Indian Journal of Science and Technology, *Vol 10(12), 10.17485/ijst/2017/v10i12/101108, March 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Confidential Data Access Control in Named Data Networking

N. Anusha* and V. Hemanathan

Sathyabama University, Rajiv Gandhi Salai, Jeppiaar Nagar, Chennai – 600119, Tamil Nadu, India;
anusha.nallapareddy@gmail.com, heman.nathan@gmail.com

Abstract

Objective: Named Data Networking (NDN) is an emerging model to replace the existing IP networks which focuses mainly on Content or the data. The notion of the work is to provide solution to the Interest Flooding Attack (IFA) .Content access is also restricted and transferred only to the permitted user by using NDN specific Authentication, Authorization, and Accounting (AAA) server. **Methods/Statistical Analysis:** Major data transferred over the IP network is Contents. This gave way for a new Content Centric Network (CCN) design known as NDN. Not all the contents in the network should be accessible by all users. There are some confidential data which should be accessible only by the specific users. This Confidential Data Access Control model solves this issue by introducing few changes in the existing packet structures and by adding interest validation algorithm in Content Provider (CP) and at the NDN routers. This model also introduces NDN specific AAA Server which does authentication and authorization to check the access restriction to the requested content by the users. NDN AAA server is associated with all the CPs. **Findings:** The system when implemented showed better results with improved performance in overall network by avoiding Flooding attack and securing content packets. **Application/ Improvement:** Hence, the proposed model of NDN is designed to improve security and also to provide access restrictions for specified users to access the content. This is an implementation paper of the previously published algorithms.

Keywords: Access Control, Authentication, Authorization, and Accounting (AAA), Confidential Data Access Control, Interesting Flooding Attack, Named Data Networks

1. Introduction

Named data Networking (NDN) is a newly proposed design which is meant for data access through the network[1]. NDN is designed to have a faster data access and security when compared to the traditional IP architecture[1]. But the data which is available in the network is accessible by all the users and there is no access restriction applied to the contents available. There is no mechanism to safeguard the confidential data access over the network. The NDN model performs data integrity and authenticity using signatures; it can reveal the possible information about the data which is requested but not their identity. The proposed system is highly aimed to provide data confidentiality. ICN is naturally aimed to prevent host-oriented attack as it follows content based communication, solutions for denial-of-service attack is worth to be discussed[1]. This is an implementation and performance analysis of the previous paper "Role Based Control Access Control in NDN[1].

**Author for correspondence*

2. Related Work

Proposed method uses two kinds of commonly used protocols i.e., IMAP (Internet Message Access Protocol) and SMTP (Simple Mail Transfer Protocol) in order transfer mails over NDN. The PUSH protocol which uses the concept of long lived interest[2] is used for the communication between the agent and the server. Information-Centric networking paradigm is used which targeted to switch the IP based Internet to a content information driven model.[3] Proposed a LIVE (Lightweight Integrity Verification) architecture which verifies the content signatures globally in NDN using the verification algorithms[4] but also with the light weight signature generation. Initially, the NDN's first Community Meeting was held at UCLA in Los Angeles, California on September 4-5, 2014[5] and same written given briefly . The current capabilities and potentialities for the NDN software platform to serve the scientific research community were discussed[6].

Proposed a project in NDN.[7] Discussed about Future Internet Architectures (FIA), Distributed Denial of Service (DDoS) attacks on NDN. An efficient cryptography fashion is followed to prevent subscription privacy and to provide publication confidentiality in a CBPS system[9]. NDN architectures have been proposed[10]. Implemented a prototype CCN (Content-Centric Networking) network stack released as open source[11]. Study on content-oriented network architectures comparing with traditional networks[12]. Discussed about the NDN Packet Format Specification[13]. Discussed about the NDN Forwarding Daemon (NFD)[14]. Discussed about the NS-3 based NDN simulator documentation[15]. Discussed about the Content Centric Networking (CCNx) Project[16].

3. Sequence Diagram of the Flow

The sequence of steps that happens in the secure content access control system for validating the interest packet and to restrict the content access to the users is shown in Figure 1. When the user sends an interest packet, NDN router receives it and checks the Content Store (CS), whether it has got it in CS or not. If it is found then it checks the access table whether it has got allow or deny access. If allow then it forwards the content packets from CS. If the result is denied, then the interest packet is dropped. Then it is not possible to map the content packet in CS of NDN router and the entry not found in access table as well. Further, it adds the entry in Pending Validation Table (PVT) and forwards the request which is waiting for validation to the Content Provider (CP). The CP then forwards it to the NDN AAA server to authenticate the user with enroll ID and to check the access level. If authenticated and allow access then the content packets are generated and sent to the NDN routers. The NDN routers then update its access table with the validation response and forward the content packets to the corresponding user.

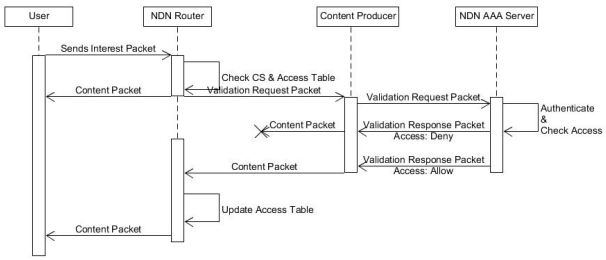

Figure 1. Sequence diagram of the packet flow.

4. Concept Design

4.1 NDN AAA Server

This section explains about the customized AAA server with limited functionalities for NDN. This AAA server receives the validation request packets from the content producer and validates the user with database and checks for content access restriction as well. In this system, a simple AAA server with basic authentication and authorization is performed with TCP connection from Content producer.

The architecture of the NDN AAA server is shown in Figure 2. Server responds to the client request which is present in the content producer. It triggers the validation request for the new users who requests content packets. User information is stored in the MySql database with content access level corresponding to the respective users.

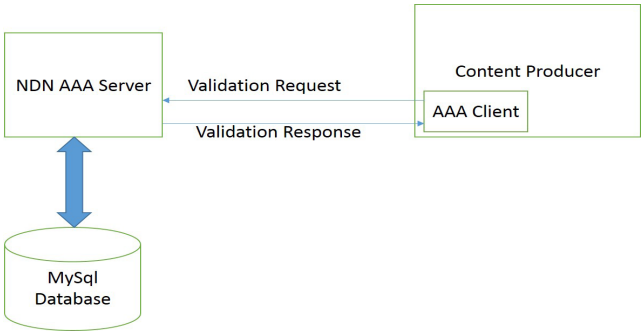

Figure 2. NDN AAA server architecture.

4.1.1 Validation Request Packet

Validation request packet is generated by the NDN routers or by CPs and forwarded to NDN AAA for content access only after the user is validated. It contains the packet type, request content name and the enroll id of the user.

4.1.2 Validation Response Packet

Validation response packet format is generated by NDN AAA server and sends it to the content producer. The validation request whether to allow or deny is placed here. It contains fields such as packet type, success/failure message, and content name and enrolls Id.

4.2 Validation Packet Sequence

Figure 1 shows the sequence of packets flow in the system. Whenever a user requests for a data, it generates an interest packet and forwards it to the next router by inserting the user enroll ID. A check is made at each and every NDN router in the CS for the requested content name. If content is found then it checks the access for the enroll ID in the Access Table. If there is an entry exists in the table with allow access then the content packets are sent. If the enroll ID is in deniable access list then it sends "Access Denied" message to the user. Even if the requested content exists in the CS, router doesn't forward the content since access restriction was applied by the CP.

If no entry exists in the Access table for the request and the enroll ID then it generates a validation request packet and forwards it to CP or to the next nearest router and adds an entry with content name and enroll ID in PVT. This helps in reducing the number of interest packets generated and flooded in to the network. Since PVT doesn't allow duplicates to be added, interest packets with same enroll id and content name gets filtered. Validation request packets are forwarded to another router next to it or to the CP based on the Forwarding Information Base (FIB). AAA server does actual authentication on behalf of CP and responds with validation response packet to say success or failure as a result. The result is then forwarded to the NDN router to update its access table with content name, enroll Id and the level of access. PVT entry is removed and sends the content packets to the user.

If CS doesn't have the requested content, then the Interest Packet is forwarded to the CP or to the next nearest router. Finally, it reaches the CP and authentication is done by AAA server. As per the access level from AAA, the CP sends the content packets to the user or restricts the access to it.

4.2.1 Interest Packet

Interest Packet is generated by the Content Requestor. It will have the enroll ID, in addition to the existing fields in the packet.

Access table maintains the list of content name with its access restrictions as allowable and deniable enroll ID's only if contents exists in the CS. The sample access table and the entries for access control are shown in Table 1. AAA server generates the enroll Id's and is used by the CP for Authentication and Authorization. A generalized ID - 0000 says that the content can be accessed by everyone without any restrictions on it. The generated enroll ID's gives information about the CP and AAA sever.

Table 1. NDN router access table

Content Name	Allowable Id	Deniable ID
/ndn/edu/sbu/me/ME_schedule.pdf	10456, 1326	1563
/ndn/org/caida/demo.mp4	25780	1563, 1326
/ndn/edu/colostate/techmeet_video.mpeg	5312	25780
/ndn/edu/arizona/network_lecture.ppt	0000	-
/ndn/com/orange/new_tariff.xlsx	0000	-
/ndn/edu/gce/cse/dot-letter-cse.docx	1563	10456, 1326

4.3 Pending Validation Table

Pending validation Table (PVT) maintains the list of entries for the validation requests packets sent and the packets for which the response is expected from the CP

or the AAA server. The sample PVT is shown in Table 2. Entry for Validation request packets are removed from PVT only if the validation response packets are received for the enroll ID and the content name.

Table 2. Pending validation table

Content Name	ID
/ndn/edu/sbu/me/ME_schedule.pdf	1563, 1326
/ndn/org/caida/demo.mp4	25780
/ndn/edu/colostate/techmeet_video.mpeg	25780
/ndn/edu/arizona/highspeed_data_lecture.ppt	2914
/ndn/com/orange/new_tariff.xlsx	2143

LIST OF ABBREVIATIONS

NDN	Named Data Networking
PIT	Pending Interest Table
PVT	Pending Validation Table
CCN	Content Centric Network
CCND	Content Centric Network Daemon
NFD	Network Forwarding Daemon
AAA	Authentication Authorization and Authorization
FIB	Forwarding Information Base
IFA	Interest Flooding Attack
LIVE	Light Weight Integrity Verification and Content Access Control
CP	Content Provider
ICN	Information Centric Network
CS	Content Store
NLSR	NDN Link State Routing
TLS	Transport Layer Security

5. Results and Discussions

In this section, results of the proposed technique are discussed.

5.1 Output

The performance of the system is measured based on the number of intermediate NDN routers that exists in the network. Also, there is one Content Producer who generates the content packets and two consumers in the NDN network topology. Out of two, one is a valid consumer and the other is an Interest Flooding Attacker, who generates some dummy interest packets. All the links in the network topology are configured at 1Mbps data rate and the frequency of interest packets is fixed at 10 per second. The actual data is collected with all these precondition values.

5.1.1 *Zero Intermediate NDN Routers in Topology*

The NDN topology with no intermediate routers is shown in Figure 3. The producers and the consumers are connected to the common NDN router. It also shows the CS information in all the nodes in the topology.

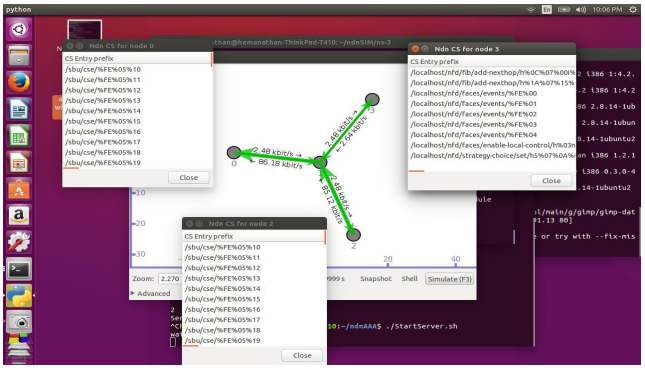

Figure 3. Zero intermediate routers with CS.

5.1.2 *Four Intermediate Routers in Topology*

The topology with four intermediate routers in the network and a common router that connects directly to the consumers is shown in Figure 4.

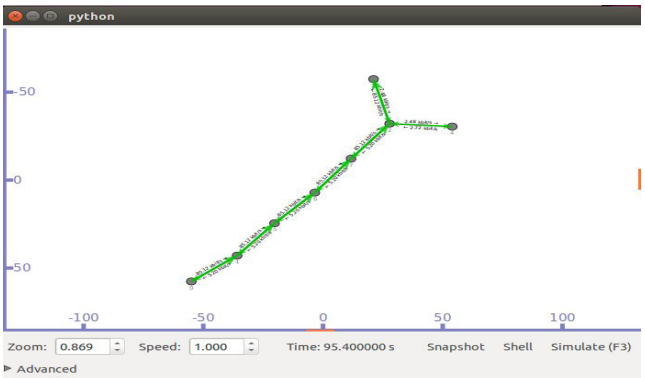

Figure 4. Four intermediate routers in topology.

5.1.3 NDN AAA Server

The NDN AAA server response while authenticating the users is shown in Figure 5. Authentication is performed whenever there is a validation request packet. It authenticates and replies back with validation response packet.

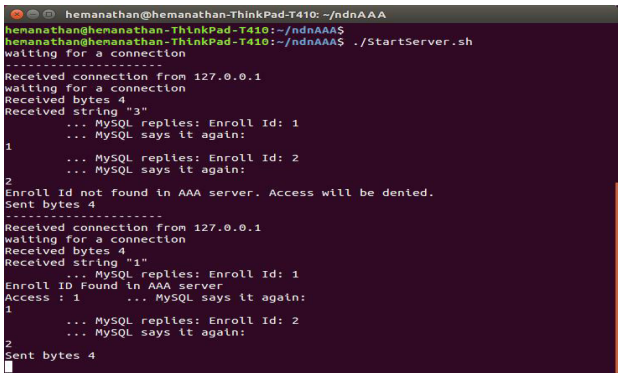

Figure 5. NDN AAA server.

5.2 Performance Analysis

The performance of the previously designed system and proposed system were compared based on the performance measurement criterion such as CPU utilization and Memory utilization. Since, the performance of routers, producers and consumers can't be measured in simulation, it is considered to measure the performance of the process. The performance data is captured on 2.6GHz processor with 2GB of Ram.

5.2.1 CPU Performance

The CPU utilization percent with access control and without access control is shown in Figure 6. It is seen that as there is an increase in the number of intermediate nodes, though there is an IFA, still the performance of the system is good.

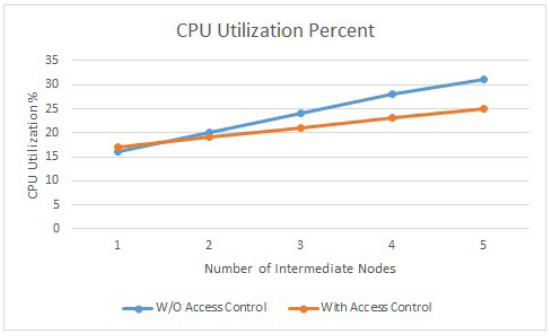

Figure 6. CPU utilization percent results.

5.2.2 Memory Performance

Memory utilization percentage is compared between the existing system and proposed system is shown in Figure 7. From the graph, it is clearly understands that performance of proposed system is higher than performance of existing system. Here, performance comparison is based on the memory utilization of the simulation process.

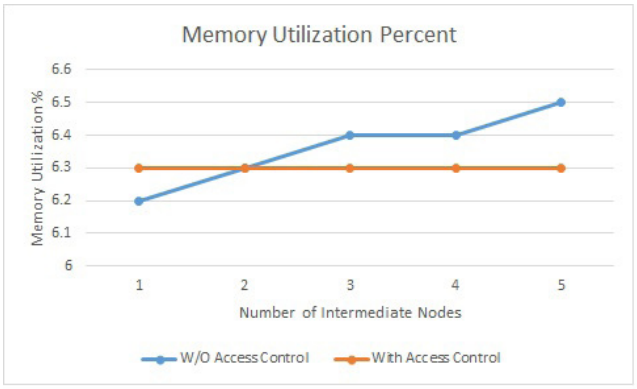

Figure 7. Memory utilization percent results.

6. Conclusion and Future Enhancements

This new model of NDN achieves greater security and content access restrictions based on the user. One of the common network attacks, IFA in NDN is prevented by this model. Improvement in the performance of the CP gains a pace in serving other users efficiently. This improves the performance of the whole network. Except the NDN router which is connected directly to the IFA attacker, all other nodes performance is good. Also, even if IFA tries to flood the network with invalid user id or the one with deniable id, this is identified and control in the entry level itself.

In future, user enrollment process can be improved in CP's AAA server. NDN AAA server can be further enhanced to support TLS based authentication mechanism. Also it can be used to simulate it for many other such connected setups to increase the topology.

7. References

1. Hemanathan V, Anusha N. Role based content access control in NDN. Journal of Innovative Technology and Education. 2015 Sep; 2(1):65–73. Crossref
2. Vetriselvi V, Sugadev C, Manimurugesan P, Vignesh NT, Rani P. E-mail application on named data networking using long lived interest. Indian Journal of Science and Technology. 2016 Feb; 9(8):1–7.
3. Vasilakos AV, Li Z, Simon G, You W. Information centric network: research challenges and opportunities. Journal of Network and Computer Applications. 2015 Jun; 52:1–10. Crossref
4. Li Q, Zhang X, Zheng Q, Sandhu R, Fu X. LIVE: lightweight integrity verification and content access control for named data networking. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Information Forensics and Security. 2015 Feb; 10(2):308–19. Crossref
5. Claffy K, Polterock J, Afanasyev A, Burke J, Zhang L. The first Named Data Networking Community meeting (NDNcomm) [Internet]. 2015 [updated 2016 Nov 17; cited 2015 Apr]. Available from: Crossref
6. NDN Community meeting (NDNcomm): architecture, applications, and collaboration [Internet]. 2014 [updated 2015 Oct 19; cited 2014 Sep 4–5]. Available from: Crossref
7. Named data networking consortium [Internet]. 2015 [cited 2015 Feb 6]. Available from: Crossref
8. Compagno A, Conti M, Gasti P, Tsudikz G.NDN Interest flooding attack and countermeasures. In the Proceedings of the IFIP Network Conference, USA. 2013. p.1–9.
9. Nabeel M, Shang N, Bertino E. Efficient privacy preserving content based publish subscribe systems. Proceedings of the 17th Association for Computing Machinery (ACM) Symposium on Access Control Models and Technologies (SACMAT), USA. 2012 Jun 20–22. p.133–44. Crossref
10. Lauinger T, Laoutaris N, Rodriguez P, Strufe T, Biersack E, Kirda E. Privacy risks in named data networking: What is the cost of performance? Association for Computing Machinery (ACM) SIGCOMM Computer Communication Review. 2012 Oct; 42(5):54–7. Crossref
11. Jacobson V, Smetters KD, Thornton DJ, Plass M, Briggs N, Braynard R. Communications of the Association for Computing Machinery (ACM). 2012 Jan; 55(1):117–124. Crossref
12. Arianfar S, Koponen T, Raghavan B, Shenker S. On preserving privacy in content-oriented networks. In the Proceedings of the Association for Computing Machinery (ACM) SIGCOMM workshop on Information-Centric Networking (ICN), Canada. 2011 Aug 19. p. 19–24. Crossref
13. NDN Packet Format Specification 0.2-2 documentation [Internet]. 2014 [cited 2014 Aug 5]. Available from: Crossref
14. NFD - Named data Networking Forwarding Daemon 0.5.1-58-g77911cc documentation [Internet]. 2014 [cited 2014 Aug 20]. Available from: Crossref
15. ndnSIM documentation [Internet]. 2014 [cited 2014 Sep 13]. Available from: Crossref
16. Cicn [Internet]. 2015 [cited 2015 Jan 19]. Available from: Crossref