# Lightweight Integrity Verification in Named Data Networking

Chaitra D B[#1], Dr. Rashmi R Rachh[*2]
*[#1]P.G. Student, [*2]Associate Professor,*
*Computer Science and Engineering, Visvesvaraya Technological University, Belgaum, Karnataka, India*

***Abstract***

*In today's period of Internet, privacy is the major issue. Various methods like encryption, authentication, digital signatures, etc. are used to provide privacy. The algorithms for generation of digital signature and its verification pose a high computational overhead, which directly affects the performance. So, Named Data Networking (NDN) is introduced where the content names are assigned to data packets as the origin and termination points addresses instead of IP addresses. However, a content provider (CP) fails to efficiently control the access to his/her content. Hence, this project aims to implement Lightweight Integrity Verification (LIVE) architecture to address the issues of data pollution and content access control. It involves acceptable computational overhead and enables monitoring content access.*

**Keywords**

*Named Data Networking, Lightweight Integrity Verification, Content Provider.*

## I. INTRODUCTION

The era without tweets, posts, email, blogs, snaps, etc. is very hard to recollect. Many individuals today have grown up having the capacity to do these things. Sometime in the past none of this was possible. What makes this conceivable today is the thing that we call the Internet. The Internet is an overall arrangement of associated systems. Each system comprises of a huge number of PCs, servers, switches, and printers. The systems that make up the Internet might be claimed and kept up by various organizations yet messages and information move over every one of them without respect to proprietorship since they all use the same set of rules for communication [1].

A Network of computers is an arrangement of PCs associated together with the end goal of sharing resources. The most well-known resource shared today among this network is the Internet. Other shared resources can incorporate a printer and other resources. A resource constrained PC is designed in such a way that it can link itself to the network of networks in order to get the required resources. Alternatively, it can be termed as a data network which allows digital telecommunication. Oracle and Sun MicroSystems introduced a concept called Network Computer which is basically a low cost PC that can be used for business networks [1].

The basic methods for establishing connection in a network are: Wired connection and Wireless connection. Wired connection involves connection through physical transmission media like twisted cables, co-axial cables, optical fiber cables, etc. However, based on the kind of network created, a wireless connection can be categorized. In the current era, wireless connection has revolutionized the Internet as it eliminates the usage of cumbersome wired connections. The networks based on wireless connection are Local Area Network, Personal Area Network, Campus Area Network, Wide Area Networks and Metropolitan Area Network. The kind of network created using wireless connection depends on the need of the user in a particular circumstance [2].

In terms of hardware used, a network is composed of number of network elements like hub, router, gateway, repeater, tunnel, switches, various kinds of bridges, etc.

Social Networking is made successful because of Internet which supports global connections anytime, anywhere. . This feature of Internet has made the communication possible in the society in a more easy and effective way. Many sites that enable social networking have risen to support digital telecommunication among the people of various regions of the world easily.

There is no owner for Internet. Turning off the Internet is impossible. Hence there is no centralized control to control the Internet. The network architecture defines how a communication network is designed. It depends on the suite of protocols used by the Internet rather than followed topology, connection method, network elements, etc.

The two major elements of network architecture are Basic Service Set and Extended Service Set. The popular network architecture is IP-based network architecture. In this architecture, the data packets are given a header consisting of origin point and termination point IP addresses. The major factors that decide network architecture are Inter Domain Routing, IP Multicasting, autonomous systems and routers [3].

Named Data Networking, abbreviated as NDN is a new network architecture where the packets are sent by names given based on the content instead of addresses [4]. A user or a device sends a request with a packet of interest with any name of content to NDN. The routers in NDN after receiving this packet forward it to a routing table called forwarding information base, which is based on name prefixes, and they store the request in a table called pending interest table. When this packet arrives at the point where the content resides, it is responded with a packet. The intermediate routers check their PITs and hand over this packet to the requester.

Meanwhile, every intermediate router caches the data packet in its local content store (CS*)* in order to use it to handle future requests with the same content name of the interest packet. Generally, a content object (e.g., a video file) may be split into multiple data packets, where each data packet has the same name prefix but different full packet name [4].

Today's Internet is a scenario of host-centric networking. Content-Centric Networking, in short, CCN is an alternative to it. It supports the distribution of content by making it easily available and hence easily available to the requested users. NDN is an illustration of CCN and is considered as a participant next generation Internet architecture in the future.

## II. LITERATURE SURVEY

***Qi Li et al.*** *[4]* addressed Distributed Denial of Service attack, in short DDoS as the most cumbersome problem today. Here packets from a high number of attacked hosts bombard the victim site by sending a huge number of requests thereby overloading the victim machines. As a consequence, the authorized users are denied to receive the requested service from the victim machine. NDN is introduced to take care of this issue.

Today's Internet is a live scenario of host-centric networking. Content-Centric Networking, abbreviated as CCN is one of its alternatives. ***A. Afanasyev et al.*** [5] proposed an implementation where CCN supports the distribution of content by making it reachable directly. The vital characteristic of NDN is support for content caching in the router which optimizes the consumption of bandwidth and reduces congestion. For popular content, it also provides fast fetching. Unfortunately, this feature is also susceptible to confidentiality of both the consumers and the producers of the content. To address this issue, the consumers and producers should indicate which content is privacy-sensitive in the beginning. Some techniques that provide certain compromises between confidentiality and latency have been proposed.

In a Content–Centric network (CCN), once the content is distributed and exists in multiple copies such as in caches, content replication servers, etc., it is very difficult to monitor the access to that content. Hence a scheme to assign access permissions has been proposed that allows the content provider of the content to handle a request for the content against the access control policies defined at the very first step, without having permission to the requestor credentials. This approach has several advantages: it supports the interoperability between various stakeholders, it also protects user identity. The above proposed system protects user credentials thereby preserves user privacy. The implementation of this scheme shows its feasibility and the strengths of an information-oriented architecture [5].

***Gergely Acs et al.*** [6] have demonstrated an implementation scheme where any intermediate node that handles a content item can protect it using the access control policy incorporated with an indicator without having permission to its definition. Therefore, stakeholders can protect the information items without having to access the definition of a control policy and can achieve successful access control over the sensitive information.

The design of NDN has many pros dealing with security. For instance, each data packet in NDN has a digital signature of an entity. This enables the network modules and users to verify its integrity and authenticity no matter where they obtain the data packet.

Yet, there are a number of important security issues to be addressed by NDN. First, existing algorithms for generation and verification of signatures are heavyweight such that they consume more resources making them impractical to implement. This disables universal verification for the correctness of the content making it extremely hard to achieve for network nodes, especially for content routers of Internet scale. Secondly, the NDN design considered supports caching and accessing of content. Therefore any node of a network which is NDN enabled can store the contents when they are received by them without any permission/approval from Content Providers (CP). Similarly, users can request and access any content that they desire from network caches arbitrarily, which is again not in CP's hands [6].

Conventionally, in application-level services like encryption-based access control or delegation-based services, content caching and access control are performed. Both efficient verification for the correctness of content and permission to access it (including caching) control are attempted to achieve with a single solution in the network layer, by leveraging the obtainable security mechanism in NDN with a fewer changes. Particularly, the proposed design is based on the fact that the available NDN design requires a signature field in every packet to allow checking for data validity [6]. Instinctively, NDN nodes are ready to temporarily store or use a data packet only after its correctness is proved in order to be assured about the meaning of the content so that is not tampered.

Named Data Networking architectures are introduced to optimize different cons of the present Internet architecture. The main concept of these theories is the support for caching content in random network locations. ***Tobias Lauinger et al.*** [7] aimed to create knowledge about privacy attacks in these architectures. Remedies for these attacks are focused to a compromise between performance and privacy.

***Giuseppe Bianchi et al.*** **[**8] put forth a scheme that allows evaluating the performance of caching technique. The core concept of this scheme was the capability to manage traffic efficiently which in turn helps to understand how performance is affected. The vital merit of this method is the capacity to forward only a part of incoming content to the cache which may be either advantageous or useless in affecting the probability of cache hit.

***Andrea Detti et al*****.** [9] discussed the importance of naming the content, storing it temporarily and its validity. In particular, they searched various naming schemes and also a variety of schemes available for digital signatures. In this proposal, the speed of the schemes mentioned above was evaluated. Also, the overhead involved and their impact on performance were taken into account. However, they found that these schemes were comparatively slow and were the main reason for the reduction of performance. The different combinations of signature schemes and naming were identified to be useful after the detailed analysis of the impact of these schemes on the probability of cache hit. Some results explain that, in the circumstance of cache loss occurred because of the overload on the processor of a node intended for security, the performance of a cache hit will not be reduced, and it might even get increased. [9].

***David Goergen et al*****.** [10] provided a thesis on CCN focusing on the requirements for security which helps to design a firewall. In specific, this firewall was capable of filtering the packets based on their signature and name. The initial firewall was designed for CCN using case study comprising the needs for security needs inside CCNx. This scheme was based on the technique where authentication and naming were of greater concern. These were used to offer new facilities similar to a normal IP firewall. Particularly, usage of semantic tools were recommended [10].

## III.METHODOLOGY

Fig.3.1 depicts the sequence diagram of LIVE architecture. It consists of three elements: Sender, Receiver and NDN Router. The sender represents the content provider who registers himself/herself with the router. The router then stores the content sent by the sender in its memory.

The content sent by the sender is fragmented by the sender in the initial stage. Also, the sender assigns MAC to each packet. These packets are sent to the router. When the router receives a request from a user, the action mentioned above is undertaken after the requested file found by browsing.

When the router receives the content from the sender, it verifies the correctness of the packet by checking its signature. If the packet is malicious, it asks the user whether to send the corrupted packet or not. This helps the receiver to get notified about the misleading content. This entire scenario is depicted in fig.3.1 where each of the above actions is represented using dotted arrows.

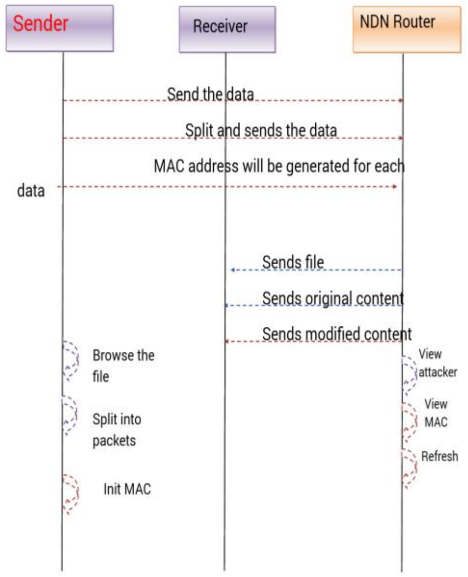


**Fig.3.1: Sequence diagram of LIVE architecture**

### A. *First Level Dataflow*

In the LIVE architecture, the flow of requested file from the source node to the router and finally to the requested receiver node comprise the data flow. This scenario is depicted in fig.3.2.

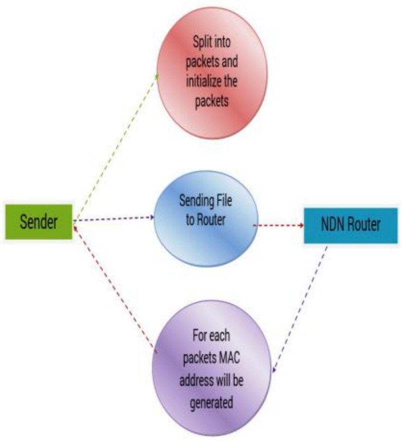

Split into packets and initialize the packets
Sender
Sending File to Router
NDN Router
For each packets MAC address will be generated

**Fig.3.2: Level-0 dataflow diagram**

### B. *Second Level Dataflow*

Fig.3.3 depicts the level-1 dataflow diagram of the LIVE architecture. This step constitutes the dataflow between the router and the receiver. The NDN router sends the packets to the receiver after receiving them from the sender. The receiver, after receiving the packets from the router can check the rightness of the data packets and can discard them if they are malicious and fail to undergo through verification.

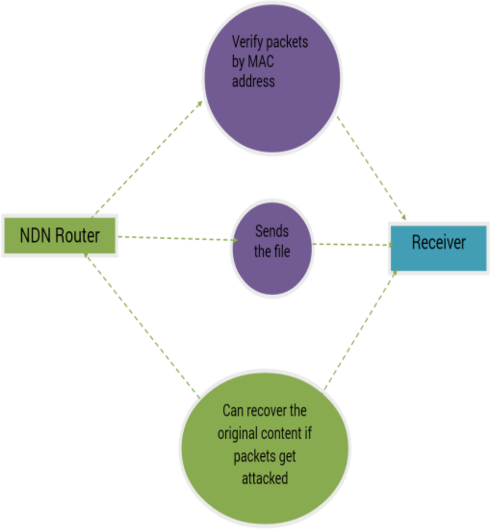

Verify packets by MAC address
NDN Router
Sends the file
Receiver
Can recover the original content if packets get attacked

**Fig.3.3: Level-1 dataflow in LIVE**

### C. *Third Level DFD*

Fig.3.4 depicts level-2 dataflow in the LIVE architecture. This step shows the dataflow between the attacker and the NDN router. The attacker can add useless content into a packet selected randomly. This malicious packet is sent to the router.

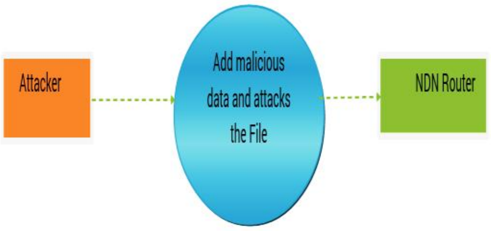


**Fig 3.4: Level-2 dataflow in LIVE**

## IV. IMPLEMENTATION

There are four modules in the implemented LIVE architecture as depicted in fig 3.5. They are Sender/Service Provider, NDN Router, Receiver and Attacker.

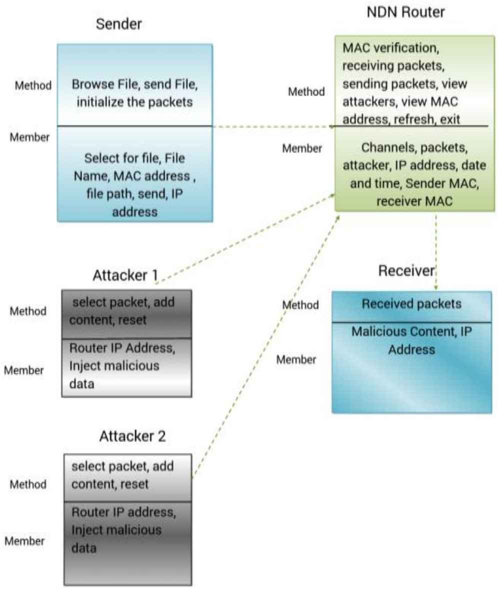

Sender
Method
Browse File, send File, initialize the packets
Member
Select for file, File Name, MAC address , file path, send, IP address
NDN Router
Method
MAC verification, receiving packets, sending packets, view attackers, view MAC address, refresh, exit
Member
Channels, packets, attacker, IP address, date and time, Sender MAC, receiver MAC
Attacker 1
Method
select packet, add content, reset
Member
Router IP Address, Inject malicious data
Receiver
Method
Received packets
Member
Malicious Content, IP Address
Attacker 2
Method
select packet, add content, reset
Member
Router IP address, Inject malicious data

**Fig 3.5: Overview of LIVE architecture**

Once the sender receives a request for data (file) as an interest packet, it encrypts the selected file using Advanced Encryption Standard algorithm. Then, this encrypted file is broken into smaller packets before sending it to the router. The NDN Router receives the packets and finds whether the packets have been modified or not using F-distance measure and Naive Bayes Classifier.

A receiver may be a public node or a private node. If the requested file is sensitive, then the private node (receiver) has to enter the file access key along with his/her IP address. File access key is not required if the requested content is not confidential and if the node is public. An attacker may attack any desired packet by injecting malicious data into it. However, the sender notifies the receiver about the attack occurred to the respected packet with a warning message. This warning message asks for the permission of the receiver in order to determine whether to receive the malicious data packet or not. The receiver can choose whether to receive the corrupted data packet or not.

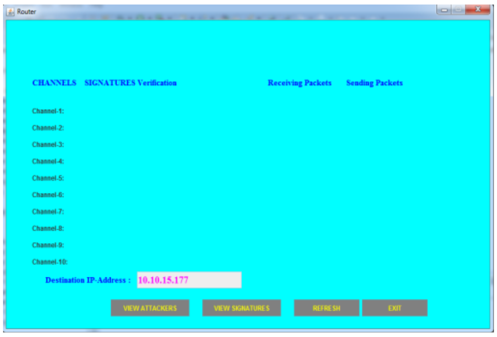
Message Authentication Code (MAC) is generated by the Message Digest using SHA-1 algorithm. A unique File Access Key is generated by the KeyPairGenerator using RSA algorithm. MAC of each received packets are compared with the MAC of each sent packets. The F-Distance algorithm and Naïve Bayes Classifier is implemented. The NDN Router is capable of recording the source and destination addresses using

Multicast Authentication based on symmetric key signature mechanism.

In this paper, the project of implementation of LIVE architecture is explained. It aims at the minimization of the computational overhead involved in generation of signatures and their verification. Also, it addresses the issue of monitoring the content access. LIVE adopts standard hash functions such as SHA-1, F-distance algorithm and Naive Bayes Classifier to generate and verify signatures. These require fewer resources when compared with the conventional algorithms required to do the same.

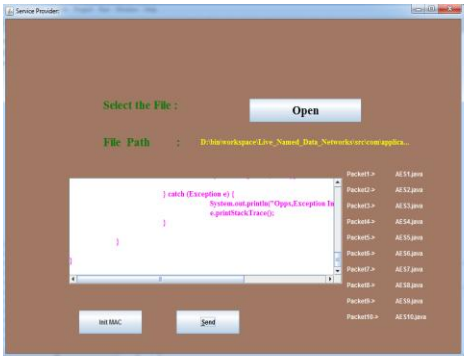
## V. RESULTS ANALYSIS

Fig.3.6 show the results of LIVE architecture. These figures depict the router module, sender module, receiver module and attacker module respectively.



Destination IP-Address : 10.10.15.177

(a)



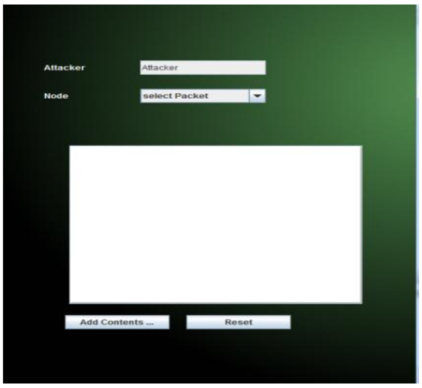
File Path : D:\bin\workspace\Live_Named_Data_Networks\src\com\applica...

```
                } catch (Exception e) {
                        System.out.println("Opps,Exception In
                        e.printStackTrace();
                }
        }
}
```

| | |
|---|---|
| Packet1-> | AES1.java |
| Packet2-> | AES2.java |
| Packet3-> | AES3.java |
| Packet4-> | AES4.java |
| Packet5-> | AES5.java |
| Packet6-> | AES6.java |
| Packet7-> | AES7.java |
| Packet8-> | AES8.java |
| Packet9-> | AES9.java |
| Packet10-> | AES10.java |

(b)

(c)



Attacker: Attacker

Node: select Packet

(d)

**Fig 3.6: (a) NDN Router module (b) Sender module (c) Receiver module (d) Attacker module.**

## VI. CONCLUSION

LIVE, lightweight integrity verification mechanism for Named Data Networking has been implemented. This enables efficient authenticity verification and content access control and hence supports to achieve content integrity. NDN contributes to addressing of Distributed Denial of Service attacks efficiently. This architecture is a candidate for next generation Internet architectures. Further refinements in encryption techniques and hashing algorithms can be undertaken in the future to make NDN a leading architecture for Internet.

## REFERENCES

[1] http://www.britannica.com

[2] http://www.techopedia.com

[3] http://www.ukessays.com

[4] "LIVE: Lightweight Integrity Verification and Content Access Control for Named Data Networking" by Qi Li, Member, IEEE, Xinwen Zhang, Member, IEEE, Qingji Zheng, Ravi Sandhu, Fellow, IEEE, and Xiaoming Fu, Senior Member, IEEE

[5] A. Afanasyev, P. Mahadevany, I. Moiseenko, E. Uzuny, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in Proc. IFIP Netw. Conf, May 2013, pp. 1–9.

[6] G. Acs, M. Conti, P. Gasti, C. Ghali, and G. Tsudik, "Cache privacy in named-data networking," in Proc. IEEE 33rd ICDCS,Jul. 2013, pp. 41–51.

[7] T. Lauinger, N. Laoutaris, P. Rodriguez, T. Strufe, E. Biersack, and E. Kirda, "Privacy risks in named data networking: What is the cost of performance?" ACM SIGCOMM Comput. Commun. Rev., vol. 42, no. 5, pp. 54–57, Sep. 2012.

[8] 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?" ACM SIGCOMM Comput. Commun. Rev., vol. 43, no. 3, pp. 59–67, 2013.

[9] 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 Proc. IEEE GLOBECOM, Dec. 2013, pp. 2108–2113.

[10] D. Goergen, T. Cholez, J. Francois, and T. Engel, "A semantic firewall for content-centric networking," in Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM), May 2013, pp. 478–484.