable the evaluation of novel resource management schemes at scale, while integrating with RIFE's prototype platform. RIFE's long term economic objective is to develop business opportunities for local authorities as well as back-haul network providers to create a sustainable value chain by introducing virtual network operators that utilize the under-used capacity in a new business relationship with local customers, enabling socially-driven business models. The involvement of a technology, equipment, satellite, and/or community network provider would allow to maximize the commercial exploitation of RIFE within real deployments and towards standard communities within the IETF/IRTF and beyond, placing RIFE in the centre of a growing community of practitioners that all share the same goal: making the Internet affordable to everybody. During my PhD, I worked on the RIFE project for a year and used system dynamics for the socio-economic modelling for RIFE. A basic introduction to system dynamics has been provided earlier in this thesis in this chapter in Section 5.2. A few stakeholders and their salient parameters were selected and their primitive mutual causal correlations were identified. The objective for using system dynamics modelling was to validate the socio-economic feasibility of RIFE, and to quantify the foreseen qualitative benefits. SD models/causal loops presented here illustrate initially identified variables/parameters and their long term impact on each other from a RIFE perspective. Four models namely Model A, Model B, Model C, and Model D are presented in this thesis. These models are works in progress as variables are being discovered, added, merged and edited. It is noteworthy that these models are in a nascent stage (causal loops only without defined equations) and are expected to evolve as an extension of my research.

5.12 Model A: Communication service providers and end user stakeholders' dynamics

This model depicts the overall holistic picture with relationships between following major **stakeholders**:

1. Virtual Network Operator (VNO)

2. Mobile Network Operator (MNO)

3. Communication Service Provider (CSP)

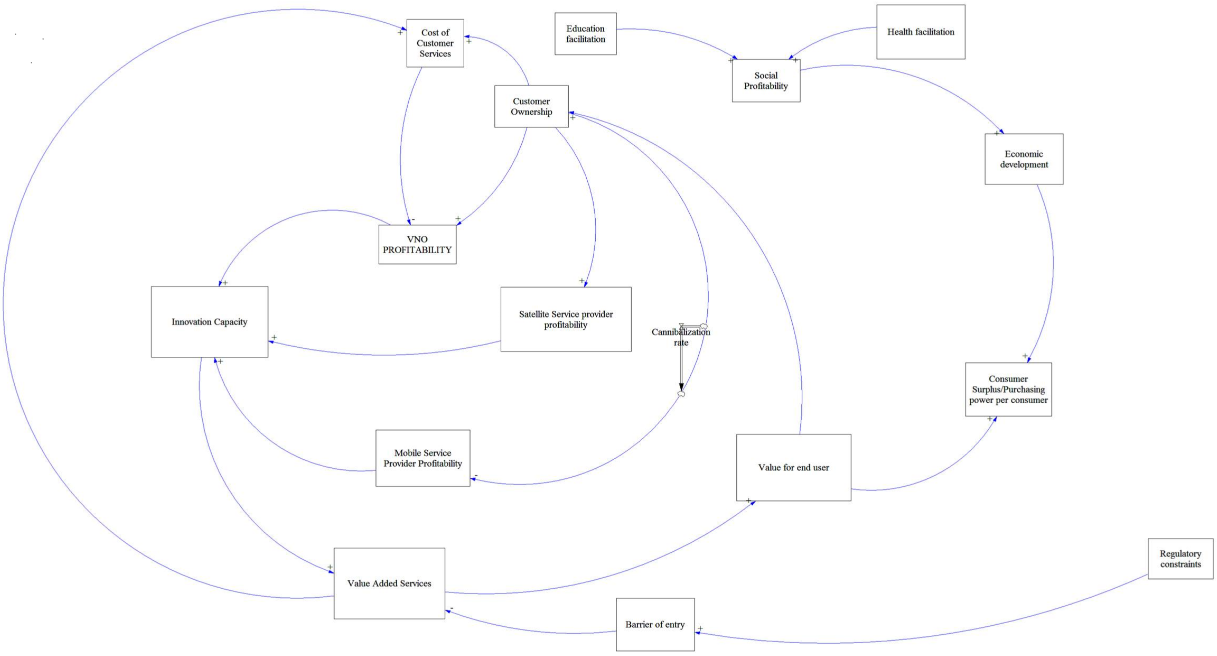


Figure 5.8: Model A: Communication service providers and end user stakeholders' dynamics

4. End user

Variables used in this model are listed below:

1. VNO profitability = profitability of the Virtual Network Operator
2. Customer ownership = the control over user experience e.g. access through billing and customer services
3. Consumer surplus = purchasing power per customer
4. Innovation capacity = the capacity to innovate/ launch a new or disruptive technology
5. Barrier of entry = barrier or deterrent in launching a new service
6. Cannibalization rate = rate at which one new innovation damages the existing business e.g. in this case the VNO service traction destroying the tier-1 primary provider network operator.

   Following variables are self-explanatory

7. Social profitability
8. Economic development
9. Education facilitation

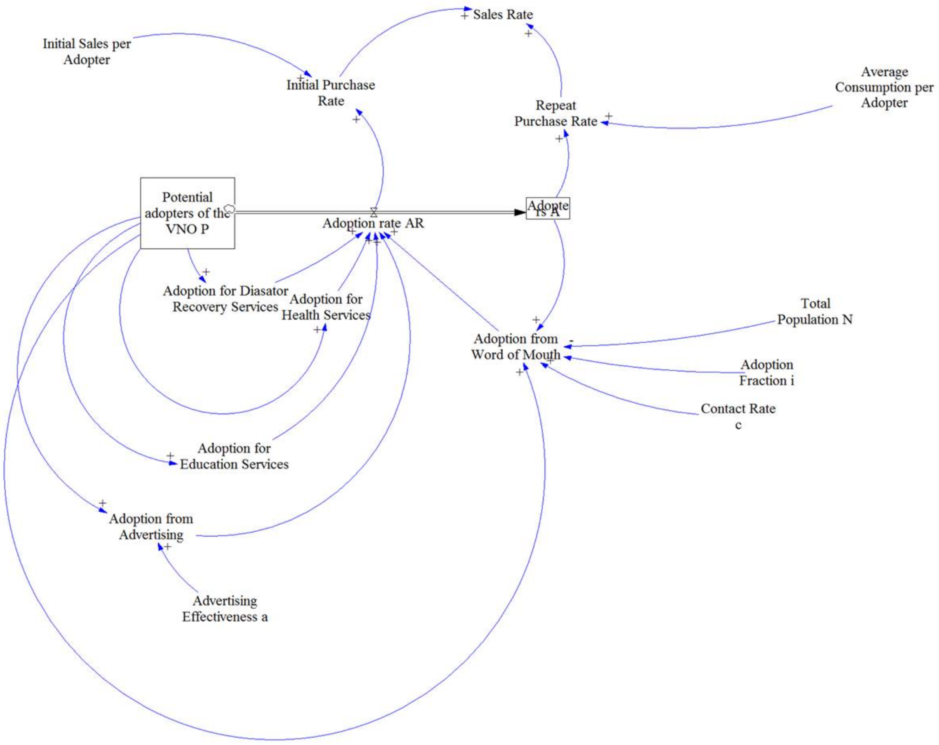

Sales Rate
Initial Sales per Adopter
Initial Purchase Rate
Repeat Purchase Rate
Average Consumption per Adopter
Potential adopters of the VNO P
Adoption rate AR
Adopters A
Adoption for Diasator Recovery Services
Adoption for Health Services
Adoption from Word of Mouth
Total Population N
Adoption Fraction i
Contact Rate c
Adoption for Education Services
Adoption from Advertising
Advertising Effectiveness a

Figure 5.9: Model B: Innovation adoption model

10. Health facilitation
11. MNO profitability
12. Satellite operator's profitability
13. Regulatory constraints

5.13 Model B: Innovation adoption model

Model B is an innovation adoption model for CSP/VNO's role in health and education provisioning. This model utilized the innovation adoption concept which may also be described as the adoption probability or feasibility of a new technology or architecture. This model can be used to test and simulate possible future internet architectures. However, here it is used to evaluate the possibility of a health provider and/or education provider to assume the additional role of VNO or vice versa.

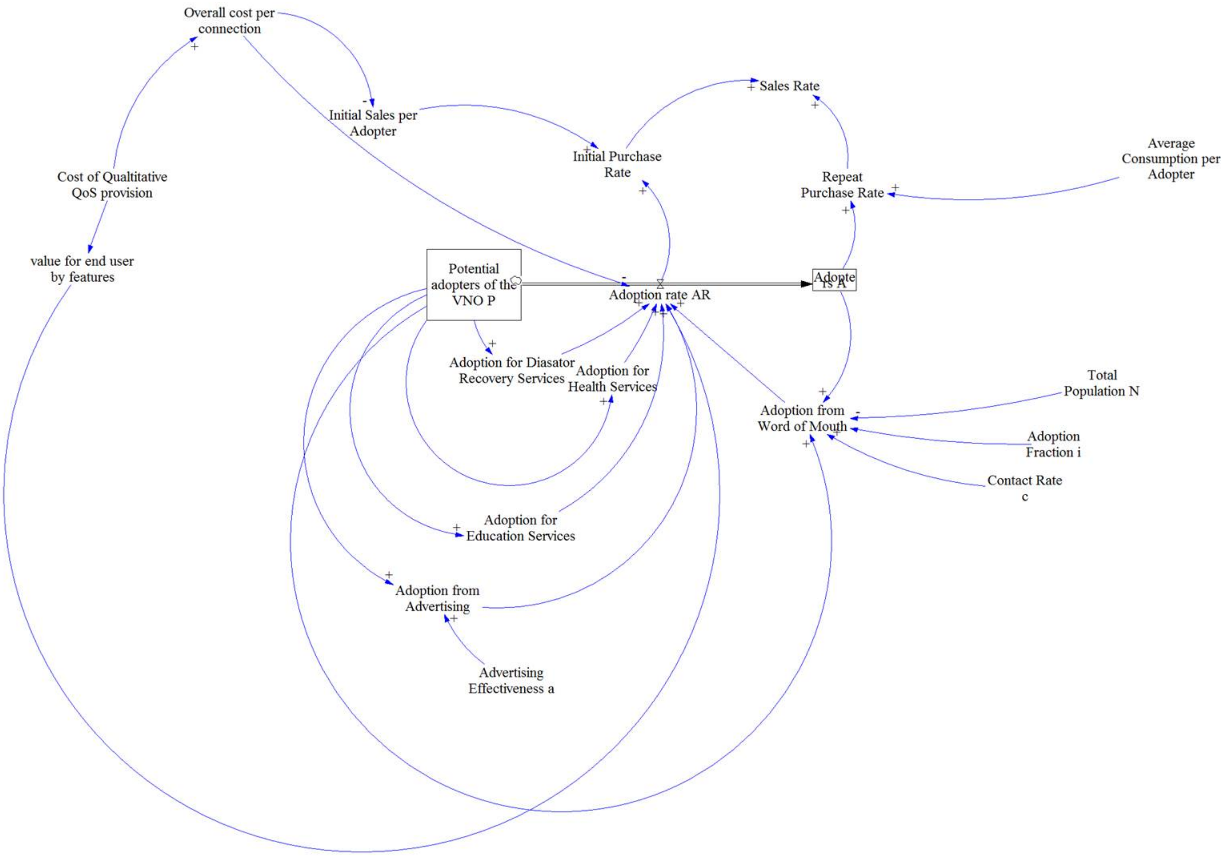

Overall cost per connection
Initial Sales per Adopter
Sales Rate
Initial Purchase Rate
Repeat Purchase Rate
Average Consumption per Adopter
Cost of Qualtitative QoS provision
value for end user by features
Potential adopters of the VNO P
Adoption rate AR
Adopte rs A
Adoption for Diasator Recovery Services
Adoption for Health Services
Adoption from Word of Mouth
Total Population N
Adoption Fraction i
Contact Rate c
Adoption for Education Services
Adoption from Advertising
Advertising Effectiveness a

Figure 5.10: Model C: Health/Education provider as VNO

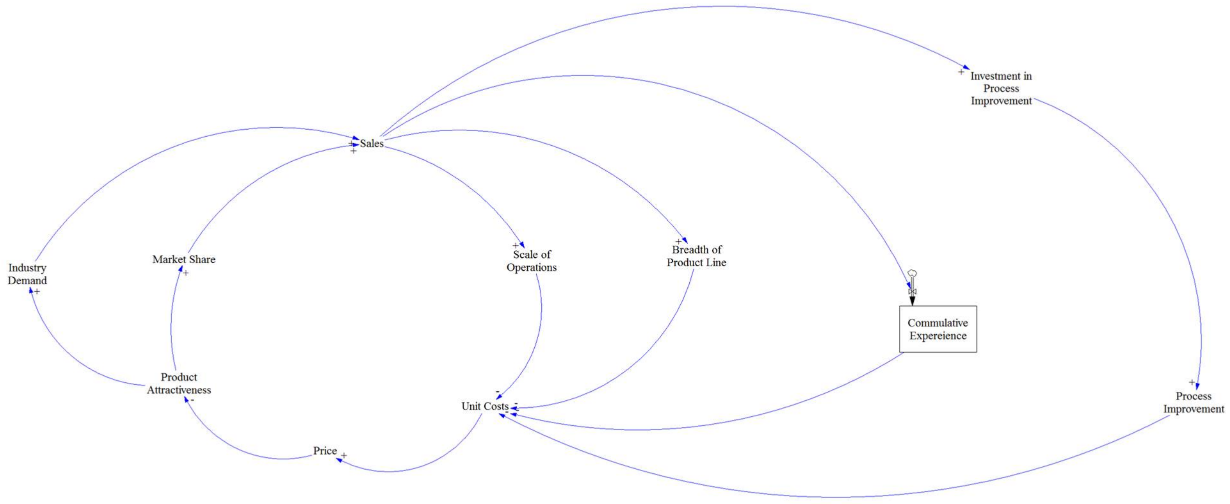


Figure 5.11: Model D: Economies of scale and economies of scope

5.14 Model C: Health/Education provider as CSP/VNO

Model C is a possible extension of the Model B presented in the last section. The main concept is the same, i.e., to evaluate the feasibility of a health provider and/or education provider to assume the additional role of Virtual Network Operator or vice versa. However, the innovation adoption model for VNO's role as Health and/or education provider shows a possible addition of flexible Quality of Service (QoS) provisioning here.

5.15 Model D: Economies of scale and economies of scope

Model D is an attempt to highlight the economies of scale and economies of scope concepts which imply that unit cost can be decreased if the scope is expanded or scale is expanded. This concept has been be derived from the scalability requirements of possible RIFE use cases.

Since two of the most significant *ilities* to be considered while designing a futuristic and future-proof internet architecture are affordability and scalability: we must gauge all prospective future internet proposals on the basis of economies of scale and economies of scope. Economies of scale and economies scope are imperative for a future internet architecture designed to overcome the global digital divide. Fig. 5.11 just depicts a basic causal loop and can be extended by introducing parameters and mathematical correlations salient to the specific internet architectural design as well as the focal stock (primary variable) to be measured.

5.16 Non-functional requirements of CCN and system dynamics modelling

The Chapters 2, 3, and 4 presented challenges to availability, integrity, and confidentiality challenges in NDN; the corresponding proposed solutions are a significant technical contribution towards a secure and trusted future internet architecture. In this chapter, we transitioned from the technical analysis to system dynamics modelling: by assigning values to and then evaluating certain qualitative parameters. Even though it may not be immediately obvious, however, these variables are salient to availability, integrity, and confidentiality of data directly and indirectly. For example, one of the parameters evaluated in the three case studies and aggregated model, i.e., *perception of intrusiveness* can also be alternatively called *privacy sensitivity*. This chapter primarily presented examples of system dynamics modelling through real life case studies. Similar evaluations could measure the impact of functional/non-functional security parameters, such as utility cost of delay, privacy sensitivity, value of availability, and integrity of data as supported by the technical solutions presented in the earlier chapters.

Chapter 6

Conclusions and future work

6.1 Conclusions from the technical evaluations

As specified in Section 1.1 of Chapter 1, the problem statement for this thesis was to evaluate if it is possible to address security requirements including Availability, Integrity, and Confidentiality for Content Centric Networking (CCN). We ventured to do so by evaluating the threats to: 1) Availability of CCN via a DDoS attack, 2) to Integrity of CCN through a content poisoning attack and 3) to Confidentiality of CCN through content name privacy threats, and their respective countermeasures. Following is a brief summary of what was achieved in context of these evaluations for each of these three areas.

1. In Chapter 2 we have considered the IFA DDoS attacks and proposed Kiram as a mitigation mechanism. However, some other DDoS attacks such as Bandwidth Depletion attack, Black-holing by prefix-hijacking, and Reflection attack are mentioned in Section 2.2. For future work we can run ndnSIM simulations for these attacks as well as do real life testing for Kiram for IFA DDoS attacks. Since Kiram is a temporal learning mechanism, a larger network and longer learning time may reveal further benefits of this approach. Further work can also be done to equip the alert message called WOE with more effective and meaningful information.

2. In Chapter 3 we explored the content poisoning attack in NDN and its mitigation through a proposed framework named Iris. We amalgamated and improvised upon the honeypot and exclusion techniques and introduced the reverse MA-ABE technique in Iris. Using these techniques as an intelligent framework, Iris detects the fake content objects, identifies, and isolates the Compromised Consumers, and eventually, the Adversarial Producers. We used AT&T topology over ndnSIM and demonstrated the effectiveness of Iris through extensive simulations. Future work in this area includes extension of trust federations in Iris and its implementation in other CCN

networks. Moreover, we continue to pursue the scalability of Iris through large scale deployments.

3. In Chapter 4, we explored name privacy in NDN through name obfuscation and gateway-oriented onion routing. Privacy and utility are optimally chosen by the user (or application) using the utility function. User privacy is a critical aspect of NDN confidentiality and the users may have variable needs of privacy based on the nature of content they intend to access. Based on this premise, we enable the user to choose from different levels of privacy related to two aspects, i.e., the name itself and its correlation with the user. The hierarchy of the name is maintained in the proposed mechanism. We used Rocketfuel topology in ndnSIM to measure the privacy protection level and the consequential network delay. For future work, other simulation topologies as well as real life test beds of these simulations can help us verify the effectiveness of our solution with the required trade-off between user's utility and privacy. Further work may also identify the impact of different users choosing different levels of privacy (name obfuscation and gateways) for the same content and same content name, upon the delay and hence utility function.

6.2 Conclusions from system dynamics

The thesis problem statement in Section 1.1 of Chapter 1 also stated the possibility of demonstrating that the trade-offs in ensuring the Availability, Integrity, and Confidentiality (AIC) in CCN by countering the salient security threats imply that the previously overlooked non-functional aspects of AIC in CCN could now be quantitatively factored into the design and deployment plans for the prospective future internet architecture.

As discussed in Chapter 5, in order to evaluate the functional and non-functional requirements of a future internet architecture, the qualitative parameters must be quantified in terms of impact on the dynamics that matter to the service providers who build and manage the infrastructures based on these architectures.

The case studies, system dynamics modelling examples, the RIFE work presented in Chapter 5 and future work proposals mentioned in the next Section 6.2.1 focus on quantifying the non-functional elements of future internet architectures; showcasing the significance of taking these pertinent variables into account, in order to remove barriers to the successful uptake and deployment of any prospective internet architecture.

6.2.1 Further System Dynamics evaluations

1. *Parameter evaluation for RIFE socioeconomic models*

Models A,B,C, and D described in Sections 5.12, 5.13, 5.14, and 5.15 are works in progress awaiting further data acquisition which is imperative for identification, addition, and consolidation of new variables salient to the innovation, governance, information security, regulatory, social, and economic aspects of a future internet design.

Next steps involve short-listing and correlating all these variables driving innovation diffusion, profitability, and sustainability of communication service providers. Relevant historical and current data is required to formulate the equations behind the causal relationships.

2. *Evaluation of the Availability, Integrity, and Confidentiality parameters*

   Chapters 2, 3, and 4 of this thesis presented availability, integrity, and confidentiality threats and their corresponding technical mitigation techniques respectively. The next step is to use the quantitative representation of the parameters evaluated (such as cost and delay to evaluate availability) to inform the design decisions for a future-proof internet architecture.

3. *Relevance for other future internet architecture proposals*

   The system dynamics modelling and evaluation approach presented in this thesis can be easily applied to other future internet architecture proposals[1] (e.g., to other ICN architectures, Accountable Internet [28], and I3 [114]) etc. Also as described earlier in this section, there is vast scope of extending this analysis to the numerous variables mentioned in Chapter 5 Table 5.1. By using real world field implementation data for CCN, financial reports from ISPs, and the market analysis as utilized in Chapter 5 (for the three case studies exploring service provider profitability, value for the end user, and collaborative innovation etc.), causal loop diagrams leading to complete System Dynamics models backed by mathematical equations, can be designed and simulated for a desired period of time. The results from these models can be used to inform internet architecture design, policy, legislation, and regulatory decisions for technology architects, policymakers, lawmakers, and regulators, and to launch business strategies for disruptive innovations by internet service providers.

[1] NSF sponsored FIA program in USA and European research initiatives are listed in Chapter 1 Section 1.2 of this thesis

Bibliography

[1] Content Centric Networking project (CCNx). http://www.ccnx.org. Accessed: 2019-03-24.

[2] Named Data Networking project (NDN). http://named-data.org.

[3] Future of Internet Irchitecture (FIA) program. http://http://www.nets-fia.net/. Accessed: 2017-09-24.

[4] About RIFE. https://www.rife-project.eu/about/. Accessed: 2019-09-25.

[5] System Dynamics. https://en.wikipedia.org/wiki/System_dynamics. Accessed: 2019-10-02.

[6] TakNet – a community white space wireless network. https://blog.apnic.net/2019/07/01/taknet-a-community-white-space-wireless-network/. Accessed: 2019-10-27.

[7] Availability. https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. Accessed: 2019-10-27.

[8] A Cisco guide to defending against distributed denial of service attacks. https://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html. Accessed: 2017-09-25.

[9] No. 1 DDoS attack protection. https://www.cloudflare.com. Accessed: 2017-09-25.

[10] Denial of service attack. https://www.britannica.com/technology/denial-of-service-attack. Accessed: 2019-10-27.

[11] History of DDoS attacks. https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/. Accessed: 2019-10-27.

[12] FortiDDoS: Advanced DDoS protection for enterprise data centers. https://www.fortinet.com/products/ddos/fortiddos.html.

[13] guifi.net. https://http://guifi.net. Accessed: 2019-10-27.

[14] What is the difference between functional and non-functional requirements. https://stackoverflow.com/questions/16475979/what-is-the-difference-between-functional-and-non-functional-requirement. Accessed: 2019-10-01.

[15] Vensim. https://vensim.com. Accessed: 2019-10-27.

[16] World internet usage and population statistics 2019 mid-year estimates. https://internetworldstats.com/stats.htm. Accessed: 2019-10-10.

[17] Eslam G AbdAllah, Hossam S Hassanein, and Mohammad Zulkernine. A survey of security attacks in information-centric networking. *IEEE Communications Surveys & Tutorials*, 17(3):1441–1454, 2015.

[18] Gergely Acs, Mauro Conti, Paolo Gasti, Cesar Ghali, and Gene Tsudik. Cache privacy in named-data networking. In *2013 IEEE 33rd International Conference on Distributed Computing Systems*, pages 41–51. IEEE, 2013.

[19] Gergely Acs, Mauro Conti, Paolo Gasti, Cesar Ghali, Gene Tsudik, and Christopher Wood. Privacy-aware caching in information-centric networking. *IEEE Transactions on Dependable and Secure Computing*, 2017.

[20] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang. Interest flooding attack and countermeasures in Named Data Networking. In *2013 IFIP Networking Conference*, pages 1–9, May 2013.

[21] A. Afanasyev, C. Yi, L. Wang, B. Zhang, and L. Zhang. SNAMP: Secure namespace mapping to scale NDN forwarding. In *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 281–286, April 2015. doi: 10.1109/INFCOMW.2015.7179398.

[22] Alexander Afanasyev, Ilya Moiseenko, Lix-ia Zhang, et al. ndnsim: NDN simulator for NS-3. university of california. Technical report, Los Angeles, Tech. Rep, 2012.

[23] Alexander Afanasyev, Cheng Yi, Lan Wang, Beichuan Zhang, and Lixia Zhang. Snamp: Secure namespace mapping to scale NDN forwarding. In *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 281–286. IEEE, 2015.

[24] Akamai. Prevent a DDoS attack with akamai, March 2015. URL https://www.akamai.com/uk/en/resources/ddos-attack.

[25] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park. Black hole attack in mobile ad hoc networks. In *Proceedings of the 42Nd Annual Southeast Regional Conference*, ACM-SE 42, pages 96–97, New York, NY, USA, 2004. ACM. ISBN 1-58113-870-9. doi: 10.1145/986537.986560. URL `http://doi.acm.org/10.1145/986537.986560`.

[26] Moreno Ambrosin, Alberto Compagno, Mauro Conti, Cesar Ghali, and Gene Tsudik. Security and privacy analysis of National Science Foundation Future Internet Architectures. *IEEE Communications Surveys & Tutorials*, 20(2):1418–1442, 2018.

[27] Donald L Amoroso and Mikako Ogawa. Japan's model of mobile ecosystem success: the case of ntt docomo. *Journal of Emerging Knowledge on Emerging Markets*, 3(1): 27, 2011.

[28] David G Andersen, Hari Balakrishnan, Nick Feamster, Teemu Koponen, Daekyeong Moon, and Scott Shenker. Accountable internet Protocol (AIP). In *ACM SIGCOMM Computer Communication Review*, volume 38, pages 339–350. ACM, 2008.

[29] Somaya Arianfar, Teemu Koponen, Barath Raghavan, and Scott Shenker. On preserving privacy in content-oriented networks. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking*, pages 19–24. ACM, 2011.

[30] Hitesh Ballani, Paul Francis, and Xinyang Zhang. A study of prefix hijacking and interception in the internet. In *ACM SIGCOMM Computer Communication Review*, volume 37, pages 265–276. ACM, 2007.

[31] Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, and Till Stegers. Format-preserving encryption. In *International Workshop on Selected Areas in Cryptography*, pages 295–312. Springer, 2009.

[32] Mihir Bellare, Sriram Keelveedhi, and Thomas Ristenpart. Message-locked encryption and secure deduplication. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 296–312. Springer, 2013.

[33] Cesar Bernardini, Samuel Marchal, Muhammad Rizwan Asghar, and Bruno Crispo. Privicn: Privacy-preserving content retrieval in information-centric networking. *Computer Networks*, 149:13–28, 2019.

[34] Andrea Bittau, Michael Hamburg, Mark Handley, David Mazieres, and Dan Boneh. The case for ubiquitous transport-level encryption. USENIX Association, 2010.

[35] Andrea Bittau, Michael Hamburg, MJ Handley, David Mazieres, and Dan Boneh. Simple opportunistic encryption. In *Proc. W3C/IAB workshop on Strengthening the*

Internet Against Pervasive Monitoring (STRINT). World Wide Web Consortium (W3C)/Internet Architecture Board (IAB), 2014.

[36] Andrei Broder and Michael Mitzenmacher. Network applications of bloom filters: A survey. *Internet mathematics*, 1(4):485–509, 2004.

[37] R. Caceres, N. Duffield, A. Feldmann, J. D. Friedmann, A. Greenberg, R. Greer, T. Johnson, C. R. Kalmanek, B. Krishnamurthy, D. Lavelle, P. P. Mishra, J. Rexford, K. K. Ramakrishnan, F. D. True, and J. E. van der Memle. Measurement and analysis of ip network usage and behavior. *IEEE Communications Magazine*, 38(5): 144–151, May 2000. ISSN 0163-6804. doi: 10.1109/35.841839.

[38] Jan Camenisch, Gregory Neven, et al. Simulatable adaptive oblivious transfer. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 573–590. Springer, 2007.

[39] Nicholas Carr. *The shallows: What the Internet is doing to our brains.* WW Norton & Company, 2011.

[40] Abdelberi Chaabane, Emiliano De Cristofaro, Mohamed Ali Kaafar, and Ersin Uzun. Privacy in content-oriented networking: Threats and countermeasures. *ACM SIGCOMM Computer Communication Review*, 43(3):25–33, 2013.

[41] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[42] Lawrence Chung, Brian A Nixon, Eric Yu, and John Mylopoulos. *Non-functional requirements in software engineering*, volume 5. Springer Science & Business Media, 2012.

[43] David D Clark. *Designing an internet.* The MIT Press, 2018.

[44] Ian Clarke, Scott G Miller, Theodore W Hong, Oskar Sandberg, and Brandon Wiley. Protecting free expression online with freenet. *IEEE Internet Computing*, 6(1):40–49, 2002.

[45] A. Compagno, M. Conti, P. Gasti, and G. Tsudik. Poseidon: Mitigating interest flooding DDoS attacks in Named Data Networking. In *38th Annual IEEE Conference on Local Computer Networks*, pages 630–638, Oct 2013. doi: 10.1109/LCN.2013.6761300.

[46] Alberto Compagno, Mauro Conti, Paolo Gasti, and G Tsudikz. NDN interest flooding attacks and countermeasures. In *ACSAC*, 2012.

[47] Alberto Compagno, Mauro Conti, Paolo Gasti, Luigi Vincenzo Mancini, and Gene Tsudik. Violating consumer anonymity: Geo-locating nodes in named data networking. In *International Conference on Applied Cryptography and Network Security*, pages 243–262. Springer, 2015.

[48] Mauro Conti, Paolo Gasti, and Marco Teoli. A lightweight mechanism for detection of cache pollution. 2013.

[49] Manuel Costa, Jon Crowcroft, Miguel Castro, Antony Rowstron, Lidong Zhou, Lintao Zhang, and Paul Barham. Vigilante: End-to-end containment of internet worm epidemics. *ACM Trans. Comput. Syst.*, 26(4):9:1–9:68, December 2008. ISSN 0734-2071. doi: 10.1145/1455258.1455259. URL `http://doi.acm.org/10.1145/1455258.1455259`.

[50] Huichen Dai, Yi Wang, Jindou Fan, and Bin Liu. Mitigate ddos attacks in ndn by interest traceback. In *Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on*, pages 381–386. IEEE, 2013.

[51] Kirkpatrick David. The facebook effect: The inside story of the company that is connecting the world, 2010.

[52] Leiwen Deng, Yan Gao, Yan Chen, and Aleksandar Kuzmanovic. Pollution attacks and defenses for internet caching systems. *Computer Networks*, 52(5):935–956, 2008.

[53] Steven DiBenedetto, Paolo Gasti, Gene Tsudik, and Ersin Uzun. Andana: Anonymous named data networking application. *arXiv preprint arXiv:1112.2205*, 2011.

[54] dictionnaire.sensagent.leparisien. imode. `http://dictionnaire.sensagent.leparisien.fr/I-Mode/en-en/`, september18, 2013.

[55] Yitao Duan. Distributed key generation for encrypted deduplication: Achieving the strongest privacy. In *Proceedings of the 6th edition of the ACM Workshop on Cloud Computing Security*, pages 57–68. ACM, 2014.

[56] Amine Elabidi, Ghazi Ben Ayed, Sonia Mettali Gammar, and Farouk Kamoun. Towards hiding federated digital identity: Stop-dissemination mechanism in content-centric networking. In *Proceedings of the 4th international conference on Security of information and networks*, pages 239–242. ACM, 2011.

[57] Facebook. Our mission. `https://newsroom.fb.com/company-info`, 2019. Accessed: 2019-10-22.

[58] Stephen Farrell and Hannes Tschofenig. Pervasive monitoring is an attack. 2014.

[59] Amos Fiat and Moni Naor. Broadcast encryption. In *Annual International Cryptology Conference*, pages 480–491. Springer, 1993.

[60] Nikos Fotiou, Dirk Trossen, Giannis F Marias, Alexandros Kostopoulos, and George C Polyzos. Enhancing information lookup privacy through homomorphic encryption. *Security and Communication Networks*, 7(12):2804–2814, 2014.

[61] P Gasti, G Tsudik, E Uzun, and L Zhang. DoS & DDoS in named-data networking. arxive-prints. Technical report, Tech Rep 1208.0952 v2, 2012.

[62] Paolo Gasti and Gene Tsudik. Content-centric and named-data networking security: The good, the bad and the rest. In *2018 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, pages 1–6. IEEE, 2018.

[63] Paolo Gasti, Gene Tsudik, Ersin Uzun, and Lixia Zhang. Dos and ddos in named data networking. In *Computer Communications and Networks (ICCCN), 2013 22nd International Conference on*, pages 1–7. IEEE, 2013.

[64] A Geetha and N Sreenath. Byzantine attacks and its security measures in mobile adhoc networks. *IJCCIE 2016*, 2016.

[65] Alex Galis Anastasius Gavras David Hausheer Srdjan Krco Volkmar Lotz Theodore Zahariadis Georgios Tselentis, John Domingue. *Towards the Future Internet A European Research Perspective*, volume 275 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. IOS Press, Nieuwe Hemweg 6B 1013 BG Amsterdam Netherlands fax: +31 20 687 0019 e-mail: order@iospress.nl, 2009. ISBN 978-1-60750-007-0. Fourier integral operators.

[66] Cesar Ghali, Gene Tsudik, and Ersin Uzun. Needle in a haystack: Mitigating content poisoning in named-data networking. In *Proceedings of NDSS Workshop on Security of Emerging Networking Technologies (SENT)*, 2014.

[67] Cesar Ghali, Gene Tsudik, and Ersin Uzun. Network-layer trust in named-data networking. *ACM SIGCOMM Computer Communication Review*, 44(5):12–19, 2014.

[68] Cesar Ghali, Gene Tsudik, and Christopher Wood. (the futility of) data privacy in content-centric networking. In *Proceedings of the ACM on Workshop on Privacy in the Electronic Society*, pages 143–152. ACM, 2016.

[69] Cesar Ghali, Gene Tsudik, and Christopher A Wood. When encryption is not enough: privacy attacks in content-centric networking. In *Proceedings of the 4th ACM Conference on Information-Centric Networking*, pages 1–10, 2017.

[70] Ali Ghodsi, Scott Shenker, Teemu Koponen, Ankit Singla, Barath Raghavan, and James Wilcox. Information-centric networking: Seeing the forest for the trees. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, HotNets-X, pages 1:1–1:6, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-1059-8. doi: 10.1145/2070562.2070563. URL `http://doi.acm.org/10.1145/2070562.2070563`.

[71] Carla Gomes, Thomas Dietterich, Christopher Barrett, Jon Conrad, Bistra Dilkina, Stefano Ermon, Fei Fang, Andrew Farnsworth, Alan Fern, Xiaoli Fern, Daniel Fink, Douglas Fisher, Alexander Flecker, Daniel Freund, Angela Fuller, John Gregoire, John Hopcroft, Steve Kelling, Zico Kolter, Warren Powell, Nicole Sintov, John Selker, Bart Selman, Daniel Sheldon, David Shmoys, Milind Tambe, Weng-Keen Wong, Christopher Wood, Xiaojian Wu, Yexiang Xue, Amulya Yadav, Abdul-Aziz Yakubu, and Mary Lou Zeeman. Computational sustainability: Computing for a better world and a sustainable future. *Commun. ACM*, 62(9):56–65, August 2019. ISSN 0001-0782. doi: 10.1145/3339399. URL `http://doi.acm.org/10.1145/3339399`.

[72] Shon Harris. *CISSP All-in-One Exam Guide*. McGraw-Hill Osborne Media, 6th edition, 2012. ISBN 9780071781749.

[73] John C Harsanyi, Reinhard Selten, et al. A general theory of equilibrium selection in games. *MIT Press Books*, 1, 1988.

[74] Woodrow Hartzog and Frederic Stutzman. Obscurity by design. *Wash. L. Rev.*, 88: 385, 2013.

[75] Oliver Heckmann, Michael Piringer, Jens Schmitt, and Ralf Steinmetz. On realistic network topologies for simulation. In *Proceedings of the ACM SIGCOMM Workshop on Models, Methods and Tools for Reproducible Network Research*, MoMeTools '03, page 28–32, New York, NY, USA, 2003. Association for Computing Machinery. ISBN 1581137486. doi: 10.1145/944773.944779. URL `https://doi.org/10.1145/944773.944779`.

[76] AKM Hoque, Syed Obaid Amin, Adam Alyyan, Beichuan Zhang, Lixia Zhang, and Lan Wang. Nlsr: named-data link state routing protocol. In *Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking*, pages 15–20. ACM, 2013.

[77] Y. Hu, F. Zhang, K. K. Ramakrishnan, and D. Raychaudhuri. Geotopo: A pop-level topology generator for evaluation of future internet architectures. In *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*, pages 90–99, Nov 2015. doi: 10.1109/ICNP.2015.29.

[78] Mohibi Hussain. Collaborative innovation and user experience control-strategies for monetization of qos of data by cellular operators. Master's thesis, Massachusetts Institute of Technology, 2013.

[79] John Ioannidis and Steven M. Bellovin. Pushback: Router-based defense against ddos attacks, 2001.

[80] Van Jacobson, Diana K Smetters, James D Thornton, Michael F Plass, Nicholas H Briggs, and Rebecca L Braynard. Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12. ACM, 2009.

[81] Andreas M Kaplan and Michael Haenlein. Users of the world, unite! the challenges and opportunities of social media. *Business horizons*, 53(1):59–68, 2010.

[82] Sriram Keelveedhi, Mihir Bellare, and Thomas Ristenpart. Dupless: server-aided encryption for deduplicated storage. In *Presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13)*, pages 179–194, 2013.

[83] Dohyung Kim, Sunwook Nam, Jun Bi, and Ikjun Yeom. Efficient content verification in named data networking. In *Proceedings of the 2nd ACM Conference on Information-Centric Networking*, pages 109–116. ACM, 2015.

[84] Mohit Lad, Daniel Massey, Dan Pei, Yiguo Wu, Beichuan Zhang, and Lixia Zhang. Phas: A prefix hijack alert system. In *USENIX Security symposium*, volume 1, page 3, 2006.

[85] Marc Langheinrich. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[86] Tobias Lauinger, Nikolaos Laoutaris, Pablo Rodriguez, Thorsten Strufe, Ernst Biersack, and Engin Kirda. Privacy implications of ubiquitous caching in named data networking architectures. *Technical Report TR-iSecLab-0812-001, ISecLab, Tech. Rep.*, 2012.

[87] Allison Lewko and Brent Waters. Decentralizing attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 568–588. Springer, 2011.

[88] Zhaogeng Li and Jun Bi. Interest cash: an application-based countermeasure against interest flooding for dynamic content in named data networking. In *Proceedings of The Ninth International Conference on Future Internet Technologies*, page 2. ACM, 2014.

[89] Sven Lindmark, Erik Bohlin, and Erik Andersson. Japan's mobile internet success story–facts, myths, lessons and implications. *info*, 6(6):348–358, 2004.

[90] Jian Liu, N Asokan, and Benny Pinkas. Secure deduplication of encrypted data without additional independent servers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 874–885. ACM, 2015.

[91] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. Controlling high bandwidth aggregates in the network. *SIGCOMM Comput. Commun. Rev.*, 32(3):62–73, July 2002. ISSN 0146-4833. doi: 10.1145/571697.571724. URL `http://doi.acm.org/10.1145/571697.571724`.

[92] VP Maslov. The zipf-mandelbrot law: quantization and an application to the stock market. *Russian Journal of Mathematical Physics*, 12(4):483–488, 2005.

[93] Spyridon Mastorakis, Alexander Afanasyev, Ilya Moiseenko, and Lixia Zhang. ndnSIM 2: An updated NDN simulator for NS-3. *Dept. Comput. Sci., Univ. California, Los Angeles, Los Angeles, CA, USA, Tech. Rep. NDN-0028*, 2015. URL `http://named-data.net/techreport/ndn-0028-1-ndnsim-v2.pdf`.

[94] Giulia Mauri, Riccardo Raspadori, Mario Gerlay, and Giacomo Verticale. Exploiting information centric networking to build an attacker-controlled content delivery network. In *Ad Hoc Networking Workshop (MED-HOC-NET), 2015 14th Annual Mediterranean*, pages 1–6. IEEE, 2015.

[95] Medium.com. The holy trinity of data security: What you need to know about the CIA triad. https://medium.com/yobicash/the-holy-trinity-of-data-security-what-you-need-to-know-about-the-cia-triad-d58931e12287.

[96] Abedelaziz Mohaisen, Xinwen Zhang, Max Schuchard, Haiyong Xie, and Yongdae Kim. Protecting access privacy of cached contents in information centric networks. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, pages 173–178. ACM, 2013.

[97] W Mullins John. The new business road test, 2003.

[98] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *Journal of the ACM (JACM)*, 51(2):231–262, 2004.

[99] Muhammad Naveed, Seny Kamara, and Charles V Wright. Inference attacks on property-preserving encrypted databases. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 644–655, 2015.

[100] Edith CH Ngai, Jiangchuan Liu, and Michael R Lyu. On the intruder detection for sinkhole attack in wireless sensor networks. In *Communications, 2006. ICC'06. IEEE International Conference on*, volume 8, pages 3383–3389. IEEE, 2006.

[101] Antonio Nucci. Architecture, systems and methods to detect efficiently DoS and DDoS attacks for large scale internet, September 1 2009. US Patent 7,584,507.

[102] Hyundo Park, Indra Widjaja, and Heejo Lee. Detection of cache pollution attacks using randomness checks. In *2012 IEEE International Conference on Communications (ICC)*, pages 1096–1100. IEEE, 2012.

[103] Praveen Paruchuri, Jonathan P Pearce, Janusz Marecki, Milind Tambe, Fernando Ordonez, and Sarit Kraus. Efficient algorithms to solve bayesian stackelberg games for security applications. In *AAAI*, pages 1559–1562, 2008.

[104] Brett DM Peary, Rajib Shaw, and Yukiko Takeuchi. Utilization of social media in the east japan earthquake and tsunami and its effectiveness. *Journal of Natural Disaster Science*, 34(1):3–18, 2012.

[105] H. Qian, R. Ravindran, and G.Q. Wang. Method and apparatus for adaptive forwarding strategies in content-centric networking, June 24 2014. URL `https://www.google.com/patents/US8762570`. US Patent 8,762,570.

[106] Zeinab Rezaeifar, Jian Wang, and Heekuck Oh. A trust-based method for mitigating cache poisoning in name data networking. *Journal of Network and Computer Applications*, 104:117–132, 2018.

[107] Zeinab Rezaeifar, Jian Wang, Heekuck Oh, Junbeom Hur, and Suk-Bok Lee. A reliable adaptive forwarding approach in named data networking. *Future Generation Computer Systems*, 2019.

[108] R. S. Sandhu and P. Samarati. Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48, Sept 1994. ISSN 0163-6804. doi: 10.1109/35.312842.

[109] Reza Shokri. Privacy games: Optimal user-centric data obfuscation. *Proceedings on Privacy Enhancing Technologies*, 2015(2):299–315, 2015.

[110] Victor Shoup. Practical threshold signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 207–220. Springer, 2000.

[111] Betsy Sparrow, Jenny Liu, and Daniel M Wegner. Google effects on memory: Cognitive consequences of having information at our fingertips. *science*, 333(6043):776–778, 2011.

[112] Neil Spring, Ratul Mahajan, David Wetherall, and Thomas Anderson. Measuring ISP topologies with Rocketfuel. *IEEE/ACM Transactions on Networking (ToN)*, 12 (1):2–16, 2004.

[113] John D Sterman. *Business dynamics: systems thinking and modeling for a complex world*, volume 19. Irwin/McGraw-Hill Boston, 2000.

[114] Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana. Internet indirection infrastructure. In *ACM SIGCOMM Computer Communication Review*, volume 32, pages 73–86. ACM, 2002.

[115] Paul Syverson. A peel of onion. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 123–137. ACM, 2011.

[116] Paul Syverson, R Dingledine, and N Mathewson. Tor: The second generation onion router. In *Usenix Security*, 2004.

[117] Reza Tourani, Satyajayant Misra, Travis Mick, and Gaurav Panwar. Security, privacy, and access control in information-centric networking: A survey. *IEEE Communications Surveys & Tutorials*, 2017.

[118] Christos Tsilopoulos and George Xylomenos. Supporting diverse traffic types in information centric networks. In *Proceedings of the ACM SIGCOMM Workshop on Information-centric Networking*, ICN '11, pages 13–18, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0801-4. doi: 10.1145/2018584.2018588. URL `http://doi.acm.org/10.1145/2018584.2018588`.

[119] Matthias Wählisch, Thomas C Schmidt, and Markus Vahlenkamp. Backscatter from the data plane–threats to stability and security in information-centric network infrastructure. *Computer Networks*, 57(16):3192–3206, 2013.

[120] Michael Walfish, Hari Balakrishnan, and Scott Shenker. Untangling the web from dns. In *NSDI*, volume 4, pages 17–17, 2004.

[121] Kai Wang, Huachun Zhou, Yajuan Qin, Jia Chen, and Hongke Zhang. Decoupling malicious interests from pending interest table to mitigate interest flooding attacks. In *Globecom Workshops (GC Wkshps), 2013 IEEE*, pages 963–968. IEEE, 2013.

[122] Dan Wendlandt, Ioannis Avramopoulos, David G Andersen, and Jennifer Rexford. Don't secure routing protocols, secure data delivery. 2006.

[123] Wikipedia. Facebook wikipedia. `https://en.wikipedia.org/wiki/Facebook`, aug 2017.

[124] Robert E Wilson, Samuel D Gosling, and Lindsay T Graham. A review of facebook research in the social sciences. *Perspectives on psychological science*, 7(3):203–220, 2012.

[125] Walter Wong and Pekka Nikander. Secure naming in information-centric networks. In *Proceedings of the Re-Architecting the Internet Workshop*, page 12. ACM, 2010.

[126] Christopher A Wood. Protecting the long tail: Transparent packet security in content-centric networks. In *2017 IFIP Networking Conference (IFIP Networking) and Workshops*, pages 1–9. IEEE, 2017.

[127] Mengjun Xie, Indra Widjaja, and Haining Wang. Enhancing cache robustness for content-centric networking. In *INFOCOM, 2012 Proceedings IEEE*, pages 2426–2434. IEEE, 2012.

[128] Xiaoyong Yuan, Chuanhuang Li, and Xiaolin Li. DeepDefense: Identifying DDoS attack via deep learning. In *Smart Computing (SMARTCOMP), 2017 IEEE International Conference on*, pages 1–8. IEEE, 2017.

[129] Zheng Zhang, Ying Zhang, Y Charlie Hu, and Z Morley Mao. Practical defenses against BGP prefix hijacking. In *Proceedings of the 2007 ACM CoNEXT conference*, page 3. ACM, 2007.

[130] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin, and Nikita Somaiya. Connection-oriented dns to improve privacy and security. In *2015 IEEE symposium on security and privacy*, pages 171–186. IEEE, 2015.

Appendix A

Additional information

A.1 Equations for the aggregated system dynamics model simulation

Following are some of the equations used in basic run simulations (from the previous work [78]) on the extended SD model described earlier in presented in Chapter 5.3 Section 5.8 and illustrated in Fig. 5.4 and Fig. 5.5 of this thesis:

1. Adoption rate = Perception of Value for Money+Word of Mouth Units: cust/year

2. ARPU= “Consumer spending (on QoS etc)”+ Platform Enrichment Units: $/year

3. Barriers to New Entrants = INTEG (customer stickiness-change adaptability by user,0) Units: dmnl [0,10]

4. Billing Interface Ownership = Firm Innovation/Time Units: dmnl/year

5. capital per service feature = RAMP(max capital/(FINAL TIME-INITIAL TIME), INITIAL TIME, FINAL TIME) Units: $/service feature

6. change adaptability by user = (Perception of Intrusiveness-User Experience Control)* Total Customer base *Time Units: cust/year

7. Collaboration Failure rate = innovation obsoletion rate + integration faults Units: dmnl/month [0,10]

8. Collaborative Innovation = INTEG (collaborative innovation rate - Collaboration Failure rate,0) Units: service features [0,100]

9. Collaborative innovation rate = 100 * innovation rate Units: service features/year

10. Competitive Advantage = Collaborative Innovation Firm Innovation-competitors average innovation level Units: service features [0,100]

11. Competitors average innovation level = constant value of 50 inferred from market data on service features of mobile service features including package plans, etc. Units: service features

12. consumer profiling = 0.8 * customer stickiness (various fractions of customer stickiness were tried) Units: dmnl [0,10]

13. Consumer spending (on QoS etc) = Perception of Value for Money Units: $/month [0,10]

14. Cost of service provider = (Billing Interface Ownership * Total Customer base)/Time + Firm Innovation Rate + 0.5* collaborative innovation rate+(Total Customer base *Customer maintenance OPEX) Units: $/year

15. Customer maintenance OPEX = MAX[OPEX, BILLING INT OWNERSHIP+OPEX] is the operational cost of maintaining one customer per year Units: $/year

16. Customer stickiness = (Barriers to New Entrants+Perception of Value for Money)*Existing customers *Time Units: cust/month [0,10]

17. Effect of capital on innovation rate = Profitability Lookup (capital per service feature/reference capital per service feature) * 0.1 * Profitability of Service Provider Units: dmnl

18. Existing customers = 1e+06 Units: customers

19. FINAL TIME = 2059 Units: year

20. The final time for the simulation. Firm Innovation = INTEG (Firm Innovation Rate-firm innovation failure rate,1) Units: service features

21. Firm innovation failure rate = constant values tested ranging 0 to 10 Units: service features/year [0,10]

22. Firm Innovation Rate = ACTIVE INITIAL (RAMP(2,0,(3 * innovation rate + 0.3 * Collaborative Innovation)), 10) Units: service features/year [0,50,1]

23. INITIAL TIME= 2019 Units: year The initial time for the simulation.

24. Innovation obsoletion rate = RAMP (1,0,0.1) * Time Units: service features/year

25. Innovation rate = Normal innovation rate * effect of capital on innovation rate Units: service features/$/year

26. Integration faults = 1 to 30 Units: service features/year

27. Max capital = fraction of profitability Units: $/service feature

28. Normal innovation rate Units: service features/year

29. Perception of Intrusiveness = 0.5 * consumer profiling + 0.5 * User Experience Control Units: dmnl

30. Perception of Value for Money = Competitive Advantage * Platform Enrichment Units: $/service feature [0,100]

31. Platform Enrichment = Collaborative Innovation + Firm Innovation Units: service features [0,10]

32. Profitability Lookup([(0,0)-(30,100)],(0.794297,4.7619),(6.17108,19.5238),(12.4644,30),(16.2525 ,35.2381),(19.8574,47.1429),(24.1955,62.381),(27.2505,62.381),(29.6334,63.8095)) Units: dmnl

33. Profitability of Service Provider = INTEG (Revenue-Cost of service provider,0) Units: $ [0,10]

34. Reference capital per service feature = various constant values tested Units:$/service feature

34. Revenue= ARPU*Total Customer base Units: $/year

35. Total Customer base = INTEG (Adoption rate + customer stickiness * Total Customer base-change adaptability by user * Total Customer base, Existing customers) Units: customers

36. User Experience Control = INTEG (user experience control rate - User Experience Control Loss rate, 1) Units: dmnl

37. User Experience Control Loss rate = Perception of Intrusiveness - Perception of Value for Money Units: dmnl/month

38. User experience control rate = Billing Interface Ownership + consumer profiling + Platform Enrichment Units: dmnl/month

39. Word of Mouth = 0.5 * customer stickiness Units: cust/month