CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

Detection of Malicious Consumer Interest Packet While Mitigating Content Poisoning Attack

by

Adnan Mahmood Qureshi

A thesis submitted in partial fulfillment for the
degree of Master of Science

in the

Faculty of Computing
Department of Computer Science

2020

My dissertation work is devoted to my loving Parents, Wife and Kids, My Teachers and My Friends. I would like to pay special gratitude to my supervisor who guided me throughout my work.

CERTIFICATE OF APPROVAL

Detection of Malicious Consumer Interest Packet While Mitigating Content Poisoning Attack

by

Adnan Mahmood Qureshi

(MCS183012)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Ayyaz Hussain	QAU, Islamabad
(b)	Internal Examiner	Dr. Amir Qayyum	CUST, Islamabad
(c)	Supervisor	Dr. Nadeem Anjum	CUST, Islamabad

Dr. Nadeem Anjum
Thesis Supervisor
November, 2020

Dr. Nayyer Masood
Head
Dept. of Computer Science
November, 2020

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
November, 2020

Author's Declaration

I, **Adnan Mahmood Qureshi** hereby state that my MS thesis titled "**Detection of Malicious Consumer Interest Packet While Mitigating Content Poisoning Attack**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad. At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.

(Adnan Mahmood Qureshi)
Registration No: MCS183012

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**Detection of Malicious Consumer Interest Packet While Mitigating Content Poisoning Attack**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me. I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited. I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Adnan Mahmood Qureshi)
Registration No: MCS183012

Acknowledgements

First, all praise to Allah Almighty, the Omnipotent, the Omnipresent, the Most Kind and the Most Merciful, who blessed and helped me throughout my studies and granted me success in every field of life. Then distinct praise to Hazrat Muhammad (peace and blessings of Allah upon him), who is the torch of guidance for whole mankind till eternity. All my sincere appreciation and gratitude to the supervisor, Dr. Nadeem Anjum, for his guidance, inspiration and mentorship throughout the thesis period. I'm deeply beholden for his constant support and assistance. Without his supervision and mentorship this dissertation would not have been possible. There are no words to convey my sincere admiration to my affectionate parents, my wife, my daughter, my son and my friends for their motivation, encouragement and prayers throughout my academic career. Finally, I would like to express my gratitude to all my able and respected teachers of Computer Science Department of Capital University of Science and Technology, Islamabad for providing me with knowledge in a very professional environment.

(Adnan Mahmood Qureshi)
Registration No: MCS183012

List of Publications

Published and Submitted Papers

- Adnan Qureshi and Nadeem Anjum, *Detection of Malicious Consumer Interest Packet while Mitigating Content Poisoning Attack with Name-Key Based Forwarding and Multipath Forwarding Based Inband Probe*, The Fifth International Conference on UK-China Emerging Technologies (UCET), 2020, Glasgow, UK (Published in IEEE Xplore).

- Adnan Qureshi, Nadeem Anjum, Rao Naveed Bin Rais, Masood Ur-Rehman and Amir Qayyum, *Detection of malicious consumer Interest Packet with dynamic threshold values*, PeerJ Journal of Computer Science (Submitted).

Abstract

As a promising next-generation network architecture, named data networking (NDN) supports routing based on names and in-network caching to retrieve content in an efficient, fast, and reliable manner. It is a Data-Centric model of communication, so we require a data-centric model of security rather than securing the channels while transmitting the data to different hosts. Data-centric confidentiality and data-centric authentication are the two parts of data-centric security models. This architecture provides inherent protection against some of the legacy attacks of IP networks, yet some new attack surfaces have emerged in this architecture that needs to be addressed. There are many new vulnerabilities in NDN architecture, which an attacker can exploit to perform a content poisoning attack (CPA). The poisoned data pollutes the in-network caches and, consequently isolates the legitimate content in the network. There are many state-of-the-art mitigation strategies for the content poisoning attack, but some new attack-surfaces have emerged with these schemes' advent. The attack-surfaces need to be reduced to make these mitigation schemes more effective and robust. This dissertation's main contribution is providing an additional security feature in the content poisoning attack (CPA) mitigation scheme that will detect and prevent malicious consumers from flooding the network with unwanted reporting packet.

Contents

List of Figures

List of Tables

Abbreviations

CCN	Content-Centric Networking
CDN	Content Distribution Networking
CPA	Content Poisoning Attack
CS	Content Store
DDoS	Distributed Denial-of-Service
DoS	Denial of Service
FIB	Forward Information Base
ICN	Information-Centric Network
IKB	Interest Key Binding
IP	Internet Protocol
IPsec	Internet Protocol security
LRU	Least Recently Used
NDN	Named Data Networking
NSF	National Science Foundation
PIT	Pending Interest Table
PKI	Public Key Infrastructure
RVs	Reputation Values
SLRU	Segmented Least Recently Used
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security

Chapter 1

Introduction

Named Data Networking (NDN) is a well-known and well-researched architecture for the next generation of the Internet, based on a data-centric approach. While the legacy network is based on a host-centric system, the NDN architecture has changed the Internet's communication model altogether [1]. It allows the distribution of data that can be acquired from any content router from the network. A content provider can produce the data in advance and place it as auxiliary storage that can be accessed by any consumer anytime, even if the producer gets offline. A producer does not have to be online, and a consumer does not have to be connected to the producer to fetch the data; Instead, the Consumer can acquire data through in-networking caches. While NDN increases content availability in the network via in-network caching, the integrity of content becomes critical, given NDN's nature [2]. Hence, NDN opens several security-related issues that are not relevant to the legacy network communication. It includes some new types of data integrity attacks where a malicious or compromised node provides a corrupted copy of the content. These issues are often ignored in NDN-related communication and caching mechanisms, hence are our main focus in the thesis.

One of the most critical attack vectors in NDN is the Content Poisoning Attack. The attacker compromises the Content Router(CR), and this compromised CR sends a reply to the legit request with totally bogus or corrupted content. This poisoned content pollutes the in-network caches of intermediate NDN routers and

thus deprives the consumers of the requested legitimate copy of content. Hu et al. in [3] proposed a comprehensive scheme to mitigate Content Poisoning Attack (CPA). A special interest packet is generated by the Consumer, which contains the hash of the poisoned data. This thesis comprehensively addresses the aspects of identification and mitigation of security flaws that can be exploited by the attacker during this CPA mitigation process.

The research problem lies in the CPA mitigation scheme proposed by Hu et al. [3]. A consumer with malicious intent can flood the network with the Interest packet containing the hash digest of legit or un-poisoned data. This hash is stored in its exclude filter field. During CPA mitigation, this packet can flood the network, which will enable multipath forwarding and on-demand verification of hash at the router. This flooding attack can severely affect the throughput of the network or even cause a denial of service for other legitimate consumers. So it's essential to mitigate and add this additional security feature along with CPA mitigation.

In this thesis, we proposed a scheme to detect the flooding attack generated by the compromised Consumer. A satisfaction test is performed to check if the excluded interest packet is non-existent in the cache or a legit packet. If the cache miss ratio (of the excluded interest packet) reaches the threshold value, it is considered an attack. A lightweight parameter is added to the Content Store data structure, which stores cache miss counter value. This value is compared with the specified threshold value. When the cache miss counter reaches near that threshold value, an event is raised that blocks the incoming malicious face. Also, in our scheme, we made the threshold value adaptable. At first initial threshold value is calculated by taking the total buffer size and dividing it by the verification rate. The proposed idea is that when cache miss ratio avg crosses 50%, and queue capacity saturates, the threshold value is reduced to half. This process continues until the value is thrashed to one.

The main contribution of this thesis is proposing security feature filling up the attack surface that can be exploited by the malicious Consumer. Further, this thesis is organized into five sections; the second section emphasizes the literature

review. The third section is the proposed approach, and in the fourth section, experiments and results are highlighted along with the conclusion in the fifth section. Our contributions are:

- Making the threshold value dynamic, which was initially set by the network operator statically.
- Detection and mitigation of the flooding attack of special interest packets generated while mitigating the content poisoning attack.

1.1 Named Data Networking

It is a proposed architecture for next generation of the Internet which is based on a data-centric approaches whereas in legacy network system was based on a host-centric approaches. It has changed the communication model of the Internet altogether. There are three main entities in NDN i.e. Consumer, Producer, and NDN Router. Each of these entities communicate with each other using the named data. In NDN, these named data primitives are structured in a hierarchical manner [4]. An example is such that if we want to access the first segment of an HTML page for the www.cust.edu.pk website, the request would look like /pk/edu/cust/www/index.html/%00. In NDN, there are two types of packets, one is the Interest Packet and the other is Data Packet (Table 1.1). The consumer initiates the request and asks for data by sending an Interest packet. The structure of the Interest packet is that it contains the name or name prefix of the data that is requested. The NDN Routers consume the name of this interest packet and forwards it towards the origin of the data. When the namespace is compared with the name mentioned in the Interest packet, a data packet is returned to the consumer. This data packet will follow the reverse path by following the Pending Interest Table 1.1.

There are three main data structures in NDN Routers:

a. FIB (Forward Information Base): Its function is to map the name prefixes of the interest packet to one or more faces (physical network interfaces). It also

specifies the direction to be taken by the Interest Packet.

b. PIT (Pending Interest Table): It contains the Interest packets that are not satisfied and has been forwarded to the upstream of the network towards the origin of the data source. PIT entry contains the information of the incoming faces i.e. physical network interfaces from where the interest packet has arrived along with the interest packet. It also indicates the downstream consumers as well. Also, it helps the router to perform the reverse path data forwarding.

c. CS (Content Store): CS is a temporary cache that holds data packets while it passes through these routers. It is a key component that helps to retrieve the most recently used data to the consumer promptly.

NDN communication model i.e. the data-centric model allows distribution of

NDN Interest Packet
Name: /pk/edu/cust/thesis
Selector:
Nonce:
Guider:

NDN Data Packet
Name: /pk/edu/cust/thesis/v_2/s_9
MetaInfo:
Content: a4:33:5b
SignatureInfo: **KeyLocator:** /pk/edu/cust/KEY/1 .....
Signature Value: 22:4e:7f.....

TABLE 1.1: NDN Packet Formats

data in such a manner that it can be acquired from any available entity, it may be the content provider or may be from the content store (in-network storage). The authors in [5] and [6] proposed different mechanisms for in-path network storage, with this model it is also not necessary that producer or consumer both have to be online or establish a connection between them before transmitting the data. A content provider can produce the data in advance and place it somewhere else as auxiliary storage which can be accessed by any consumer anytime even if the producer gets offline. Y. An et al. in [7] proposed different approaches to retrieve data swiftly and in an energy-efficient way. A producer does not have to be online and a consumer does not have to connect with the producer for fetching the data, instead it can acquire data through in-networking caches as well. So the data-centric

model induces data-centric security issues. Integrity and availability of Data is the main concern in the NDN Model, which requires mitigation mechanisms.At the network layer of NDN, data-centric security is mandated via a digital signature on each data packet. A digital signature is added by the content provider (producer) to every data packet associating the data to the packet name when data is being generated. Authentication can be performed by the consumer on the data packet by verifying the signature using the Content Providers' public key. One area of research that requires attention is the efficient detection and mitigation mechanism of the Content Poisoning Attack. This attack isolates legit contents from the network and propagates the fake or malicious content to the consumer. In interest packet, in which the content name is matched with this malicious content is returned either from the cache of the intermediate router or directly from the producer. Along the way back this malicious content is copied on each intermediate router's cache thus it contaminates the whole network. There is a built-in security mechanism in NDN/CCN/ICN i.e. signature verification though it is avoided at routers because it has large computational overhead, [5]. To make CPA mitigation more effective and robust, the attack surface needs reduction. This thesis's main contribution is to identify a possible attack scenario in the CPA mitigation mechanism and propose a remedy for this threat. A new security feature is proposed that will prevent malicious consumers from flooding the network with unwanted reporting packet during the CPA. To make CPA mitigation more effective and robust, the attack surface needs reduction. This thesis's main contribution is to identify a possible attack scenario.

1.2 Problem Statement

The problem-focused is to detect malicious consumers during content poisoning attack mitigation. An enhancement in security mechanism is required to handle this issue. This security feature should detect malicious interest packet which is re-issued by the consumer after verification of the content, during the CPA

mitigation strategy. This malicious interest packet with an excluded filter field can add processing overhead at the edge router in the consumers' domain.

1.3 Research Questions

This thesis has formulated the following research questions:
RQ1: What will be the mechanism to detect the attack initiated by the consumers with malicious intent? **RQ2:** What will be the parameters which will contribute to mitigating the malicious consumers' reissued interest packet flooding attack?

1.4 Purpose

The purpose of this study is to propose a mechanism to detect and mitigate the flooding attack of the reissued Interest packet generated by a consumer during CPA mitigation.

1.5 Scope

The scope of this thesis is to prevent a compromised consumer from flooding the next NDN router by reissued Interest Packets during CPA.

1.6 Proposed Approach

A consumer with malicious intent can flood the network with the Interest packet containing the hash digest of legit or un-poisoned data. This hash is stored in its exclude field. During CPA mitigation, this packet can flood the network. Consequently, it would enable multipath forwarding and inline verification of hash at the router. It can adversely affect the throughput of the network or even can cause

DDoS. So, it's important to mitigate and add this additional security feature along with CPA mitigation.

Possible Attack Scenarios (Research Problem): During the CPA, the reissued Interest Packet by the consumer stores the poisoned data hash in the excluded filter field. The compromised consumer can flood the next router with the reissued Interest packets containing legit data hash. This will result in a cache miss. The Inline verification at the router will also be enabled which can consume a lot of processing power of the router. This way the process of CPA mitigation will be severely affected. It should be considered as an attack.

The NDN-routers' service manager maintains the stats of cache misses of reissued Interest packets. It'll continuously monitor these values. Once the cache misses exceeds the threshold value, the router will drop the future reissued interests coming from this face as it is considered as a malicious consumer. This will be done temporarily and delisted will be done at the discretion of the network operator.

Excluded Interest Packet Satisfaction Test: To prevent the Malicious Consumer to send a fake excluded Interest packet, a satisfaction test is performed to check if the excluded interest packet is a non-existent data in cache or a legit packet in the cache, in case of a cache miss (of the excluded interest packet) ratio reaches near the threshold value i.e. is set by the operator, it is considered as an attack.

Chapter 2

Literature Review

2.1 NDN's Data-Centric Security

At the network layer of NDN, data-centric security is mandated via a digital signature on each data packet. A digital signature is added by the content provider (producer) to every data packet associating the data to the packet name when data is being generated. Authentication can be performed by the consumer on the data packet by verifying the signature using the Content Providers' public key. This authentication can be performed even if the data is retrieved from some other entity other than the content provider, [9].

Zhang et al. [10] stated that If a content providers' public key is not distributed or the consumer has no information about this public key, in that case, the data producer places the signing key name into the specific field of the data packet. It is known as the KeyLocator field (Figure 2.1). A consumer can acquire a public key by following this field of KeyLocator and can retrieve it just like a normal data packet. A public certificate is the public key information in the data packet. A consumer can acquire multiple keys in a hierarchical chain until it reaches a pre-trusted key from the trust anchor. Then iteratively a consumer can start from the trust anchor to each retrieved key signature verification until it reaches the target data. This process i.e. keys lists acquired between the trust anchor and

target data is knows as the trust chain. This process is shown below in figure 2.1. A list of rules is required to the consumer so that it can derive trust correctly from the trust chain. So we can say that these rules for derivation and trust anchors make a trust model. It is also known as a security context. This security context is specific to a particular application. For example, the security context of cust thesis in the above example cannot be the same as with that of another e.g. media producing application. So in NDN, a producer and consumer must have the same security context to correctly authenticate the data. However, there is no concrete mechanism in which a trust model and authentication of data can be specified directly in the NDN application.

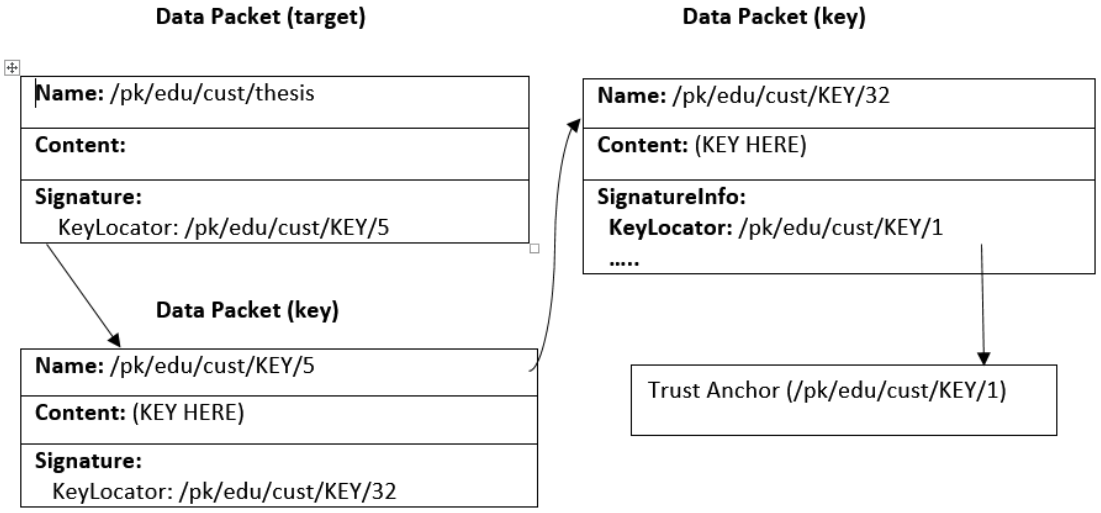

FIGURE 2.1: Trust Chain Mechanism

2.1.1 Internet Security

Point to Point communication is the main design goal of this architecture so consequently, the security goal of this architecture is to protect the point-to-point communication channel. Several security implementations have been developed to achieve this goal such as IPSec, TLS, SSL and SSH, etc. All of the above-mentioned architectures achieve security in two steps. First, they authenticate each endpoint involved in communication and secondly an encrypted channel is

established between these two endpoints. These two endpoints communicate with each other securely when this channel is established. There are further two ways to authenticate the endpoints, either through the pre-shared private keys or through public/private keys (public-key cryptography). One end has to prove its authenticity to the other endpoint through a particular pre-shared secret key or via some private key which corresponds to a particular public key. In public-key cryptography, for authentication, we use public keys which are usually linked to a particular subject such as IP Address, domain name, etc. This bond between the public key and subject is the basis of authentication of endpoints which must be secured. However, in PKI (Public Key Infrastructure) the public key and subject linkage can be stored in the hosts but it can be done on small scale and not recommended for the enormous number of hosts on the internet. PKI System users normally start with one or more keys which are pre-trusted and endpoints develop trust gradually through each key and subject association. In today's internet, currently, there are three types of PKI running i.e. the Certificate Authority (CA), Web-of-Trust and DNSSEC. The difference between these types is that of trust management. Certification Authority system consists of two roles, one is the certificate providers and the other is the certificate owners. The key and subject association is developed by the certificate providers and the rest of the users trust this CA. Web-of-Trust uses real-world entities based trust management, in which a user develops trust based on the identities of the provider of association. The capability-based trust management is provided by the DNSSEC in which the key and subject association is checked by the DNS Validator whether it is managed by someone who belongs to that particular DNS Domain. Two endpoints after authentication communicate with each other using a secure channel. These two hosts first share a temporary session key. The sender uses this session key to encrypt the data whereas the receiver can only decrypt this ciphertext which is sent by the sender. No other entity can see this data in plain text but the only ciphertext is visible. This session key belongs to the communication channel and is established temporarily and when the same data is sent over a different channel then the new session key is exchanged and encryption is done once again using this new session key.

2.1.2 Security Issues In NDN

Kumar et al. [11] explained some of the most common attacks within the existing TCP/IP model such as Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack, eavesdropping (snooping), masquerading, TCP Replay Attack, Man in the Middle Attack, repudiation, and traffic analysis attack. An intruder attempts at Snooping to access and use sensitive user data for their benefit. Snooping involves several threats, such as eavesdropping and capturing the keystrokes using the key loggers. The absence of the host's identity does not make snooping in NDN possible. An attacker tricks the user to anticipate trends of Internet use when performing a traffic analysis attack. For other attacks, the attacker could use this information collected from this attack. NDN being data-centric rather than host-centric, it does not have any Host-ID such as IP address, this attack in NDN is extremely difficult to perform. In a modification attack, the attacker compromises the confidentiality and integrity of a consumer. However, this attack is not possible in NDN, because a consumer can detect and verify the content by comparing its signature. If router gets compromised, then it is possible that a corrupted data packet may be sent to the consumer. Consumers after receiving the publishers' public key can validate this corrupted data. In a replay attack, the attacker performs Man in the Middle attack and tries to get a copy of the message from the sender, then after modifying the message and he/she sends it to the receiver. The recipient assumes that the actual sender has forwarded the message but in fact, it is the modified message from the attacker with malicious intent. This type of attack is also not possible in NDN because the interest packet is identified by the name and for the uniqueness of the namespace in the network, a nonce is used. When the same interest packet reaches the router (with the same name and nonce), the router assumes the packet is duplicate and it is replayed; it will, therefore, be purged from the PIT table. NDN, therefore, protects itself at the network layer level from the replay attack. In the case of repudiation, the sender or recipient of the message may be an attacker. The sender may say that the message has not been sent and the recipient may likewise state that it has

not received the correspondence. In NDN, this attack is also unlikely to happen because the user and publishers have a paradigm of trust. In DoS attacks, an attacker can compromise the availability goal by flooding the network with a large number of messages, consequently will consume the bandwidth. This attack prevents legitimate users from accessing or utilizing a network resource such as bandwidth. In NDN, this attack is not easy to perform because DoS requires a host with an IP address, but in NDN it does not have an IP address or any other host identity. However, an attacker can flood the NDN network with a bogus interest packet with non-existing data. These interest packets will start to fill up the PIT, which may prevent legitimate users from sending the request to the content provider, and consequently, the legitimate interest packets will drop. In NDN architecture, some inherent security features protect us from some of the legacy security attacks by default but still there are some emerging security concerns in this new architecture that needs to be addressed. Security, privacy, and access control are the three major domains that need to be covered in NDN architecture. Several attacks are possible in NDN such as Content Poisoning attack, Content pollution attack, Naming Attack, and Denial of Service attack. In privacy, it can be classified into five categories such as content privacy, signature privacy, client privacy, name privacy, and cache privacy, [10, 12–14]. In access control, there is some mechanism that needs to be addressed are content encryption, content attributes, clients' identity, and authorized sessions as shown in figure 2.2.

2.1.3 Attack Types In NDN

In NDN there are four main types of security threats that are briefly discussed in the coming sections, [11, 15].

2.1.3.1 Flooding Attack Of Interest Packet

In an interest flood attack, an attacker can deplete the network resources by flooding the network with a large number of interest packets batches. PIT, network

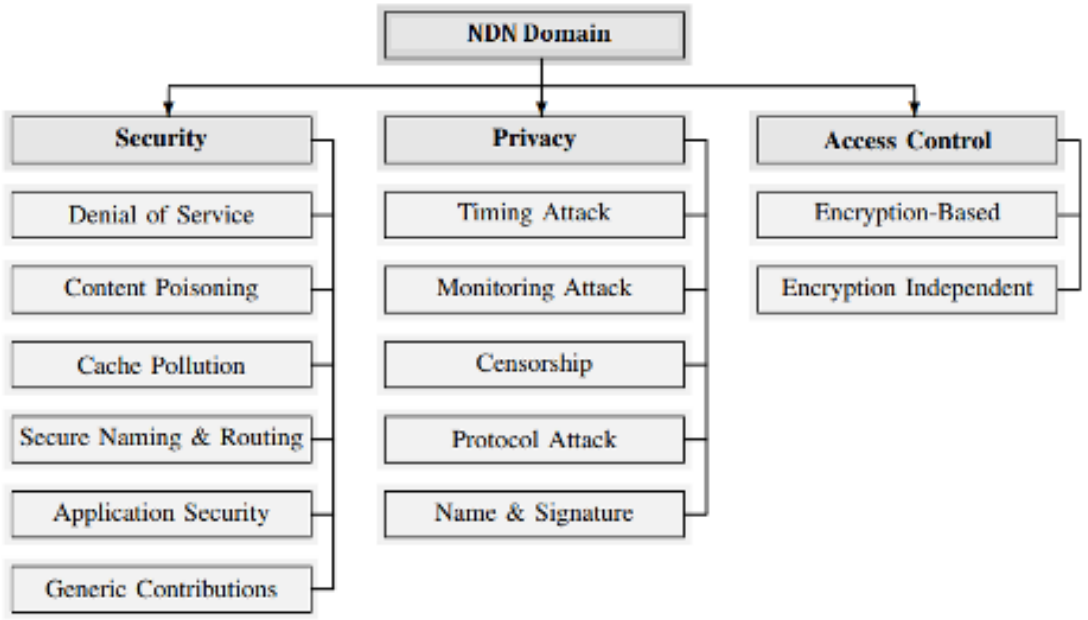

FIGURE 2.2: Attack Types In NDN

bandwidth, and producer resources availability to the legit users will be compromised with this attack. This attack consumes NDN resources that restrict legitimate users from accessing them.

2.1.3.2 Cache Pollution Attack

Wang et al. [16] discussed the anatomy of this attack. In this attack, the attacker attempts to fill the cache by demanding the data packets which are unpopular and not in demand. As a result, the NDN routers' impact ratio decreases. Therefore, the cache hit ratio of the interest packet of the legitimate user will thrash. This will increase the latency and reduce the throughput of the network.

2.1.3.3 Cache Privacy Attack

In this attack, the adversary compromises the users privacy. A newly accessed item lies in the routers' cache and the requester gets a quick response of these types of data. The intruder compiles a list of content that is vulnerable to privacy and inquires it by using brute force approach to check if it is recently cached or

not. This way an adversary can judge the user's data access patterns and hence his privacy gets compromised.

2.1.3.4 Content Poisoning Attack

In CPA, the attacker compromises the router and this malicious router sends a reply to the legit request with totally bogus or corrupted content. These contents of intermediate routers that are involved in NDN communication are stored in CS. This poisoned content spreads when other legitimate consumers request the same content. Literature is having information regarding the mitigation strategy of CPA. Contents in NDN are of three types, i.e. legit contents, fake or poisonous contents, and corrupted contents. A valid signature of valid content is generated through the private key of a legit publisher. Similarly, a valid signature of fake content can also be generated with any private key that is not associated with the namespace of the publisher. Whereas the corrupted content are those which do not have a valid signature.

In a Content Poisoning Attack, an attacker takes over a router and replies to incoming interests with fake content. Wu et al [17] explained that if this fake or corrupted content is requested by a consumer, it will result in the spreading of this malicious content on intermediate routers' content stores. This will result in the spreading of this poisonous content all over the network. This verification is usually performed by the consumers which use the content verification process using the signature of the content. In NDN every router can verify the arriving contents on its own but this verification at line speed takes resources and it is impractical.

Gasti et al. [8] described two ways through which a content poisoning attack can be carried out. The first way is that the attacker compromises the routers, which spreads the poisoned content while satisfying the requested interest packets. In figure 2.3, the attacker has compromised an intermediate router and placed an invalid content C1 (oval) and it'll deliver the invalid content to the client if it receives the interest packet from the client with the valid namespace of the content. So instead of getting a valid content C1 (rectangle) from the content provider, the

consumers' interest will be satisfied by invalid content by the compromised router. This scenario can have adverse effects on the network, as other routers can also get poisoned from this content being the intermediate router for the other consumers. The second way is that poisoned content is distributed via compromised publishers.

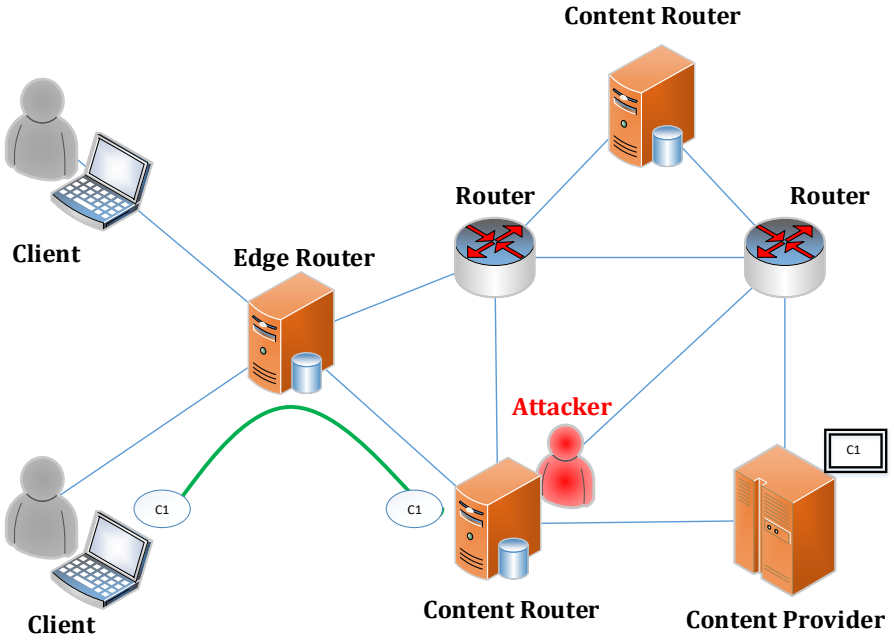

FIGURE 2.3: Content Poisoning Attack Scenario

Compromised publishers can anticipate the data which will be in high demand e.g. highlight of a popular football match, and create malicious content. So in this way, a compromised producer or router can reply with a malicious data packet against a legitimate interest packet.

2.2 CPA Detection And Mitigation Approaches

Content Poisoning Attack can be detected and mitigated through two major approaches as shown in figure 2.4 below i.e. Collaborative Signature Verification and Consumer Dependent approach. The former approach is those in which NDN

routers collaborate to verify the signature of the content and the latter approach uses extra fields in the Interest and Data packets or uses clients' feedback.

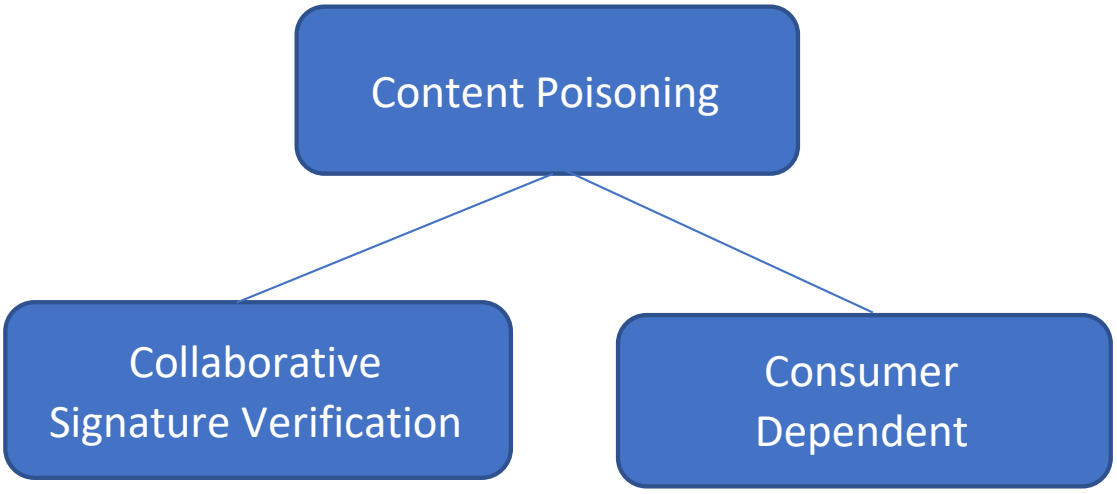

FIGURE 2.4: Content Poisoning Attack Mitigation Approaches

2.2.1 Mitigation Of CPA Using Collaborative Signature Verification Approach

This approach proposes that the signature of packets should be verified by the routers. This increases a load of signature verification on the routers so to reduce and to balance the load router marks the verified chunk and this will serve as an indicator for the peer routers that this packet has already been validated and verified. This approach is further classified as follows:

2.2.1.1 Self-Certifying Interest/Data Packet (SCID)

Gasti et al. [8] proposed an approach in which a client has to acquire the data chunk's hash, name, and signature from the producer of the content before sending the interest packet. This information is available in the interest packet. When a router receives this chunk of data, it checks its validity by comparing its' hash with the hash that is present in the interest packet. The advantage of this approach is that it less computationally intensive than the RSA signature verification but the downside of this approach is that it has to acquire the hashes for each data chunk

beforehand. Also, this information has to be stored in the router cache until it is verified. This way latency to retrieve the content and storage capacity at the router increases, this approach limits the scalability of the system. There are two types of SCID that the author has discussed. i.e.

1. **S-SCID (Static Content)** In this approach, the cryptographic hash computed over its data, name, and signature is automatically appended to the name of every data packet when it is created. A consumer can use this last hash component in the Interest packet by requesting a data packet by name. The downside of this approach is that the consumer has to know the hash beforehand. However, the advantage is that the NDN router can verify the content by comparing the hash values of both the interest packet and the received content. The received data chunk also has the value of the next data chunk, [8].

   Limitations of S-SCID: The hash content that a consumer has to request cannot be guessed or anticipated. Also, each data chunk is linked with the next data chunk so this approach also imposes restrictions on inter-packet dependencies. This technique cannot handle dynamic content as well. So a consumer cannot acquire the hash of a data chunk as data may not exist at that moment is the dynamic nature of the chunk.

2. **D-SCID (Dynamic Content)** In this type, PPKD (Publisher Public Key Digest) is included in the NDN interest packet. PPKD is the SHA-256 hash which is the hash of the content provider's public key whose data is requested. Every NDN router either at edge or intermediate will ensure that this data packet matches the same public key is present in the PPKD field of interest packet. The advantage of this technique is that it prevents the attacker to induce the bogus content against the requested interest packet. However corrupted content can still be induced in the data packet as an attacker can still refer to the valid producer's public key. This is possible because by default NDN routers do not verify the content signature as it is

the responsibility of the consumer to do the verification of the content when it is received, [8].

2.2.1.2 Probabilistic Techniques

1. Probabilistic Independent Verification

   In [8] author has proposed this technique in which the router randomly verifies a subset of content stored in its cache. The packets which are corrupted are purged from the cache immediately and those with the valid signature are flagged and after that, they have not verified again. The probability with which a data packet is checked by one router is

$$P = 1 - \prod_{i=1}^{n}(1 - \frac{1}{v_i}) \tag{2.1}$$

   $\frac{1}{v_i}$is the fraction of packets which are verified at any given time in the routers' cache.

2. Probabilistic Disjoint Verification This scheme is more effective as the verification load is evenly distributed among the routers that are in the same autonomous system (AS) [18]. To secure this scheme a secret key is used for AS by using a keyed hash function.

$$P = 1 - \prod_{i=1}^{n}(1 - \frac{n}{v_i}) \tag{2.2}$$

   $\frac{1}{v_i}$ ($V_i < n$ for all I belongs to [1, n]) is the fraction of packets which are verified at any given time in the router's cache.

2.2.1.3 Collaborative Techniques

Neighbor Verification Feedback

To increase the individual router's signature verification throughput, this cooperative approach is used in which each router exchanges information of the valid

content. So in this way cryptographic operations can be reduced as routers are verifying a large number of packets and share this information with other nodes in the network.

If a router encounters a corrupted packet, it issues a special interest packet and sends it as a warning to all of its interfaces. This interest packet Hop field is set to 2 that it'll not propagate past one hop. When this special interest packet is received by the next-hop router, it checks the reference packet in its cache, if not present it is discarded. Otherwise, this content is verified, and if the verification fails this next-hop router creates its special interest packet and warns its next hope. In this way, this warning is propagated throughout the network.

2.2.1.4 Check Before Storing Approach

Kim et al. [19] used a technique known as CBS (Check before Storing), in this technique contents are checked probabilistically before they are stored in the content store of the router. At the network layer of NDN, data-centric security is mandated via a digital signature on each data packet. A digital signature is added by the content provider (producer) to every data packet associating the data to the packet name when data is being generated. Authentication can be performed by the consumer on the data packet by verifying the signature using the Content Providers' public key. Authors have measured that before the expiration of the content in the cache, only 10% of cached contents are requested again. So they proposed that cache is divided into serving content and by-passing content [20]. The serving content is requested while they are in the cache and by-passing contents are dropped from the cache before the specific interest. So the author proposed that for cache replacement, segmented LRU policy is used in which it verifies only the signature of the serving contents. When the content is verified it is moved to the cache segment of the serving content. Also, the verified chunk is marked in the serving content segment of the cache to avoid multiple verifications. This scheme also has some shortcomings i.e. verification will be required for any content that is requested twice, which can add latency and increase the processing overhead at the routers. An adversary can request fake content and can enforce

verification by requesting it multiple times which may lead to DoS/DDoS attack. Kim et al.[21] extended the work in [19] by developing some mathematical models which is further extended in [21] and identified a new type of attack i.e. verification attack which is mentioned in [22]. In this attack, CS is filled with a large number of bogus content. Then the same content is requested by the attacker using the compromised consumers. To mitigate this attack, the author proposed two phased approach that is detection phase and the identification phase. In the first phase, a parameter for detection is used which is calculated by taking the ratio of the content hit to the number of verifications performed on the content. Then the second phase is initiated in which a monitoring mechanism is adopted by the router in which it detects the malicious interfaces through which different verified contents were forwarded.

2.2.1.5 Identity Based Signature Scheme

Ullah et al. [23] proposed a scheme for IoT-based NDN networks, in which content security and integrity are ensured through an identity-based signature scheme. In this approach, a lightweight sized key is used while ensuring the same level security as that of bilinear pairing, ECC (Elliptic Curve Cryptosystems), and RSA (Rivest-Shamir-Alderman). This scheme is derived from the concept of Hyper-elliptic curves. This scheme is analyzed by comparing its performance in terms of cryptographic operations of other CPA schemes and is efficient because of its small key size. The author in this scheme proposed that this scheme is subjected to security analysis for its feasibility.

2.2.1.6 Register Before Publishing With Smart Forwarding

Yue et al. [24] proposed another scheme for mitigating CPA in IoT-based NDN Networks. The proposed approach used in this thesis for mitigating the CPA attack is focused on name-key based binding rule and smart forwarding method. This scheme is effective for CPA mitigation but it is prone to DDoS through

Interest flooding attack. The simulation result showed that this scheme is effective if less than 25 % of the NDN network is under the CPA attack.

2.2.2 Mitigation Of CPA Using Consumer Dependent Approach

2.2.2.1 Consumer Feedback

As per NDN specification, a consumer verifies all the signatures of the requested data packets. So a feedback-based approach is used to verify the content at the router [8]. This approach is the extended version of the NVF technique as discussed in the previous section. However, this approach has some new challenges such as there is no trust relationship between the router and the consumers. Consumers can also be compromised and in this way, false feedback can consume network resources.

2.2.2.2 Content Ranking Algorithm

Ghali et al. [25] proposed a technique in which the ranking of content is calculated and stored in the exclude field of the interest packet and the range of the values are between 0 and 1. When new content arrives in it is ranked 1, which gets downgraded if the content is ranked by the consumer and included in the excluded field of the consumer. This approach is somewhat similar to the technique mentioned above in [8] so it has the same limitations.

2.2.2.3 Interest Key Binding Rule

Ghali et al.[26] highlighted some of the NDN architecture vulnerabilities such as the PPKD field and name's digest are not the essential components of the Interest packet. Also, there is no such trust model that is adopted unanimously by the consumer's applications to fetch the content's hash securely. Based on these

vulnerabilities, a technique is proposed, which enables an IKB rule to ensure trust. According to this rule, the Interest packet must include the producer's (content publisher's) public key. For producers, it is also implied that KeyLocator field in data packet should retain the public key. Its implication on the router is that public key hash of the content received should be caclulated and compared with the PITs' PPKD field. The content gets purged if verification fails. Upon successful verification, content gets stored in the content store of that particular router. IKB implication for consumers is that it has to acquire and validate the public key of the content provider before initiating the Interest packet for that particular data packet. So to acquire a trust model, three approaches were proposed, one is that public keys of the content provider should be installed in the client application, the second one is the universal key name service and the third one is global search based service. Also to reduce the workload of the core routers, the author has proposed that an Interest Key Binding check on the data packet should be performed at the edge routers whereas core routers should perform this check probabilistically. The cons of this approach are that it is assumed that the verifying router is trusted, but in case if it is malicious it can verify the bogus IKB to be correct. So this scheme lacks scalability and has overhead.

2.2.2.4 Forwarding Strategies

DiBenedetto et al. [27] proposed an approach in which consumers upon verification failure send a report packet which will act as feedback to the other entities of the NDN Network. When consumers detect a poisoned content, a special interest packet is generated by the network stack and the information regarding the poisoned content is stored in this special report packet. When the router receives this special interest packet, it acts as one of the two proposed mitigation options that the author proposed. One is Immediate Failover and the second one is Probe First. In the first approach, the malicious face is marked with a low priority value for the future. And in the probe first technique, the node upon receiving the special interest packet known as report packet stops forwarding the interest packets of the namespaces on which the attack is underway. Also, that particular

node informs their next-hop routers about this malicious namespace. Nguyen et al.[28] explained three vulnerabilities in NDN architecture, first one is unregistered remote provider, then multicast forwarding, and the last one is the best route forwarding. The reason for the first vulnerability is that the interest packet can be satisfied with any data packet that is received from any of the faces. Therefore, a malicious producer can induce malicious content and get it satisfied before it gets satisfied by the legit producer. In NDN faces are registered in the corresponding values in the FIB table so while doing multicast forwarding the interest packet is forwarded to all these faces. So, it is quite possible that malicious producers can satisfy the interest packet with its malicious content. A router ignores a similar interest packet in the best route forwarding that has the same name and selectors but different nonce when it is received during the suppression interval of retransmission. The interest received after this interval shall be transferred via the next lowest possible cost; thus an interest packet can be satisfied with poisoned contents by a malicious producer.

2.2.2.5 Name Key-Based Forwarding And Multipath Forwarding Based Inband Probe

Hu et al. [3] proposed a comprehensive system to mitigate CPA and this thesis is all about the identification of security flaws and propose a mitigation strategy to address this flaw in this system. In the following sections, this base system is elaborated in detail. This system is comprised of three phases. First is the route building phase, then there is a normal content retrieval phase and the last one is the recovery phase in chase content poisoning has occurred. It is required that NDN routers should enable name-key based forwarding to forward interest towards registered content sources and to specify legitimate content sources every route advertisement should be authenticated with a trust management system. In case, content poisoning occurs on intermediate routers then a mechanism of Multipath Forwarding based Inband Probe is performed. In this approach, an interest packet with an exclude filter (poisoned content) is reissued and forwarded via alternate paths. When this packet reaches a particular router, it enables cached contents'

on-demand signature verifications. Verification of cached content is performed between the malicious payload that is included in the interest packets' exclude filter or in the Data Packet that is returned and gets matched with the reissued interest packet. There are two benefits of this approach, first, with multipath forwarding there is a great chance that consumer will acquire the legitimate content and other is legitimate content can be restored on the intermediate router via alternative forwarding options. This way poisoned contents will be purged and for future requests, legitimate contents will be returned from the routers' cache, thus it'll increase the overall throughput of the network. Three phases are described below in figure 2.5.

a. Route Building Phase: In this phase, each producer of the content is mandated to register a PPKD of the content that it is generating and making it available for the consumers. When a consumer asks for this content and content prefix is announced, then the producer should dispense a certificate for its authorization under that particular name prefix. It is assumed that for managing the namespaces a manager for assigning the namespaces is present in the system. This assignment manager is present and preinstalled on every NDN router and other nodes. The authorized keys for the namespaces can easily be accessed by any node before requesting the content. It is the responsibility of the routing announcer of the access router to check it is authorized to provide the content against the announced prefix. After successful authorization, the router enters the prefix and it's PPKD into FIB and forwards it to the next-hop routers. If authorization is failed, this announcement is expunged from the system. So, in this way a mutual trust is established between routers. This guard against the prefix hijacking attack. Also, it'll save consumer node energy by avoiding the signature verification of the poisoned content. In algorithm 2.6, arguments of Name-Key Based pairs, nonce, list of incoming interfaces are passed. If the content is found in the CS then the corresponding data packet is returned. If no data is found then an entry of Interest packet is done in the PIT table if it is a unique request. If no PIT entry is found then the interest packet will be forwarded according to the FIB entries.

b. Normal Content Retrieval Phase: A consumer when issues a request,

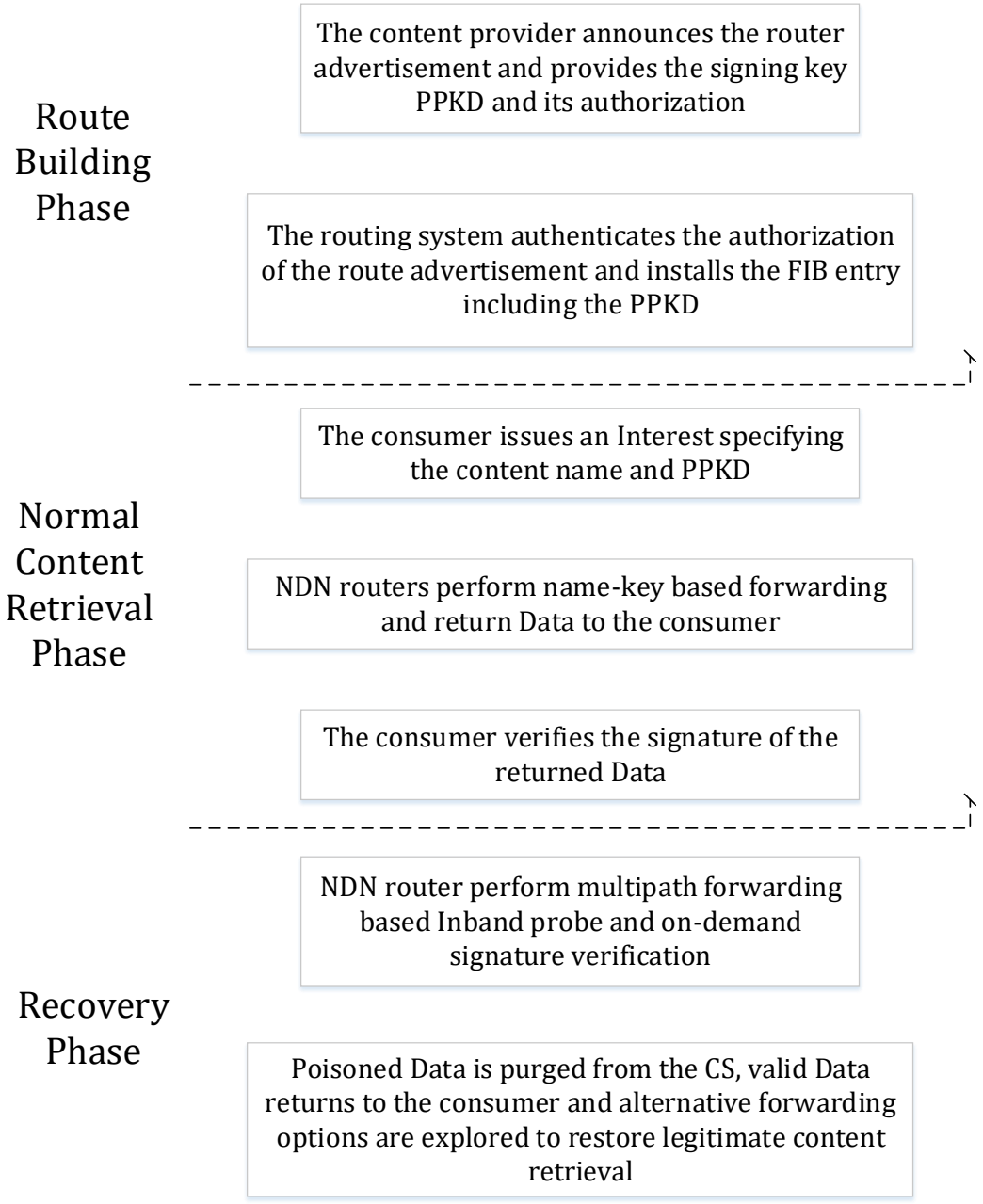

FIGURE 2.5: Three Phases Of CPA Mitigation

specifies the content provider attribute in the interest packet. Now the consumer has to validate the PPKD of the content provider before issuing the interest. This certificate from the content provider can be acquired by the consumer in two ways, first is that either the assignment authority respond with one or more certificate corresponding to the name prefixes in the interest packet. The other way is that consumer is provided with a searching service which should search

globally via some search engine. Consumers would provide an interest packet as a search query to the search engine and in reply, most relevant certificates will be returned. But before using the search engine it is assumed consumer somehow has acquired search engine root public keys securely. So after PPKD verification, when the interest packet reaches the NDN router, it forwards the interest packet using name-key pair. It compares not only the namespace of the content as done in traditional NDN architecture but in this technique, PPKD is added to the NDN stack and added to the FIB along with the namespace, so PPKD of interest is also compared in FIB entry. Also, the Content Store and PIT should store the PPKD value relevant to the content. So when the content provider receives the interest packet from the consumer, a PPKD entry is stored in the KeyLocator field of the Data packet. It is ensured that the content provider has included the PPKD in the KeyLocator field. Signature verification of each data packet is not performed by the intermediate routers to avoid verification overhead [29]. Only the PPKD of the Data packet and PPKD of the corresponding interest packet is matched. NDN Router's forwarding algorithm is shown 2.7. In this algorithm, functionality of multipath forwarding of special interest packet is implemented. First if poisoned data is found in the CS then it purges that content and raises the cost of that particular next hop.

c. Recovery Phase: On-path content poisoning cannot be removed from name-key based forwarding. On-path routers can be compromised and can serve the interest packet with poisoned content. PPKD specified in the interest packet and that of the data packet are compared by intermediate routers during the on-path content poisoning attack but this will only handle the fake data packets. It'll not solve the problem of corrupted data which still can be returned to the consumer with valid PPKD.

To mitigate this problem, on-demand signature verification is enabled on routers to purge the corrupted content and multipath forwarding based in-band probe mechanism would explore alternate paths and restore legitimate content in intermediate router caches.

Poisoned content can be detected by the consumer. After detection, the consumer

Algorithm 1 Interest Forwarding using Name-Key Pair

```
Require: INTERREST_PACKET (Content_Name; PPKD; nonce; Incoming_Interface)
ContentStoreEntry ← FindInContentStore (Content_Name; PPKD)
if ContentStoreEntry is > 0 then
        Return ContentInCS
else
        PitEntry ← FindInPIT (Content_Name; PPKD)
        if PitEntry is > 0 and nonce.IsUnique = TRUE then
                ifaces.Add (Incoming_Interfaces)
        else
                FibEntry FindInFIB (Content_Name; PPKD)
                if FibEntry is > 0 then
                        MinCostHop = FindMinCostHops (NEXTHOPS)
                        ForwardInterest (Interest, MinCost)
                else
                    Cache.Purge (Interest)
                end if
        end if
end if
```

FIGURE 2.6: Interest Forwarding Using Name-Key Pair

issues the interest packet again and calculate the hash of the malicious content. Then it includes this has in the exclusion filter field of the reissued interest packet. When an intermediate router receives this interest packet, it forwards it to multiple paths and enables inline signature verification on the intermediate routers, if excluded data is found in the cache. Here routers have to do only one verification as PPKD is specified in each data packet and if it is found malicious then this cached data is purged from the routers CS.

The cached copies of malicious content are immediately purged as the consumer reissues the excluded filter interest packet soon after it is verified to be poisoned. So this way, network nodes will be protected against further escalation of malicious content. This process is elaborated in Algorithm 2.7.

When PIT entry is consumed upon arrival of the data packet, intermediate routers should verify that if this data packet is not associated with the interest packet that has an exclusion filter field. Data packets that have just returned from poisoned faces and are satisfied against excluded filters interest packet, they are also verified from intermediate routers. This mechanism is elaborated in Algorithm 2.8.

So summary is that a consumer with malicious intent can flood the network with the Interest packet containing the hash digest of legit or un-poisoned data. This hash is stored in its exclude field. During CPA mitigation, this packet can flood the network. Consequently, it would enable multipath forwarding and inline verification of hash at the router. It can adversely affect the throughput of the network or even can cause DDoS. So, it's important to mitigate and add this additional security feature along with CPA mitigation.To prevent the Malicious Consumer to send a fake excluded Interest packet, a satisfaction test is performed to check if the excluded interest packet is a non-existent data in cache or a legit packet in the cache, in case of a cache miss (of the excluded interest packet) ratio reaches near the threshold value i.e. is set by the operator, it is considered as an attack. Delivery of legitimate content can be guaranteed to the consumer via the forwarding of reissued interest packet through multiple paths and on-demand signature verification, this is possible only if a path exists between a consumer and legitimate content source and there is no compromised node in between the path. But forwarding of reissued interest via multiple paths can examine the poisoned content using the same channel that the adversary used to poison the data. It can restore legitimate cache for future interest packets. In the recovery phase, the role of maintaining the states of the forwarding plane is very important as it uses the sliding window concept to store on-demand signature verification result history results. This result is stored against each FIB entry in the next hop field. The next-hop node becomes less preferred and its corresponding face is declared poisoned if its sliding window value of poisoned data exceeds the threshold value. This face will not be used to forward interest packets as it is now the least preferred next-hop node.

2.3 Comparisons Of CPA Mitigation Approaches

The following table is a summarized view of the CPA Mitigation approaches:

Algorithm 2: Forwarding of Reissued Interest Packet along Multiple paths

```
Require: INTEREST_PACKET (Content_Name; PPKD; nonce; IncomingInterface;
excluded)
1:  ContentStoreEntry ← FindInContentStore (Content_Name; PPKD)
2:  if ContentStoreEntry > 0 then
3:      if INTEREST.HasExcludedData ( ) = False then
4:          Return ContentInCS
5:      else
6:          if HasExcludedData (DATA) = True then
7:              Raise EVENT (FibEntry) //Alert: FibEntry
            end if
8:          if IsPoisoned (DATA) = True then
9:              Purge (this.DATA)
                NextHop.Cost ++
11:         end if
12:     end if
13: else
14:     PITCount ← FindInPIT (Content_Name; PPKD; ExcludedFilter)
15:     if PITCount is > 0 and nonce.IsUnique = TRUE then
16:         ifaces.Add (Incoming_Interfaces)
17:     else
18:         FIBCount ← FindInFIB (Content_Name; PPKD)
19:         if FIBCount is > 0 then
20:             if NextHop hop= 1 then
21:                 ForwardInterest (hop)
22:             else
23:                 foreach hop & flag = null
                    Malicious iface do
24:                     ForwardInterest (hop)
                    \\ Multiple Paths
25:                 end for
26:             end if
27:         end if
28:     end if
29: end if
```

FIGURE 2.7: Forwarding Of Reissued Interest Packet Along Multiple paths

2.4 Summary

Based on the analysis of existing techniques to detect and mitigate CPA, as described in this Chapter, there is still a need to sort out some challenges while developing a CPA mitigation strategy [3]. To design a comprehensive mitigation strategy of CPA, three main challenges need to be elaborated: First, to acquire legitimate content, what may be the alternate routes on which Interest Packet

Algorithm 3: Data Packet Arrival at NDN Routers

```
Require: DATA_PACKET (Content_Name; PPKD; iface)
1:   ContentStoreEntry ← FindInContentStore (DATA)
2:   if ContentStoreEntry > 0 then
3:         CS.PurgetData (DATA)
4:   else
5:         PITCount ← FindInPIT (Content_Name; PPKD; ExclusionFilter)
6:         if PITCount = 0 then
7:              PURGE (DATA)
8:         else
9:              if INTEREST.HasExcludedData ( ) = True
               AND IsPoisoned (DATA) = True then
10:                       Purge (DATA)
11:                       MinCostHop = FindMinCostHops (NEXTHOPS)
12:                       ForwardInterest (Interest, MinCost)
13:             else
14:                       ForwardDATA (ReversePath)
                          CS.Add (DATA)
15:             end if
16:        end if
17:  end if
```

FIGURE 2.8: Data Packet Arrival At NDN Routers

can be forwarded? If somehow the system can forward the request to a legitimate content source via some alternative route then the chances of CPA can be reduced. Although in the IKB technique which was proposed by the author in [26], a publisher public key digest (PPKD) is specified in the interest packet by the consumer but still it is possible that interest can be forwarded towards the malicious content source. There are two ways in which it can be done, first, anyone can use any prefix to advertise content and that can also be done without any authentication and authorization as per NDN specifications. So routers can't determine either they are forwarding the content towards legitimate content sources or malicious source. Ghali et al.[26] highlighted some of the NDN architecture vulnerabilities such as the PPKD field and name's digest are not the essential components of the Interest packet. Also, there is no such trust model that is adopted unanimously by the consumer's applications to fetch the content's hash securely. Based on these vulnerabilities, a technique is proposed, which enables an IKB rule to ensure trust. According to this rule, the Interest packet must include the producer's (content publisher's) public key. IKB implication for consumers is that it has to acquire and validate the public key of the content provider before initiating the Interest packet

TABLE 2.1: CPA Detection And Mitigation

Ref	**NDN Node**	**Detection**	**Mitigation**	**Overhead**
Gasti et al. [8]	Consumer, Router	Signature, PPKD	SSCIC, DSCIC	Verification of Random Signatures
Ghali et al. [25]	Consumer	Signature	Content Ranking	Content Ranking Calculation
Ghali et al. [26]	Router	PPKD and Signature	Interest Key Binding	Signature Verification
Nam et al. [19]	Router	Signature	SLRU Extension	Signature Verification
Kim et al. [21]	Router	Signature	SLRU Extension	Signature Verification
Wu et al. [17]	Consumer, Router	Signature	Reputation Based Forwarding	Signature Verification
Kim et al. [22]	Router	Signature in case of cache-hit	SLRU Extension	Signature Verification
DiBenedetto et al. [27]	Consumer, Router	Signature	Modified Forwarding Strategy	Complete Bogus Packet in Reissued Interest Packet
Hu et al. [3]	Consumer, Router	PPKD and Signature	Name-key based forwarding and mulitpath forwarding based Inband probe	Signature Verification (Hash matching is fast due to PPKD entry)

for that particular data packet. So to acquire a trust model, three approaches were proposed, one is that public keys of the content provider should be installed in the client application, the second one is the universal key name service and the third one is global search based service. The second challenge is how to restore valid content if content poisoning has occurred in on-path intermediate routers. If legitimate content sources are registered and specified by the consumer then there is a chance that CPA can be reduced but this is possible only when the content source is malicious. If an on-path intermediate router is malicious then CPA is still possible. To mitigate on-path content poisoning, alternate paths should be adopted by the NDN routers to restore legitimate content.

TABLE 2.2: Comparison Of Malicious Consumer Interest Packet

Reference	Checked by	Proposed Solution	Energy Efficient	Security Features
Gasti et al [8]	Consumer and Router	SSCIC & DSCIC	Yes	Cannot detect corrupted content
Ghali et al [25]	Consumer	Content Ranking Algorithm	No – Overhead of calculating the content ratings	Do not handle malicious consumer in case it reports false content rating.
DiBenedetto and Papadopoulos [27]	First Consumer and then router	Modifying Forwarding Strategy	No – uses Complete bogus packet in report	Only handles the malicious consumer identity but do not handle the corrupted data
Approach in this Thesis	First Consumer and then Router	Name-Key Based Forwarding and Multipath Forwarding Based Inband Probe	Yes – Only use a PPKD extra field and use bogus/corrupted data hash in excluded filter field of interest packet	Can block a malicious consumer generating false special interest packets.

The last challenge is that an efficient system is required to mitigate the CPA. Caching content at line-speed is still a big challenge for NDN routers, so a CPA mitigation system is required which will not add a significant burden on NDN routers. Energy management in routers is an important issue. Gao et al. [18] evaluated that CPA and caching issues can consume a considerable amount of routers' energy which can add instability to the whole system. Hu et al. in [3] have implemented a robust and efficient mechanism to mitigate the CPA. This system is comprised of three phases. First is the route building phase, then there is a normal content retrieval phase and the last one is the recovery phase in chase content poisoning has occurred. It is required that NDN routers should enable

name-key based forwarding to forward interest towards registered content sources and to specify legitimate content sources every route advertisement should be authenticated with a trust management system. In case, content poisoning occurs on intermediate routers then a mechanism of Multipath Forwarding based Inband Probe is performed. In this approach, an interest packet with an exclude filter (poisoned content) is reissued and forwarded via alternate paths. When this packet reaches a particular router, it enables cached contents' on-demand signature verifications. Verification of cached content is performed between the malicious payload that is included in the interest packets' exclude filter or in the Data Packet that is returned and gets matched with the reissued interest packet. This way poisoned contents will be purged and for future requests, legitimate contents will be returned from the routers' cache, thus it'll increase the overall throughput of the network In the following chapter, the security weakness of this system will be highlighted and a mitigation strategy is proposed, which is the main research area of this thesis.

Chapter 3

Proposed Approach

3.1 Introduction

The CPA mitigation, the approach using name-key based forwarding and Multipath forwarding based Inband probe is quite comprehensive and fills most of the attack surface regarding the Content Poisoning Attack. However, with the advent of the structural changes in the NDN architecture, it has induced a new attack vector that can be exploited by the adversary and with this attack, the whole system can collapse. So it is very crucial to highlight this aspect. One of the crucial attack vectors that have emerged with this technique is the flooding of the reissued Interest Packet that contains the excluded filter field and it is the main research contribution of this dissertation. A consumer with malicious intent can flood the network with the interest containing the hash digest of a legit or unpoisoned data in its exclude field which can flood the network and enable multipath. It can harm the throughput of the network or even can cause DDoS. Based on the research gap mentioned in the preceding section, this thesis has formulated the following research questions: RQ1: What will be the mechanism to detect the attack initiated by consumers with malicious intent? RQ2: What will be the parameters which will contribute to mitigating the malicious consumers' reissued

interest packet flooding attack? So it's important to mitigate and add this additional security feature in the above technique. This scenario is depicted in Figure 3.1.

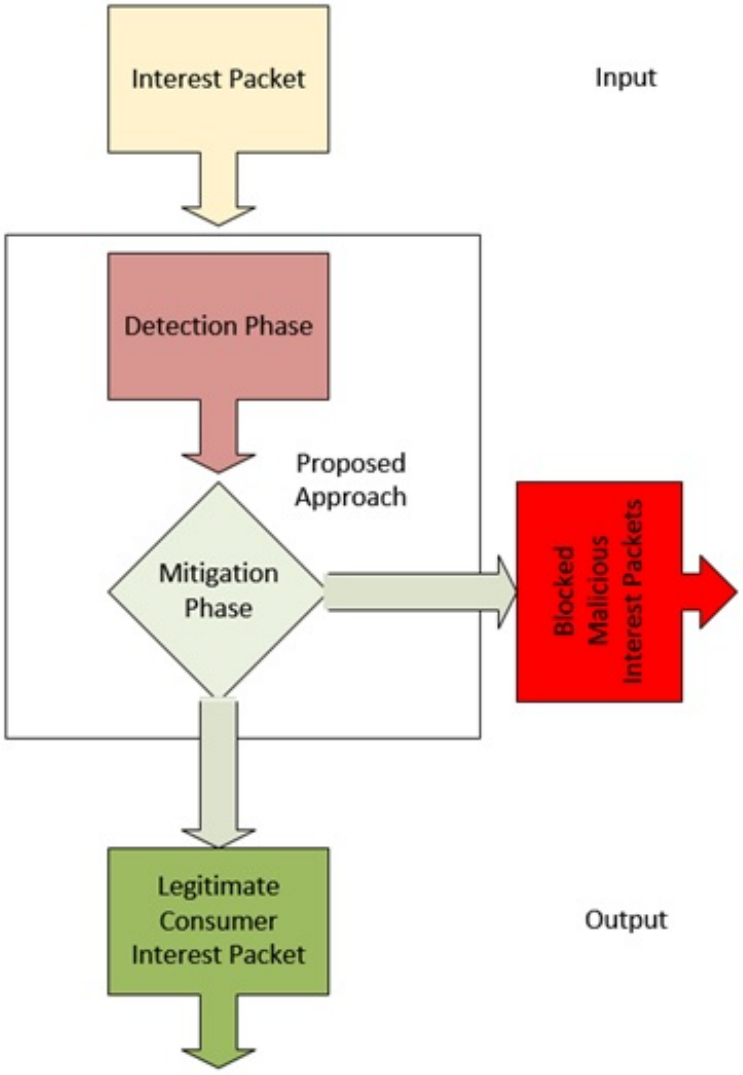

FIGURE 3.1: Block Diagram For Proposed Approach

3.1.1 Special-Interest Flooding Attack Detection Scheme

During the CPA, the reissued Interest Packet by the consumer stores the poisoned data hash in the excluded filter field. The compromised consumer can flood the next router with the reissued Interest packets containing legit data hash. This will

result in a cache miss. The Inline verification at the router will also be enabled during this process, which can consume a lot of processing power of the router. When a consumer with malicious intent bombards these excluded Interest packet, although they get discarded at the next router upon verification, it'll drastically increase the processing overhead on the router. Other legitimate consumers will face a denial of service from this router. This attack vector should be taken into account and a mitigation strategy should be devised for such attacks. This way the process of CPA mitigation will be severely affected. The block diagram as shown in Figure 3.2 depicts the scenario of flooding attack of Interest Packet with excluded filter. The first block shows that the normal Interest packet is generated by the consumer. Then a decision is taken in the next block that whether it is a normal Interest packet or an Interest packet with an excluded filter field. In case it is a normal Interest packet it is directed towards normal NDN operations otherwise it is passed to the next module of On-Demand Signature Verification. Here signature verification is performed against PPKD in the Content Store. If verification fails then this packet is discarded otherwise it gets purged from the CS of the router. In case, if poisoned data is found in the CS, the normal process is initiated and content poisoning mitigation will commence as per the method mentioned in Chapter 2. When a consumer is compromised and it starts flooding the NDN Network with the excluded filter enabled Interest packet, it will trigger On-Demand Signature verification for each bogus packet and the next NDN router will get saturated. The queue will be occupied and after a while, there will be lesser space for legitimate excluded filter Interest packet. This will hamper the CPA Mitigation strategy badly. So this scenario is considered as an attack and needs mitigation.A consumer with malicious intent can flood the network with the interest containing the hash digest of a legit or unpoisoned data in its exclude field which can flood the network and enable multipath. It can harm the throughput of the network or even can cause DDoS The block diagram of the proposed approach has been elaborated in Figure 3.2 and Algorithm 4 (Figure 3.6)in the coming sections.

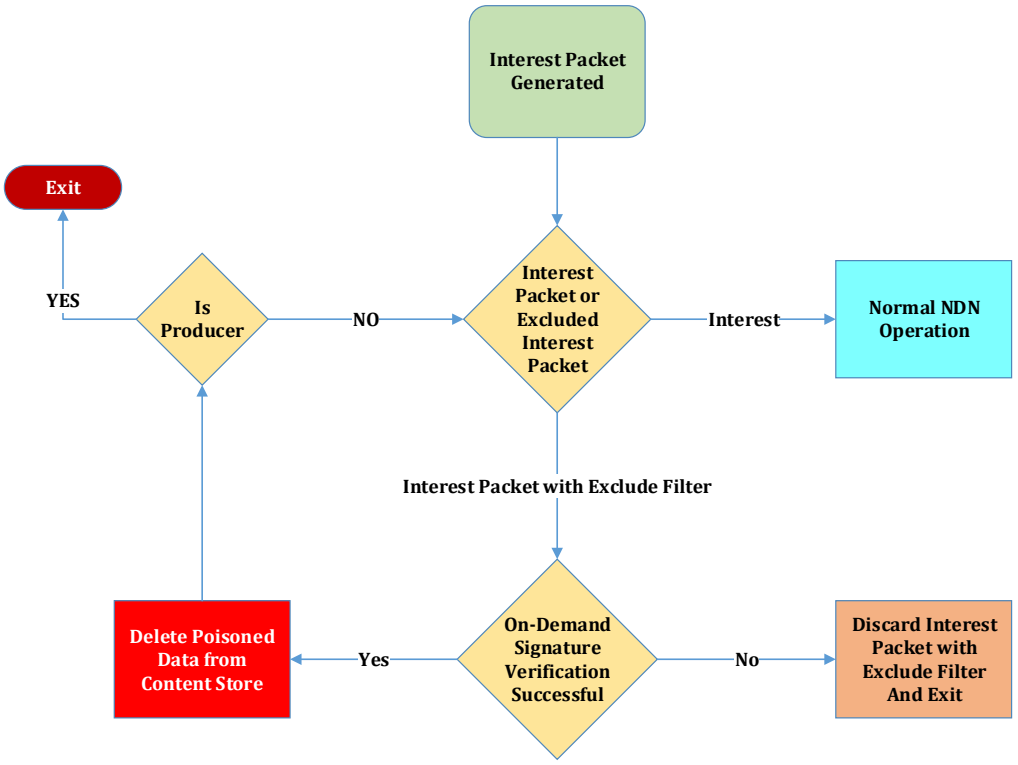

FIGURE 3.2: Detection Scenario: Flooding Attack Of Special Interest Packet

3.1.2 Special-Interest Flooding Attack Mitigation Scheme

In this thesis, a reactive approach is proposed to mitigate this attack. The router structure is shown in the Figure below which is depicting the virtual queues scenarios. These queues are shared among different consumers on FIFO queueing discipline. The queue of router saturates if the flooding rate is more than the verification rate. Before the special interest packets get verified they are temporarily stored in these queues. To prevent the Malicious Consumer to send a fake excluded Interest packet, a satisfaction test is performed to check if the excluded interest packet is a non-existent data in cache or a legit packet in the cache, in case of a cache miss (of the excluded interest packet) ratio reaches near the threshold value i.e. is set by the operator, it is considered as an attack. Summary is that during the CPA, the reissued Interest Packet by the consumer stores the poisoned data

hash in the excluded filter field. The compromised consumer can flood the next router with the reissued Interest packets containing legit data hash. This will result in a cache miss. The Inline verification at the router will also be enabled which can consume a lot of processing power of the router. This way the process of CPA mitigation will be severely affected. This attack is a kind of a flooding attack of special interest packet and it requires mitigation.

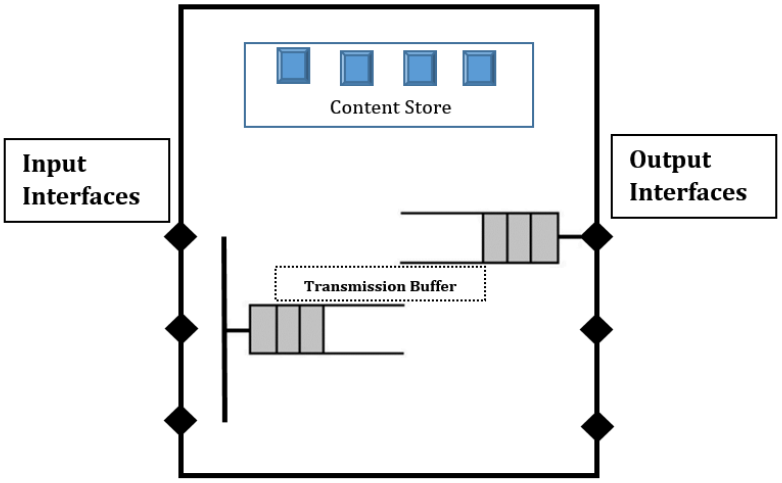

FIGURE 3.3: NDN Router Model

3.1.2.1 Reactive Approach

A virtual queue is utilized in NDN Routers for incoming reissued Interest packets from the consumers. FIFO queue is shared among all the incoming faces for reissued interest packets. This is a temporary place holder for these packets until they get verified according to the procedure mentioned in the preceding sections. The allotted memory for the transmitting packets should be different from the one used for caching. If the same CS is used for both transmitting packets and data chunk then the CS will be congested with the data chunks that are waiting to be satisfied by the pending Interest packets. Ref figure 3.3, for simplicity PIT and FIB data structures are not depicted in the figure. In order to prevent the Malicious Consumer to send a fake excluded Interest packet, a satisfaction test

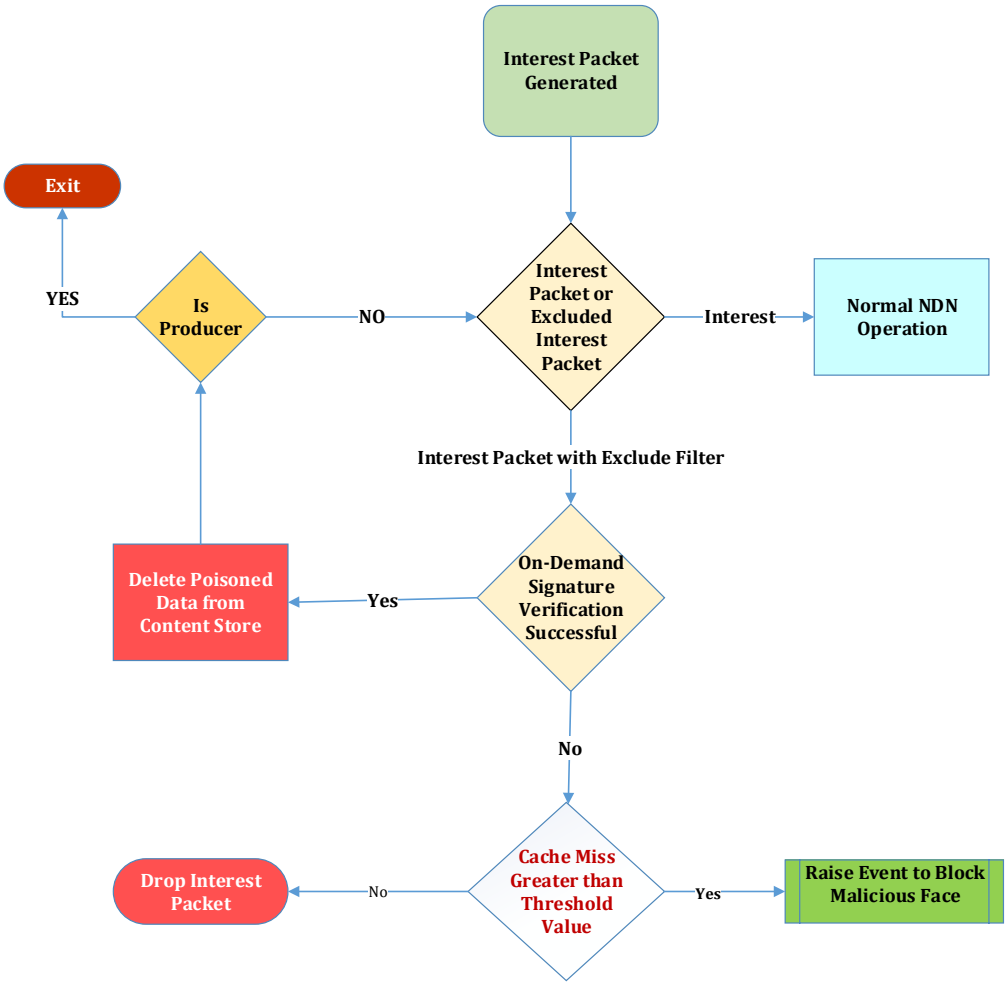

FIGURE 3.4: Mitigation Scenario: Flooding Attack of Special Interest Packet

is performed to check if the excluded interest packet is a non-existent data in the cache or a legit packet in the cache. In case, a cache miss (of the excluded interest packet) occurs and the ratio reaches near the threshold value i.e. set by the operator, it is considered as an attack. On-demand verification at the router is not enabled unless there is a cache hit for excluded interest packet, this will reduce the overhead of content verification at the router of each data packet. However, in case of a cache miss, this excluded interest packet is discarded. If a consumer with malicious intent floods the edge router with the fake interest packet with the exclude filter it'll degrade the performance of that particular edge router. The NDN-router service manager at the NDN Router especially at the edge of the network in the consumer domain maintains the stats and checks these values. The

router will drop the future reissued interests coming from this face that has the excluded data packet as it is considered as a malicious consumer upon hitting the threshold value. This will be done temporarily and delisted at the discretion of the network operator. This mechanism is elaborated in Algorithm 4 (Figure 3.6). Following are the data structures for CS, PIT, and FIB along with the required changes to mitigate this flooding attack in Table 2.1, Table 3.2 and Table 3.3 respectively: A new lightweight parameter is added in the CS Data Structure (Figure 3.5) to retain the cache miss counter of invalid reissued Interest packet with excluded filter field. This value is compared with the threshold value. Block diagram can show the birds-eye view of this proposed mechanism in figure 3.4

We have introduced a block of proposed approach. The reissued Interest packet upon several caches miss and hit the specified threshold value will trigger an event and blocks this malicious face. On the next iteration, this reissued packet from the malicious consumer face will be blocked. It is evident from the Figure 3.5

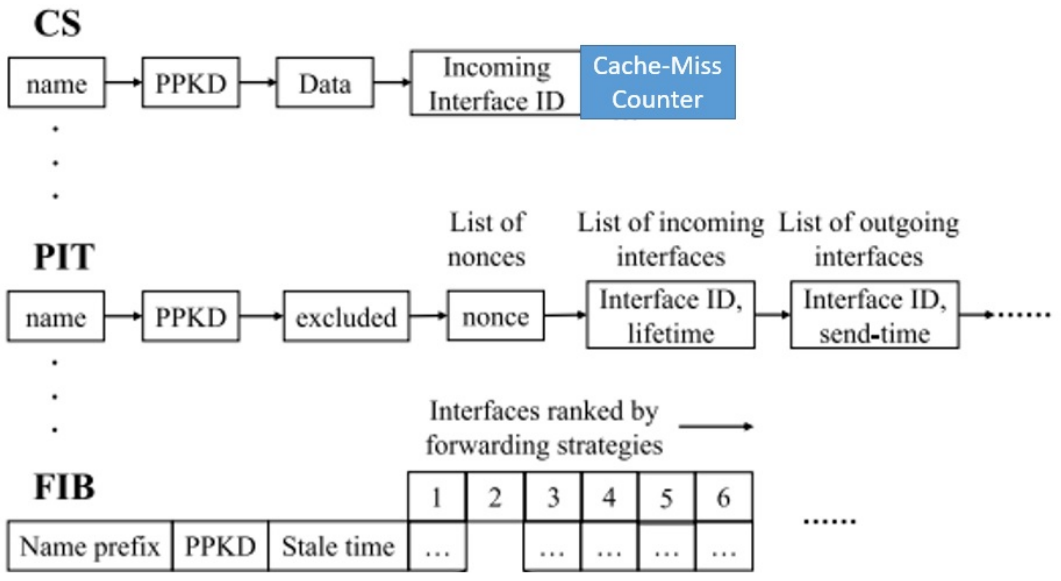

FIGURE 3.5: Modification In CS Data Structure

that Content Store, Pending Interest Table and Forward Information Base data structures contain Name and PPKD fields each. Name-Key Based forwarding is possible with the help of these two fields. Pending Interest Table contains both

List of Incoming Interfaces and Outgoing Interfaces. Also, the excluded filter field is present in the PIT structure. This field is matched during the Content Poisoning Attack Mitigation process. The consumer upon verification of poisoned content places the hash of that poisoned data in the excluded field of Interest packet which is compared against the excluded field of the PIT table. The Content Store data structure is modified and a lightweight parameter is added to it. This parameter retains the cache miss counter value and gets incremented if a cache-miss occur against a particular Incoming Interface ID. This value is compared against the specified threshold value. In algorithm 3.6, a scheme for detection and mitigation of flooding of malicious special interest packets is implemented. Name-Key-based pair as Content Name and PPKD, nonce, list of incoming interfaces, hash in the excluded field, threshold value and the cache miss counter values are passed as arguments to this function. RESULT variable is an enumerated data having values of Cache-Hit and Cache-Miss. Hash comparison is performed for PPKD value in the excluded filter field and that of stored in Content Store data structure. If RESULT is a cache-miss then the cache-miss counter value gets incremented and this value is retained in the modified CS data structure. If the cache-miss counter value becomes equal or exceeds the threshold value then an event will be triggered that will raise a flag and declare that incoming face malicious. Also, the same malicious face will be blocked. If the result is a cache-hit then bogus content is searched in the content store against the Name-Key-based pair, if bogus content is found then that poisoned data gets purged and the same interest packet is forwarded on multiple paths. This mechanism will restore legitimate content to the consumer.

Table 3.1: CS Data Structure

CONTENT_STORE	
Field	**Type**
Name	String
PPKD	String (HASH)
Data	Binary
Incoming Interface ID	List of Strings
Cache-Miss-Counter	Integer

Table 3.2: PIT Data Structure

PENDING_INTEREST_TABLE	
Field	**Type**
Name	String
PPKD	String (HASH)
Excluded	Binary
Nonce	List of nonce Strings
Interface ID, Time-Out	List of Strings (incoming interfaces) Comma Separated List
Interface ID, Time_Interest_Packet_Forwarded	List of Strings (outgoing interfaces) Comma Separated List

Table 3.3: FIB Data Structure

FORWARD_INFORMATION_BASE	
Field	**Type**
Name Prefix	String
PPKD	String (HASH)
Excluded	Binary
Nonce	List of nonce Strings

Algorithm 4: Detection & Mitigation of Flooding Attack of Reissued Interest Packet

```
Require: REISSUED_INTEREST_PACKET (Content_Name; PPKD; nonce;
IncomingInterface; excluded, THRESHHOLD, CACHE_MISS_COUNTER)
      //RESULT is Enumerated Data having values CACHE_HIT & CACHE_MISS
1:    RESULT ← HashComparison (PPKD_HASH_ExcludeFilter; PPKD_CS)
2:    if RESULT = CACHE_MISS then
3:          CACHE_MISS_COUNTER += 1
4:          if CACHE_MISS_COUNTER = THRESHOLD then
5:                RAISE_EVENT (FLOODING_ATTACK_MITIGATION)
6:                RAISE_EVENT (INCOMING-INTERFACE-POISONED-FLAG)
7:                PIT.DROP (Interest)
6:                EXIT
7:          end if
8:    else if RESULT=CACHE_HIT
9:    ContentStoreEntry ← FindInContentStore (Content_Name; PPKD)
10:   if ContentStoreEntry > 0 then
11:         if INTEREST.HasExcludedData ( ) = False then
12:               Return ContentInCS
13:         else
14:               if HasExcludedData (DATA) = True then
15:                     Raise EVENT (FibEntry) //Alert: FibEntry
16:               end if
17:               if IsPoisoned (DATA) = True then
18:                     Purge (this.DATA)
19:                     NextHop.Cost ++
20:               end if
21:         end if
22:   else
23:         PITCount ← FindInPIT (Content_Name; PPKD; ExcludedFilter)
24:         if PITCount is > 0 and nonce.IsUnique = TRUE then
25:               ifaces.Add (Incoming_Interfaces)
26:         else
27:               FIBCount ← FindInFIB (Content_Name; PPKD)
28:               if FIBCount is > 0 then
29:                     if NextHop hop= 1 then
30:                           ForwardInterest (hop)
31:                     else
32:                           foreach hop & flag = null
33:                           Malicious iface do
34:                                 ForwardInterest (hop)
                              \\ Multiple Paths
35:                           end for
36:                     end if
37:               end if
38:         end if
39:   end if
```

FIGURE 3.6: Detection And Mitigation Of Flooding Attack Of Special Interest Packets

3.1.2.2 Proactive Approach

This approach helps the Network Operators set up the threshold value automatically during the special interest packet flooding attack by a malicious consumer. This approach aims to select the threshold value in an automated fashion based upon statistical monitoring of buffer capacity and cache miss ratio. In this approach, a Network Management software continuously monitors the cache miss ratio and buffer capacity when a special interest packet is flooded by the compromised consumer. When the cache miss ratio average over a while results in a buffer overflow, the threshold value is thrashed to half. This process continues unless the threshold value becomes one. This mechanism is elaborated in Algorithm 5 (Figure 3.7). At this stage, the incoming face causing the flooding attack will get blocked till the particular timeout.

$$InitTH = QueueSize/VerificationRate \tag{3.1}$$

$$Cache\_Miss\_Ratio = CM/(CM + CH) \tag{3.2}$$

Network Management Software will continuously monitor the Cache_Miss_Ratio and Buffer Size of the queue. In algorithm 3.7, arguments like total queue size, list of incoming interfaces, packet verification rate, cache miss and cache hit values are passed. At first, the initial threshold value is set by taking the total queue size and divided it by the verification rate. Then current queue size is acquired from the NDN service manager which continuously watches the stats of the router. The running average of cache miss ration is calculated after specific intervals. The proposed idea is that if the cache miss ration values exceed 50% and queue capacity saturates then this threshold value is reduced to half. This process continues in a particular thread in which it sets up the specific threshold value against the particular incoming interface until the threshold value becomes less than one. Then that malicious face is blocked. This algorithm activates only in case when cache miss ration exceeds 50%.

Algorithm 5: Automated Threshold Value

Require: **SET_THRESHOLD_VALUE** (Total_Queue_Size; IncomingInterface; PktVerificationRate, Cache_Miss_Value, Cache_Hit_Value)

```
//Initialize Threshold Value
1: THRESHOLD_VALUE = Total_Queue_Size / PktVerificationRate
2: Current_Queue_Size = FUNCTION_Get_Queue_Occupation( )
3: WHILE ( TRUE )
4: IF (THRESHOLD_VALUE<=1) THEN RETURN 1
5: CACHE_MISS_RATIO = CACHE_MISS_VALUE / (CACHE_MISS_VALUE  + CACHE_HIT_VALUE)
6: IF ( Current_Queue_Size / Total_Queue_Size >= 1) THEN
7:       IF (CACHE_MISS_RATIO > 50) THEN
8:             THRESHOLD_VALUE = THRESHOLD_VALUE * 1/2
9:       END IF
10: END IF
11: RETURN THRESHOLD_VALUE
12: END WHILE
```

FIGURE 3.7: Algorithm: Dynamic Threshold Value

Chapter 4

Experimental Results

4.1 Network Topology

4.1.1 Network Topology With One Malicious Consumer

In scenario 1, The network topology that we used in our simulations consists of two routes from the consumer to the producer. Two paths routes that are used in this scenario are 0-1-2-4-6-7-8 and 0-1-3-5-7-8, these paths are between the consumer and a producer [30], as can be seen in figure 4.1 below: In the above scenario, it is evident that consumers with malicious intent can flood the network with unwanted interest packet with excluded field occupied by the non-malicious or legit payload. If not mitigated at the edge router, all the routers will enable the on-demand verification and this way router performance will degrade with time. This problem can be mitigated by enabling a mechanism at edge routers of NDN and setting a threshold value that if it hits this value then block that interface through which these malicious excluded interest packets are coming. This way rest of the network will be safe from acquiring this malicious packet from consumers and ultimately the performance of the intermediate routers will not be degraded. So to handle this issue Network Manager at NDN Edge Router enables this mechanism in which malicious interest packet with exclude field is dropped in case of a cache

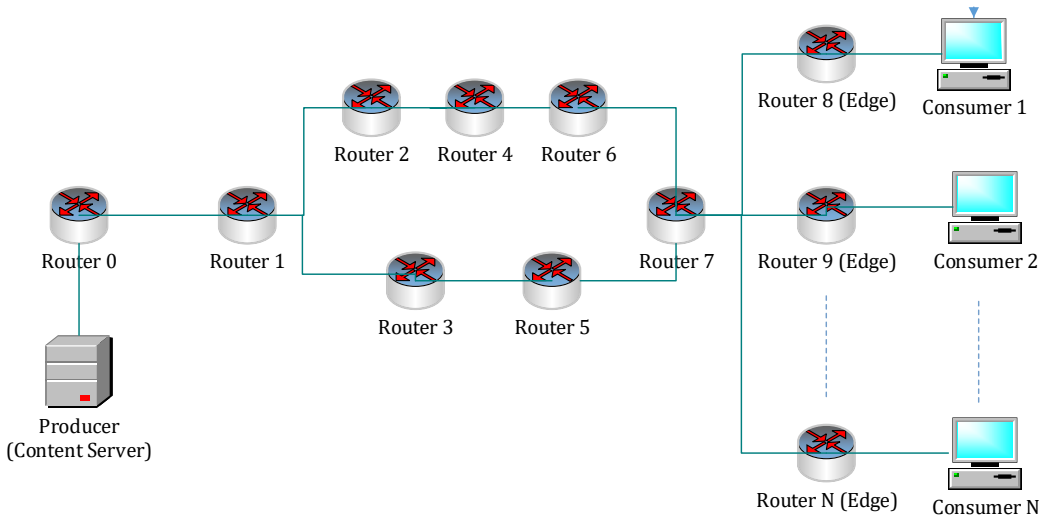

FIGURE 4.1: Network Topology with One Malicious Consumer

miss and upon hitting the threshold value, the interface from which these excluded interest packets are received is blocked and added to the delist data structure. The timeout to get out of this delist data structure is at the desecration of the network operator.

4.1.2 Network Topology With Two Malicious Consumers

In scenario 2, The network topology that we used in our simulations consists of two routes from two consumers (i.e. Consumer 1 and Consumer 2) of the same domain to the producer via Router 8 (edge router). The routes that are used in this scenario is 0-1-2-4-6-7-8 and 0-1-3-5-7-8, these paths are between the consumer and a producer [30], as can be seen in figure 4.2 below: The main thing to note in this scenario is that Consumer 1 and Consumer 2 are in the same domain. At router 8, the virtual queue for Incoming Reissued Interests is shared between these two consumers. The Queuing mechanism used in this scenario is FIFO. In this scenario, there are two consumers with malicious intent and can flood the network with unwanted interest packet with excluded field occupied by the non-malicious or legit payload. If not mitigated at the edge router, the virtual queues will be fully occupied for the legit reissued interest packet and consequently, packets will

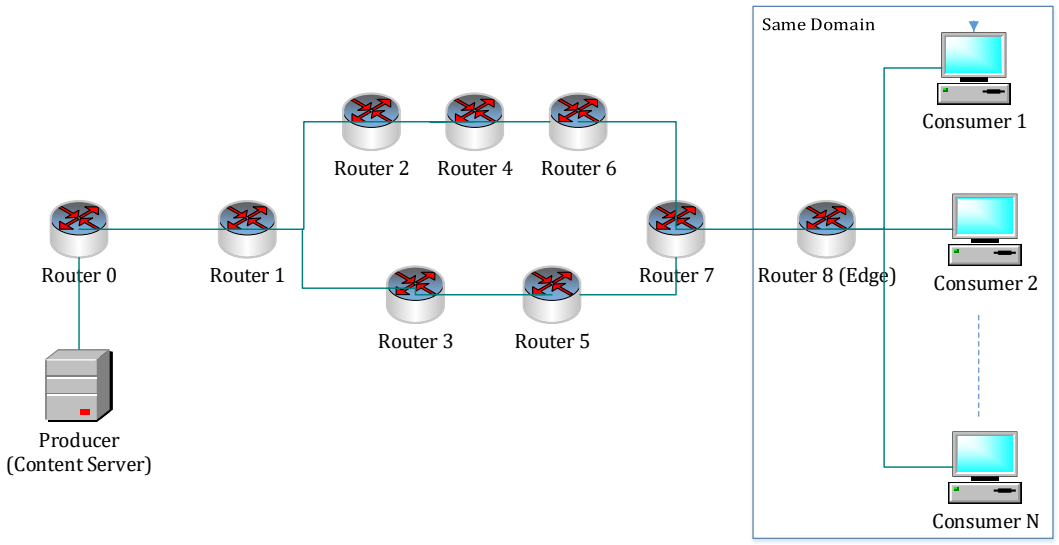

FIGURE 4.2: Network Topology with Two Malicious Consumers

drop. This problem can be mitigated by enabling a mechanism at edge routers of NDN and setting a threshold value that if it hits this value then block that interface through which these malicious excluded interest packets are arriving. This way rest of the network will be safe from acquiring this malicious packet from consumers and ultimately the performance of the intermediate routers will not be degraded.

4.2 Simulation Environment

For proof of concept and to run this scenario, a custom-built NDN Simulator is developed in C# language in Visual Studio 2019. The main interface along with the nodes configurations is shown in figure 4.3. There are three modes of this application. Users can select NDN Router Mode, Consumer Mode and Producer Mode. This simulator is configured as per the scenario requirement as per topology in Figure 4.1 and Figure 4.2.

The consumer module can bombard the next NDN router with the Normal Interest Packet, the Special Interest Packet and the Malicious Special Interest Packet. The packets are bombarded in the batches form, the default value is 100 packets. This module can also flood the random batches of these packets. GUI of the consumer

module is shown in Figure 4.4.

NDN Router module GUI is shown in Figure 4.5. This module receives the bombarded packets from the consumers and displayed in pane along with the timestamp. Users can set up different queue sizes to test different parameters. Also threshold value can be configured to validate our proposed approach.

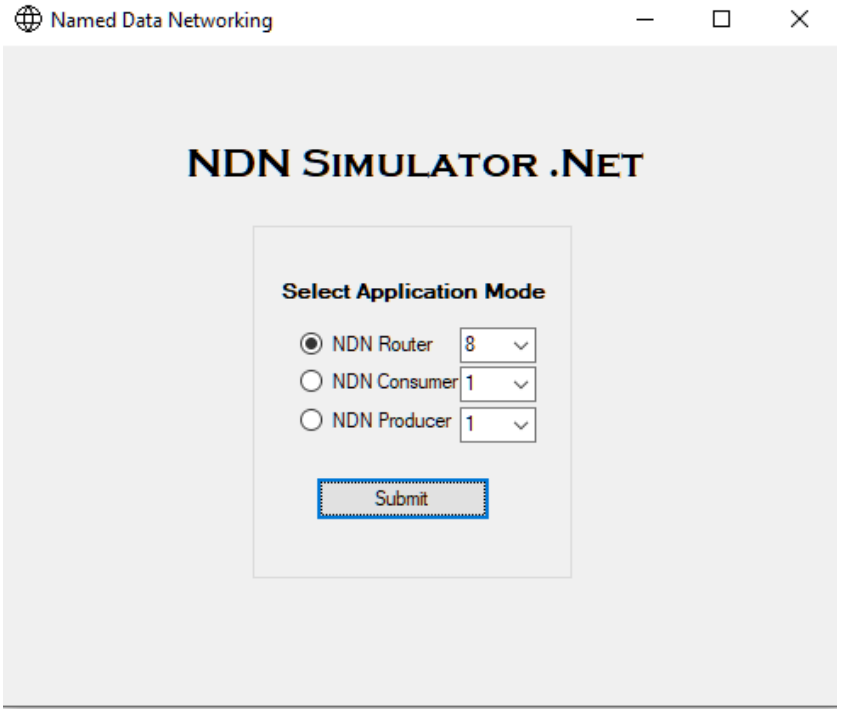

FIGURE 4.3: Consumer Module

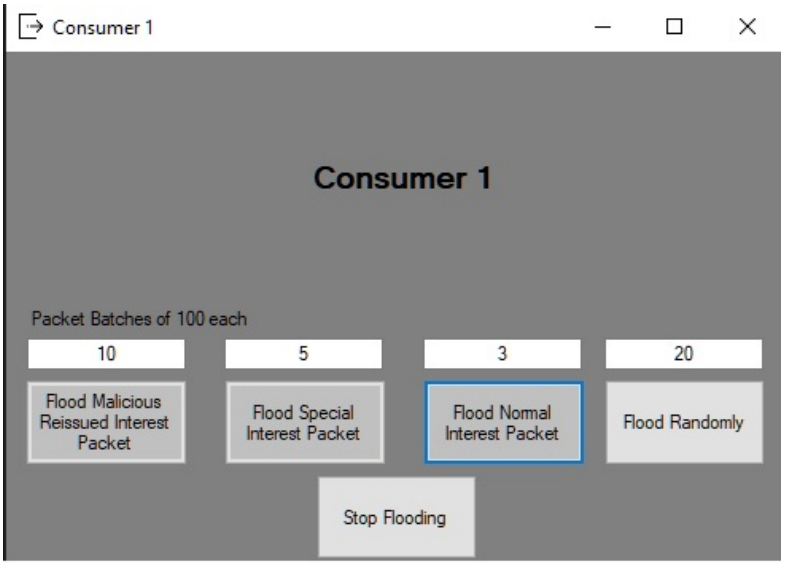

FIGURE 4.4: Simulation Environment

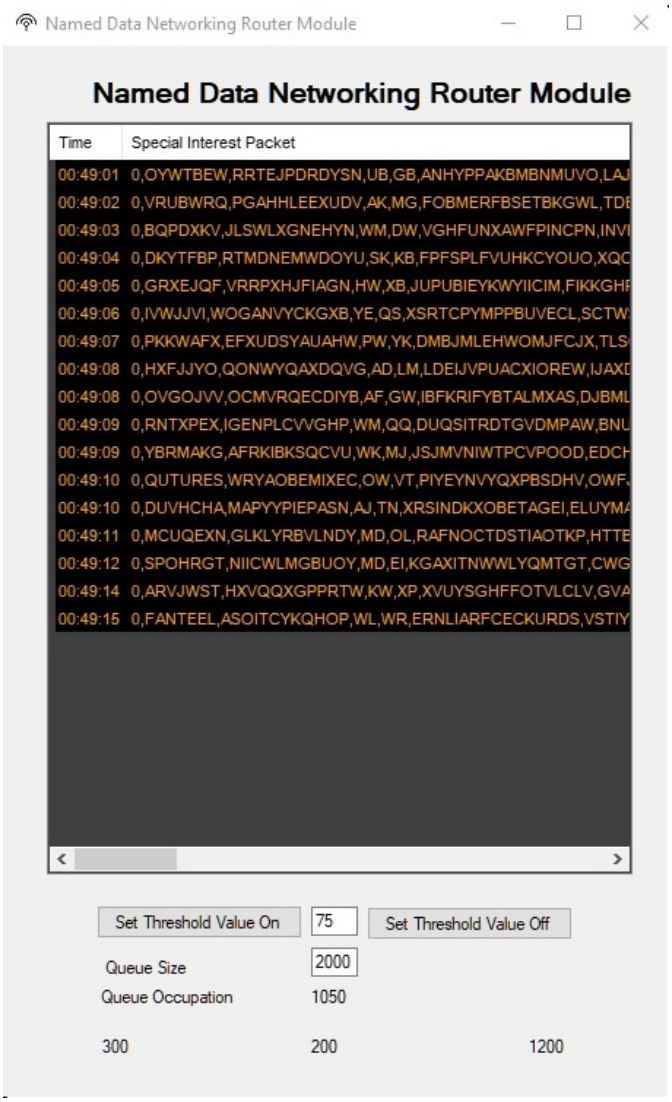

FIGURE 4.5: Router Module

4.3 Parameter setting for simulation

Table 4.1 displays the parameter settings for our simulation environment. Interest packet flooding rate is 100 Interest packets per second per malicious consumer. The virtual queue length for the NDN edge router is configured for two different scenarios. In one scenario i.e. one malicious consumer, its queue size is set to 500 packets and 1000 packets is set for the second scenario in which two malicious consumers bombards these interest packets. Verification rate is restricted to 25

Interest packets per second and threshold value is configured to three which is multiple of the verification rate.

TABLE 4.1: Simulation Parameters for Flooding Attack and its Mitigation

Parameter	Default Value
Request Rate	100 Interests/second/Consumer (Interest with Exclude Parameter)
Interest Packet Max Queue Length	500 (Experiment 1 and Experiment 2) 1000 (Experiment 3 and Experiment 4)
Verification of Interest Packet	25 Interest/second
Number of Malicious Consumers	1 (Experiment 1 and Experiment 2) 2 (Experiment 3 and Experiment 4)
Threshold Value	3

4.4 Experiments and Result

4.4.1 Flooding Attack By One Malicious Consumer

In this experiment, we have calculated the cache miss ratio of the interest packet containing the exclude filter and compared it with the Queue Length. Upon flooding the router with fake interest packet, the verification process takes time and meanwhile, the queue of interest packets will start increasing. After every second 25% fake packet will drop and 75% will be added to the queue. Initially, no threshold value is set, and after sometime congestion at the router's incoming interest packet queue will occur which will result in a drop of other future packets at this router. The experiment result is depicted in Figure 4.6.

4.4.2 Mitigation Of Flooding Attack By One Malicious Consumer

In the second experiment, our proposed scheme is enabled at the edge routers in Network Management software. Upon cache miss threshold value reaches 3, it'll block the incoming face of the consumer and further no interest will be received

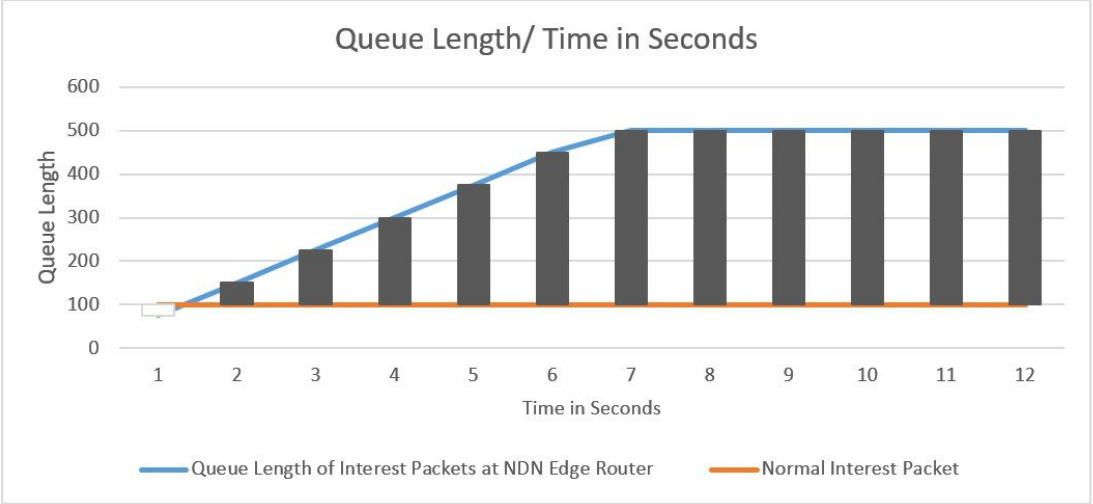

FIGURE 4.6: Experiment: Flooding Attack with One Malicious Consumer

from this malicious consumer face. After hitting a threshold value i.e. according to the cache miss value, the face is blocked and fake packets begins to be dropped from queue upon verification at rate of 25 interests/second. At 12 seconds the queue will be empty and router is no more. The experiment result is depicted in Figure 4.7.

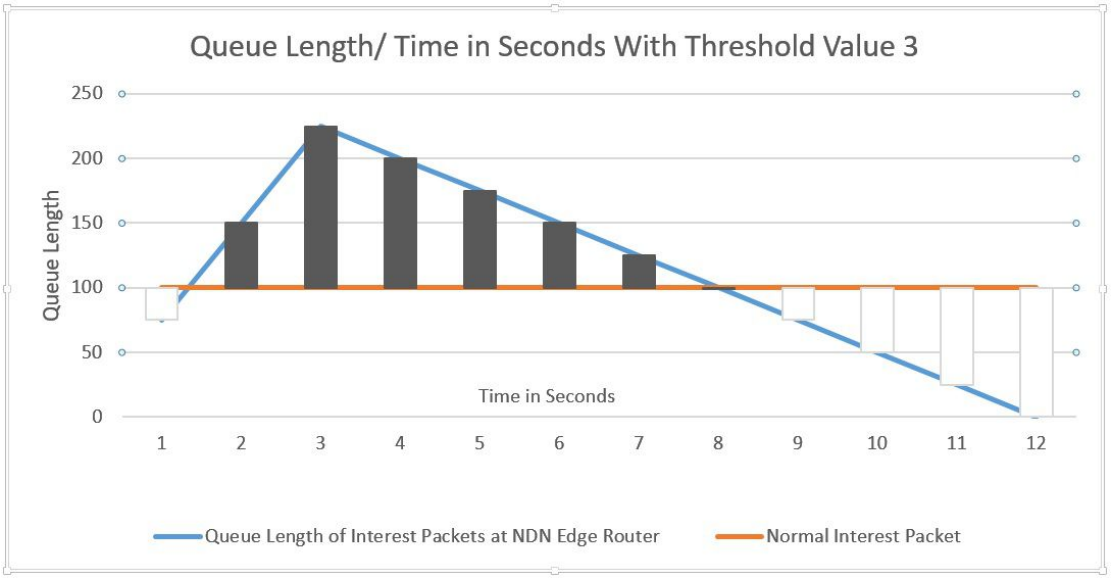

FIGURE 4.7: Experiment: Mitigation of Flooding Attack with One Malicious Consumer

4.4.3 Flooding Attack By Two Malicious Consumers

In the third experiment, Consumer 1 starts flooding the network with fake interest packets with the excluded filter, the queue will begin to saturate as the verification rate is slow as compared to the flooding rate. In the 6th second, Consumer 2 also starts to flood the network, consequently, the queue begins to saturate linearly.

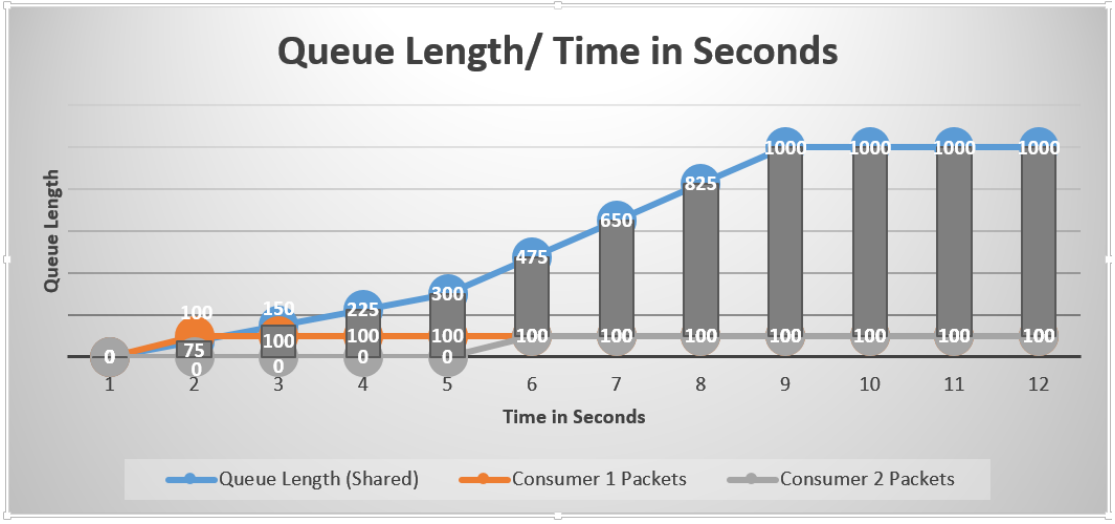

FIGURE 4.8: Experiment: Flooding Attack with Two Malicious Consumers

Initially no threshold value is set, and at 9th second congestion at router's incoming interest packet queue will occur which will result in drop of other future packets at this router.

4.4.4 Mitigation Of Flooding Attack By Two Malicious Consumers

In the fourth experiment, our proposed scheme is enabled at the edge routers in Network Management software. Upon cache miss threshold value reaches 3, it'll block the incoming face of the consumer1 after 3 failed verification at 4th second, further no interest will be received from this malicious consumer face. At 6th second, Malicious consumer 2 starts to saturate the queue which will, and similarly, after 3 failed attempts this face gets blocked as well and queues start to thrashed after both of the malicious consumer faces are blocked.

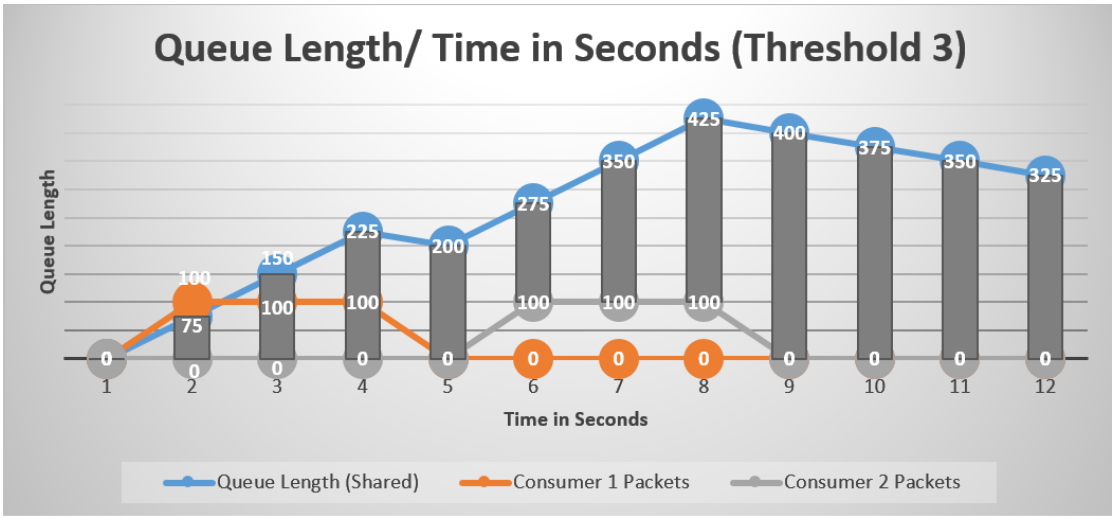

FIGURE 4.9: Experiment: Mitigation of Flooding Attack with Two Malicious Consumers

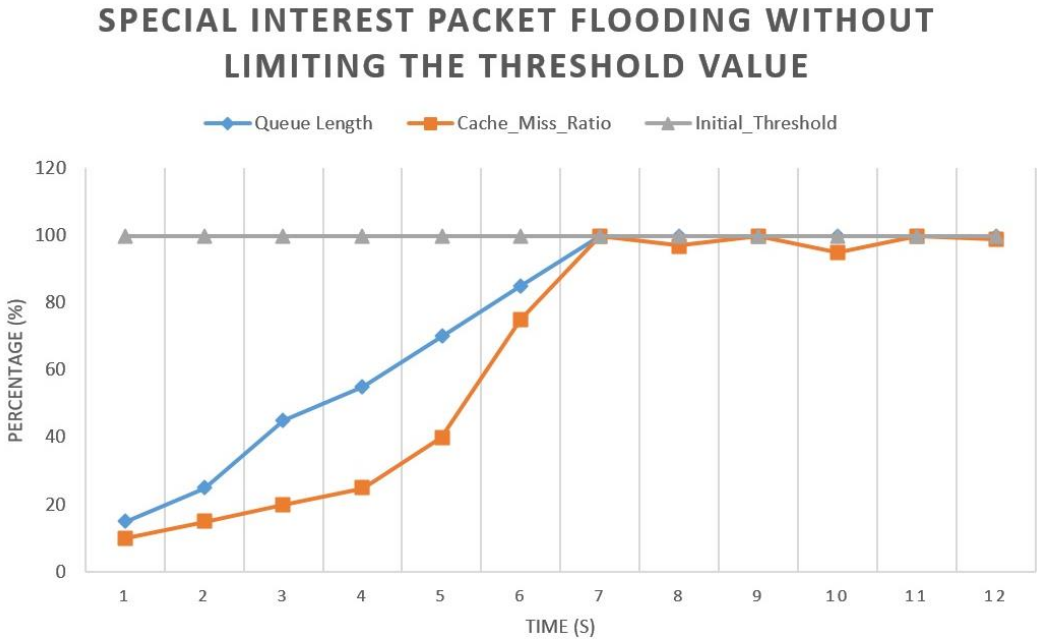

FIGURE 4.10: Without Dynamic Threshold Value

4.4.5 Dynamic Threshold Value

It is evident in the experiment that with the increase in the Cache_Miss_Ratio, the Queue size will increase because the flooding rate is greater than the verification rate. Also, Cache_Miss has penality on the processor of the router, which can increase the processing overhead. In the graph (Figure 4.10), the initial threshold

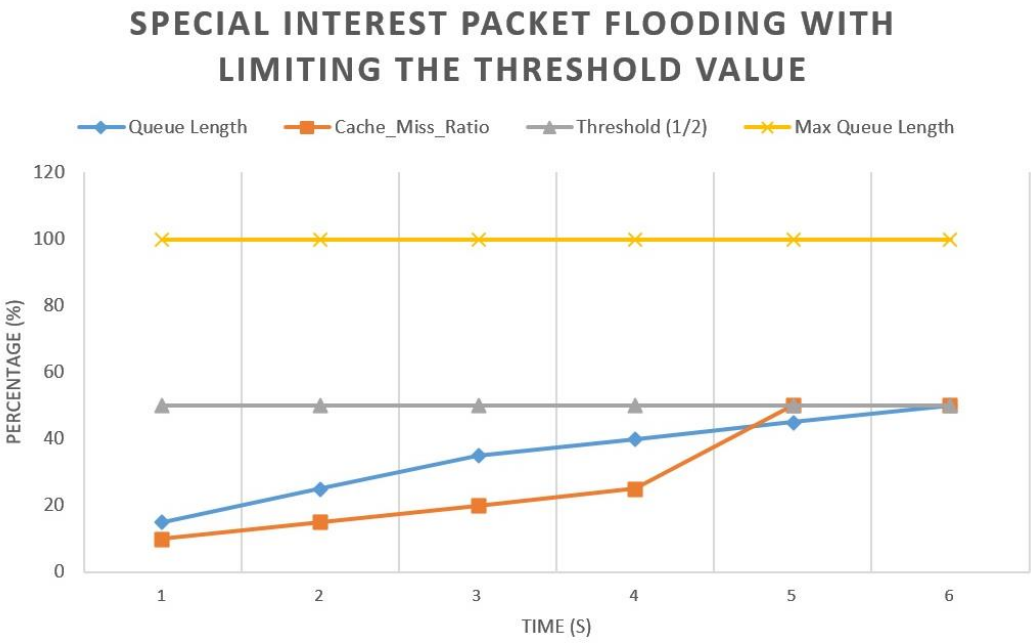

FIGURE 4.11: With Dynamic Threshold Value

value is set to buffer size divided by the packet verification rate. At 7th second the queue is filled up to 100 percent. At this stage, the new packets will start to drop. Here, the system should act prudently and reduce the threshold value to half of the current value, and if flooding continues threshold value is reduced to half as shown in Figure 4.11, and so on till the value is reduced to 1. At this stage, the incoming face is blocked as it is considered as an attack. The queue will not be saturated, and memory will be available for other interest packets to get processed. If the flooding attack continues, we will multiplicatively decrease the threshold value to another half. This mechanism will continue against that particular flooding malicious face until the threshold value reaches 1. At this stage, that particular face will be blocked and considered as a malicious face. The face will be blocked until the timeout, whose value will be at the network operator's discretion. This approach helps the Network Operators set up the threshold value automatically during the special interest packet flooding attack by a malicious consumer. This approach aims to select the threshold value in an automated fashion based upon statistical monitoring of buffer capacity and cache miss ratio. In this approach, a Network Management software continuously

monitors the cache miss ratio and buffer capacity when a special interest packet is flooded by the compromised consumer. When the cache miss ratio average over a while results in a buffer overflow, the threshold value is thrashed to half. This process continues unless the threshold value becomes one.

4.5 Quantitative Analysis

4.5.1 Effectiveness And Accuracy Of Proposed Solution By Comparing The Throughput Of The Normal Special Interest Packets

TABLE 4.2: Simulation Parameters For Effectiveness of Proposed Approach

Parameter	Default Value
Request Rate	100 Interests/second/Consumer (Special Interest Packets)
Interest Packet Max Queue Length	500
Verification of Interest Packet	25 Interest/second
Number of Malicious Special Interest Packets	2000 pkts
Number of Normal Special Interest Packets	1000 pkts
Number of Malicious Consumers	1
Threshold Value	3

In the first scenario, 2000 malicious interest packets are bombarded by one compromised consumer. 1000 Normal Interest Packets were also induced in the system by a legitimate consumer in the same domain. In this scenario, no threshold value is set. The maximum throughput of a particular face is 100 bps. Initially, the throughput of the normal interest packets was up to 90% of the total capacity which is the desired result. But in the subsequent seconds, the Malicious packets entered the router. Queue capacity started to saturate, the throughput of the normal interest packet will start to drop as the queue gets filled up with the bombarded malicious packets. The processing overhead also started to increase because of the cost of the cache-miss penalty and verification overhead. This scenario is depicted in Figure 4.12.

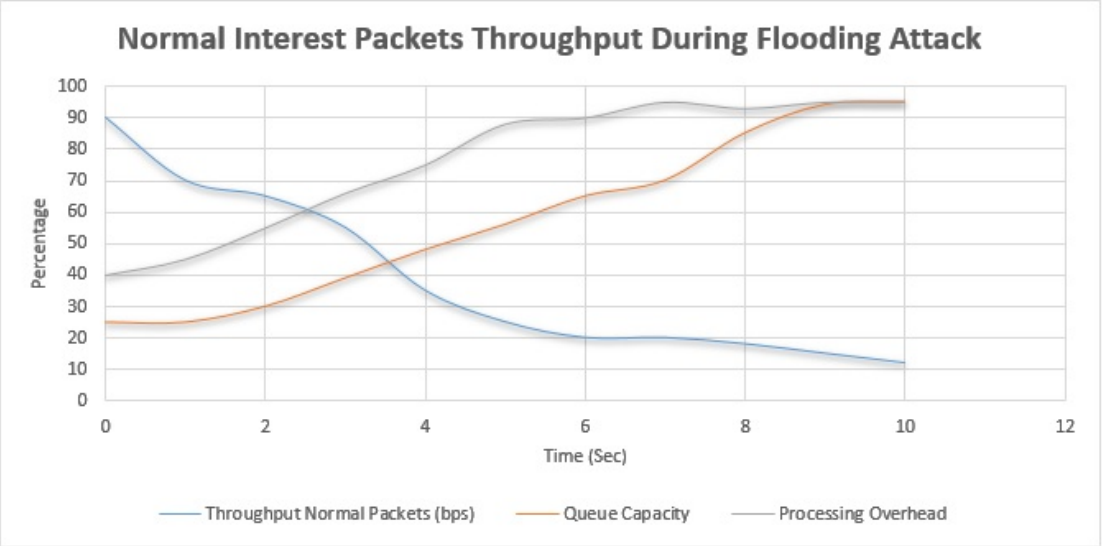

FIGURE 4.12: Throughput Of The Normal Special Interest Packets In Flooding Attack Scenario

In this second scenario, again 2000 malicious interest packets are bombarded by one compromised consumer. 1000 Normal Interest Packets were also induced in the system by a legitimate consumer in the same domain. In this scenario, our proposed solution is placed and activated inside the NDN Router service manager. The maximum throughput of a particular face is 100 bps. The throughput of the normal interest packets was up to 90% of the total capacity which is the desired result. But in the subsequent seconds, the Malicious packets entered the router. Queue capacity started to saturate, then the proposed solution gets activated and blocks the malicious face when the cache miss counter value reached the threshold value. Then we can see that according to our simulation environment after 3rd-second malicious packets didn't enter the router queue and throughput of the normal interest packet will start to raise and other factors like processing overhead and queue capacity ratio gets into the normal working range. This scenario is depicted in Figure 4.13.

2000 Malicious Packets bombarded were detected and dropped successfully by our system. System accuracy proved to be 100%. Also 1000 legitimate special Interest packets were processed and no packet was dropped.

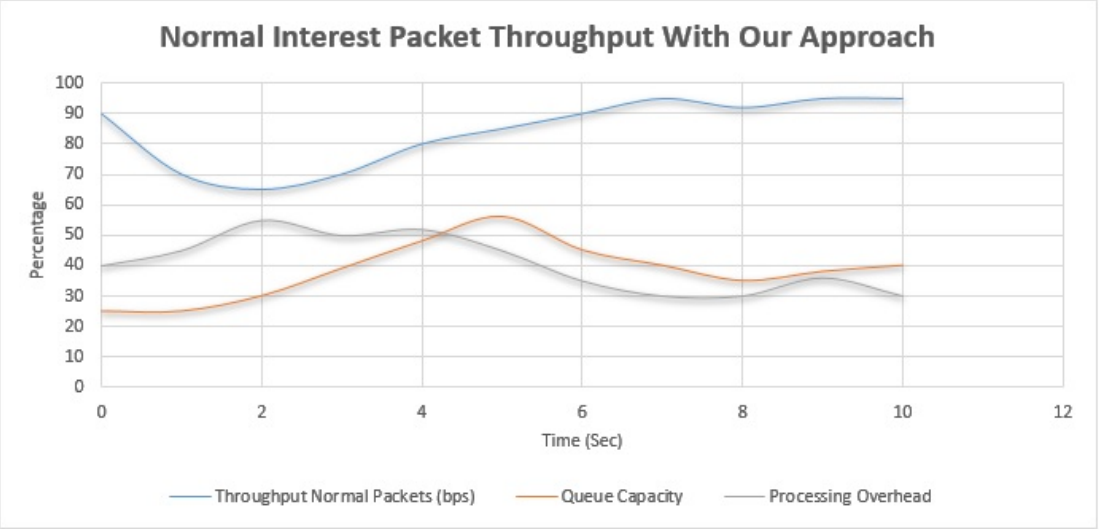

FIGURE 4.13: Throughput Of The Normal Special Interest Packets In Flooding Attack Scenario With Proposed Mitigation Strategy

4.6 Qualitative Comparison

4.6.1 Evaluation And Comparison With Existing Approaches

TABLE 4.3: Qualitative Comparison

Category	**Proposed Approach**	**DiBenedetto et al**	**Gasti et al.**
Malicious Content Detection Rate	Very High	High	High
Legitimate Content Retrieval Rate	Very High	Very Low	N/A
Reporting Packet Size	Lightweight (Hash)	Heavyweight (Complete Bogus Packet)	N/A
Trust Anchor	Yes	Yes	No
Verification Overhead	Very Low	Very High	Very High
Compromised Consumer Detection	Yes	Yes	No
Bogus Report Packet Detection	Yes	Partial	No

In Chapter 2, two major categories are defined for mitigating content poisoning attacks, one is using a Collaborative Approach and the other is Consumer Dependent Approach. Our proposed mechanism belongs to the consumer dependent category, so we'll compare the security and performance aspects of our approach

with the other approaches that fall in the Consumer Dependent category of CPA. DiBenedetto et al. in [27] used an evasion scheme to mitigate a content poisoning attack called Immediate Failover, this scheme reduces the ratings of the next-hop node which brought back the malicious content for future interest packets. This scheme has a flaw, it blocks the legitimate producers as well which are located adjacent to the malicious producer see figure 16. Also, the Report packet generated by the consumer is a heavyweight packet that carries a complete payload along with cryptographic keys. During the evasion process, it verifies the signature on every node which has a great performance impact on the whole NDN system. In figure 16 as an example, if data is produced by Producer 1 under the prefix

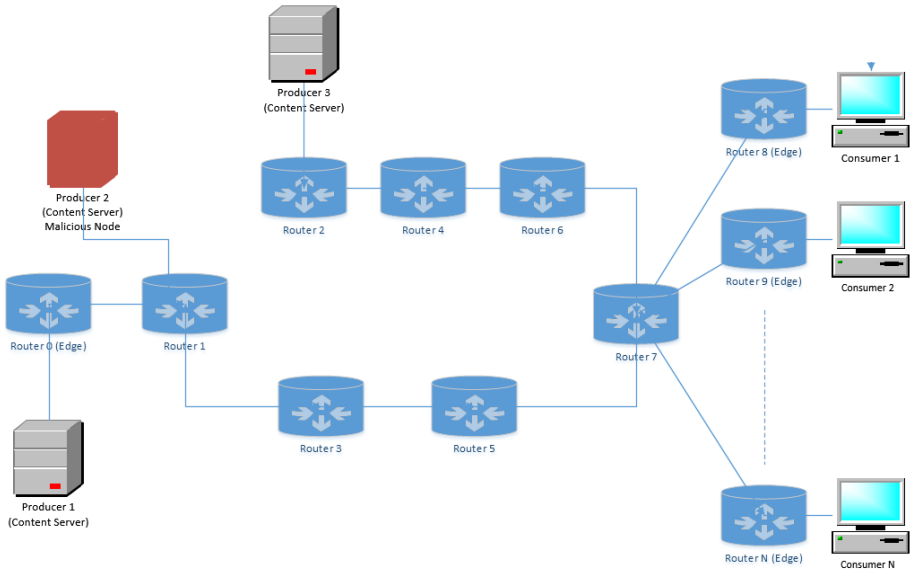

FIGURE 4.14: Immediate Failover Scheme Flaw

of /abc/legitdata and a malicious producer Producer 2 produces the malicious data payload under the same prefix /abc/legitdata. Now when a Consumer e.g. Consumer 1 request for the data with the name prefix /abc/legitdata, it'll follow the shortest path first and will fetch the data from Producer 2. When Consumer 1 verify the data to be bogus it'll generate a Report packet which will contain the complete bogus packet along with the cryptographic keys and send it on the reverse path when this Report packet reaches Router 8 it'll set next-hop node i.e. Router 7 to least preferred node which will also prevent the other consumers to fetch legitimate date from Producer 1. Also to prevent the Report flooding attack,

this scheme uses the Self-ID parameter in the report packet to identify the sender of the report [27]. So it has to maintain and develop a prior trust relationship with the sender and share secrets to identify the sender. But still, if a malicious consumer alters the report packet with invalid data, this scheme cannot handle this situation and this packet will be processed and dropped at the next-hop node. So when a consumer with malicious intent floods the next hop with the bogus Report packet it'll be considered as a flooding attack which is not handled in this scheme.

Similarly, Gasti et al. in [8] and Ghali et al. in [26] also Neighboring Verification Feedback scheme which may involve consumer as well. If a consumer is compromised, this approach will induce some new challenges such as there is no trust relationship between the router and the consumers, so it can generate false feedback that can consume network resources and disrupt the normal NDN operations.

How our approach handles the issues mentioned above: now consider the same example as in figure 16, we can see that there is an on-path content poisoning that occurred at Router 7. When the consumer will generate the special interest packet with the hash of the bogus content in the excluded filter field of the interest packet, it'll use the same channel (in-probe) and when it reaches the Router 7 it'll enable the inline verification of the content on that router and purge the malicious data. So on-path content poisoning will be removed from all of the routers till it fetches the Data packet from the legit content source. It'll reinstate the good content on the intermediate routers and turn off the in-line verification upon the restoration of the content.

Also, the special interest packet is very lightweight as it contains only the hash of the bogus data which gets verified against the data with the PPKD value of the content store. Also, only one verification is required at the router as PPKD in the content store and the special interest packet is compared.

In the end, our scheme also handles the malicious interest packet with exclude filter field which is dropped in case of cache miss as malicious data is not present in the content store, the threshold value against the face gets incremented upon

the cache hit. So the interface from which these excluded interest packets are received gets blocked once it hits the threshold value and this face is added to the delist data structure.

So our proposed approach provides and covers most of the attack surfaces which other schemes failed to achieve. Also as compared to the approach by DiBenedetto et al. in [27], our special interest packet is lightweight and it keeps the mitigation process lightly loaded over the network. Only a PPKD value is added to the NDN Stack.

Chapter 5

Conclusion and Future Directions

5.1 Conclusion

The main contribution of this dissertation is to devise a mechanism that identifies and prevents the compromised consumers from flooding the network with special Interest packets that are generated during the mitigation process of Content Poisoning Attack. The compromised consumers place the hash of an un-poisoned content in the excluded filter field of the special interest packet which causes cache miss at the edge router. Owing to bombardment of these special Interest packets, it'll tremendously increase the processing overhead on the NDN Router. The cost is in terms of Cache-Miss penalty and verification overhead. Also, the queue capacity of the NDN Router gets saturated. Consequently, the legitimate requests from the other consumers get dropped or face a substantial amount of delays. We also observed the damaging effect of multiple malicious consumers flooding the edge router which was also well handled by using proposed technique. Using the mitigation technique mentioned in this dissertation, the Network Service Manager at NDN Edge router can enable a mechanism in which upon hitting a certain threshold value, it blocks that malicious face temporarily from where these special Interest packets are being generated. The delist timeout is also set by the operator depending upon the network situation. We also have made the threshold value

dynamic by adjusting the initial threshold according to cache-miss ratio and queue capacity values.

5.2 Future Directions

An improvement in this technique can be done by incorporating Quality of Service solutions in NDN Routers. Multiple Virtual queues for special Interest packets can be maintained in NDN Routers to handle the flooding of these packets. Different queuing disciplines and algorithms like Adaptive Virtual Queue (AVQ), Credit-Based Fair Queuing, Weighted Fair Queuing, Quick Fair Queueing, and Class-Based Queuing can be tested to augment our approach. Also, traffic shaping and rate control mechanism can be used to hold back the malicious face.

Bibliography

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, ser. CoNEXT '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 1–12. [Online]. Available: https://doi.org/10.1145/1658939.1658941

[2] S. Tarkoma, M. Ain, and K. Visala, "The publish/subscribe internet routing paradigm (psirp): Designing the future internet architecture." 05 2009, pp. 102–111.

[3] X. Hu, J. Gong, G. Cheng, G. Zhang, and C. Fan, "Mitigating content poisoning with name-key based forwarding and multipath forwarding based in-band probe for energy management in smart cities," *IEEE Access*, vol. 6, pp. 39 692–39 704, 2018.

[4] C. Fang, F. R. Yu, T. Huang, J. Liu, and Y. Liu, "A survey of green information-centric networking: Research issues and challenges," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1455–1472, 2015.

[5] A. Detti, A. Caponi, G. Tropea, G. Bianchi, and N. Blefari-Melazzi, "On the interplay among naming, content validity and caching in information centric networks," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 2108–2113.

[6] X. Hu and J. Gong, "Opportunistic on-path caching for named data networking," *IEICE Transactions on Communications*, vol. E97-B, pp. 2360–2367, 11 2014.

[7] Y. An and X. Luo, "An in-network caching scheme based on energy efficiency for content-centric networks," *IEEE Access*, vol. 6, pp. 20 184–20 194, 2018.

[8] P.Gasti, G.Tsudik, E.Uzun, and L.Zhang, "Dos & ddos in named-data networking," *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, 08 2012.

[9] I. Ribeiro, A. Rocha, C. Albuquerque, and F. Guimarães, "Content pollution mitigation for content-centric networking," in *2016 7th International Conference on the Network of the Future (NOF)*, 2016, pp. 1–5.

[10] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "An overview of security support in named data networking," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 62–68, 2018.

[11] N. Kumar, A. Singh, A. Aleem, and S. Srivastava, "Security attacks in named data networking: A review and research directions," *Journal of Computer Science and Technology*, vol. 34, pp. 1319–1350, 11 2019.

[12] J. M. Wein, J. J. Kloninger, M. C. Nottingham, D. R. Karger, and P. A. Lisiecki, "Content delivery network (cdn) content server request handling mechanism with metadata framework support," Jul. 3 2007, uS Patent 7,240,100.

[13] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[14] H. Hassanein and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 1–1, 07 2015.

[15] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 566–600, 2018.

[16] Y. Wang, Z. Qi, K. Lei, B. Liu, and C. Tian, "Preventing "bad" content dispersal in named data networking," in *Proceedings of the ACM Turing 50th Celebration Conference - China*, ser. ACM TUR-C '17. New York, NY, USA: Association for Computing Machinery, 2017. [Online]. Available: https://doi.org/10.1145/3063955.3063993

[17] D. Wu, Z. Xu, B. Chen, and Y. Zhang, "What if routers are malicious? mitigating content poisoning attack in ndn," in *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016, pp. 481–488.

[18] M. Gao, K. Wang, and L. He, "Probabilistic model checking and scheduling implementation of energy router system in energy internet for green cities," *IEEE Transactions on Industrial Informatics*, vol. PP, pp. 1–1, 01 2018.

[19] S. Nam, D. Kim, and I. Yeom, "Content verification in named data networking," in *2015 International Conference on Information Networking (ICOIN)*, 2015, pp. 414–415.

[20] G. Bianchi, A. Detti, A. Caponi, and N. Blefari Melazzi, "Check before storing: What is the performance price of content integrity verification in lru caching?" *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 3, p. 59–67, Jul. 2013. [Online]. Available: https://doi.org/10.1145/2500098.2500106

[21] D. Kim, S. Nam, J. Bi, and I. Yeom, "Efficient content verification in named data networking," in *Proceedings of the 2nd ACM Conference on Information-Centric Networking*, ser. ACM-ICN '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 109–116. [Online]. Available: https://doi.org/10.1145/2810156.2810165

[22] D. Kim, J. Bi, A. Vasilakos, and I. Yeom, "Security of cached content in ndn," *IEEE Transactions on Information Forensics and Security*, vol. PP, pp. 1–1, 07 2017.

[23] S. S. Ullah, I. Ullah, H. Khattak, M. A. Khan, M. Adnan, S. Hussain, N. U. Amin, and M. A. K. Khattak, "A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with internet of things," *IEEE Access*, vol. 8, pp. 98 910–98 928, 2020.

[24] P. Yue, R. Li, and B. Pang, "Register before publishing with smart forwarding, mitigate content poisoning attack in icn," in *2019 IEEE Intl Conf on Parallel Distributed Processing with Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2019, pp. 210–217.

[25] T. G. U. Ghali, Cesar and Ersin, "Needle in a haystack: Mitigating content poisoning in named-data networking," 01 2014.

[26] C. Ghali, G. Tsudik, and E. Uzun, "Network-layer trust in named-data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, 02 2014.

[27] S. DiBenedetto and C. Papadopoulos, "Mitigating poisoned content with forwarding strategy," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2016, pp. 164–169.

[28] T. Nguyen, X. Marchal, G. Doyen, T. Cholez, and R. Cogranne, "Content poisoning in named data networking: Comprehensive characterization of real deployment," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017, pp. 72–80.

[29] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, "Live: Lightweight integrity verification and content access control for named data networking," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 308–320, 2015.

[30] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson, "Measuring isp topologies with rocketfuel," *IEEE/ACM Transactions on Networking*, vol. 12, no. 1, pp. 2–16, 2004.