Role Based Content Access Control in NDN

V. Hemanathan
Department of Computer Science & Engineering
Sathyabama University, Chennai
Tamil Nadu, India

N. Anusha
Department of Computer Science and Engineering
Sathyabama University, Chennai, India

Copyright © 2015 V. Hemanathan and N. Anusha. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Named Data Networking (NDN) is a proposed content-centric design for the future internet architecture, in which IP addresses are replaced with application name or the content. The content plays a major role in routing the request and response. The content is accessible by all the users in the network whoever sends an Interest Packet to the content provider and it is not restricted.

This Role Based Content Access Control mechanism will provide the contents specific to user based on the role to which it was assigned. Each and every user’s will be authenticated with our new AAA server specifically designed for NDN and will be validated against the access control policy. Only if a user has access to the content then the Content Packets will be sent or else access will be denied. In this method, when Content Provider receives Interest Packet from the user, it will be forwarded to AAA server and based on the response, the decision is made. In addition to that, NDN routers will also have an access table which will maintain the content name and the allowable & deniable enroll ID’s. Based on the access table, it allows or denies the access to content packet or to the content provider. If there is no entry in the access table for the enroll ID, then it adds an entry into Pending Validation Table and sends validation request to Content Provider (CP) which will validate with AAA server and reply back with allow or denial message. This avoids Interest Flooding Attack in NDN network and reduces computational load in the Content Provider.

Keywords: Interesting Flooding Attack, Role based Content Access Control, AAA, and Named Data Networks
1. Introduction

Named data Networking (NDN) is a new content-centric design for data access over the network. NDN design has more advantages than the existing IP architecture in terms of faster data access and security. Though it has got more advantages, it still lacks privacy in the content which is delivered to the end user. The NDN model naturally supports data integrity and authenticity with signatures, but names in Interests can reveal information about requested data, albeit not the identity of the requestor [4]. The privacy issue is solved here in our proposed design. ICN is intrinsically immune to host-oriented attack because of content based communication, solutions for denial-of-service attack is worth to be addressed [4].

2. Background

a. NDN Basics

NDN (Named Data Networking) is a new buzzword which is going in around the world for its merits in replacing the existing IP architecture. Content is the mostly utilized entity all over the world via Internet. Why not the network be, the content-oriented when it is the most widely accessed entity and that gave birth to the new architecture named NDN. It is completely based on the content which is available in different servers.

NDN is a new network architecture that delivers packets by content names but not packet addresses [2]. A User who is in need of data sends an interest packet to the content provider. The interest packet first reaches the NDN router which checks its Content Store (CS) for the content. If it exists in CS then it forwards the content packet to the user. If the content is not available in CS then it checks the Pending Interest Table (PIT) and Forwarding Information Base (FIB). NFD (Network Forwarding Daemon) is a network forwarder that implements and evolves together with the Named Data Networking (NDN) protocol [5]. NFD runs in all NDN routers which constructs its FIB with NLSR (NDN Link State Routing Protocol). If there is an entry in PIT for the same content then it just forwards to corresponding interface, if it is not then adds an entry in PIT and forwards the interest packet. The same way it passes through the number of NDN routers and reaches the content provider. Once the interest packet reaches the content provider, it then generates the content packet and the signature and sends it to the end-user. The signature is generated for integrity verification i.e. to trust the origin of the content and not from the fake data provider. The NDN routers when it receives the data packets, it does an Integrity check to confirm that it was originated from the valid content provider. It then adds it into Content Store (CS) and removes the entry from PIT and forwards it to the user.
b. Issues

Open challenges in NDN are the Security and Privacy. There are few Security issues in NDN such as open access to available content and the interest flooding attack. We provide solution for these two issues in our new model.

Open Content Access

Content provider provides content to all the users irrespective of who the user is. There is no restriction on the content such as “who can access what kind of data”. There are some sensitive or confidential which cannot be made accessible for all users. This kind of data has to be controlled in the way such that only the authorized users can access the content.

Interest Flooding Attack

Interest packets are flooded in the network to reduce the bandwidth of the network thereby they create the slowness of network or choke the network. This makes other users not access the content in the network. This interest flooding attack also solved here in this new model.

3. Concept Overview

Our new model helps in controlling the content access to the user and the Interest flooding attack. The changes proposed in the existing system are a new field addition in Interest packet, two new packet types and new tables in NDN router for access information.

- Interest Packet includes one more field to have the user enroll ID.
- New packet types - Validation Request Packet and Validation Response Packet.
- New tables in NDN routers which maintain additional information for access control and validation request.

User would send an interest packet with enroll ID which he has got it from corresponding Content Provider. The NDN router’s receives the interest packet and checks the content name, if it exists in Content Store. If it exists then checks for the access whether the enroll ID has got allow access or deny access. Based on that, decision is made whether to send or not to send. If there is no information about access details then it sends a validation request to Content Provider for authentication and authorization and then it sends the content packet if got access for it.

4. Concept Design

This section explains our proposed model in detail with all the data structures to be implemented and the pictorial representation for all the changes. Fig.4 is the proposed model for Content access control.
A. Packet types

**Interest packet**
Fig.1 shows the Interest packet structure. It contains the existing fields for the Interest packet and in-addition to it, the enroll ID which will be present.

![Fig.1. Interest packet Format](image1)

![Fig.2. Validation Request Format](image2)

![Fig.3. Validation Response Format](image3)

**ii. Validation request packet**
Fig.2 shows the sample validation request packet which will be generated by the NDN routers to validate the user for content access.

**iii. Validation response packet**
Fig.3 shows the validation response packet format. It contains the response for the validation request whether to allow or deny.

B. Access Table
Access table contains the content name which is available in the Content Store (CS) and the allowable and deniable enroll ID’s. Table 1.1 shows the sample access table and the entries for access control. The enroll ID’s are generated by the AAA server which the Content Provider uses for Authentication and Authorization. A generalized ID - /ndn/0000 says that the content is access globally and there is no access restriction to it. The enroll ID’s are generated based on the content provider’s name prefix which helps in identifying the AAA server appropriately.

<table>
<thead>
<tr>
<th>Content Name</th>
<th>Allowable Id</th>
<th>Deniable ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ndn/edu/sbu/me/calendar.pdf</td>
<td>/edu/sbu/10456,</td>
<td>/gce/cse/1563</td>
</tr>
<tr>
<td></td>
<td>edu/sbu/1326</td>
<td>/gce/cse/1563,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/edu/sbu/1326</td>
</tr>
<tr>
<td>/ndn/org/caida/demo.mp4</td>
<td>/org/caida/25780</td>
<td>/edu/sbu/1326</td>
</tr>
<tr>
<td>/ndn/edu/colostate/techmeet_video.mpeg</td>
<td>/edu/colostate/5312</td>
<td>/org/caida/25780</td>
</tr>
<tr>
<td>/ndn/edu/arizona/network_lecture.ppt</td>
<td>/ndn/0000</td>
<td>-</td>
</tr>
<tr>
<td>/ndn/com/orange/new_tariff.xlsx</td>
<td>/ndn/0000</td>
<td>-</td>
</tr>
<tr>
<td>/ndn/edu/gce/cse/dot-letter.dcox</td>
<td>/gce/cse/1563</td>
<td>/edu/sbu/10456,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/edu/sbu/1326</td>
</tr>
</tbody>
</table>
C. Pending Validation Table

Pending validation Table (PVT) contains the entries for the validation requests sent and awaiting for the response from the Content Provider or the AAA server. Table 1.2 shows the sample Pending Validation Table. When NDN router receives the validation response packet for the specific enroll ID and the content name, it then removes the entry from the PVT.

Table 1.2 Pending Validation Table

<table>
<thead>
<tr>
<th>Content Name</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ndn/edu/sbu/me/calendar.pdf</td>
<td>/gce/cse/1563,</td>
</tr>
<tr>
<td></td>
<td>/edu/sbu/1326</td>
</tr>
<tr>
<td>/ndn/org/caida/demo.mp4</td>
<td>/org/caida/25780</td>
</tr>
<tr>
<td>/ndn/edu/colorstate/tech</td>
<td>/org/caida/25780</td>
</tr>
<tr>
<td>meet_video.mpeg</td>
<td></td>
</tr>
<tr>
<td>/ndn/edu/arizona/network</td>
<td>/edu/annauniv/2914</td>
</tr>
<tr>
<td>lecture.ppt</td>
<td></td>
</tr>
<tr>
<td>/ndn/com/orange/new_tariff.xlsx</td>
<td>/com/airtel/2143</td>
</tr>
</tbody>
</table>

D. Interest validation Algorithm

Interest validation is done in both NDN routers and in the Content Provider. Algorithm1 explains the Interest packet validation in NDN router and Algorithm2 explains the validation in Content Provider side.

Fig.4. Proposed design for Role based Content Access Control
Input: Interest Packet (IntPacket)

if (IntPacket.ContentName exists in ContentStore) then
   EnrollID := IntPacket.EnrollID;
   if(enrollID exists in AccessTable) then
      //Check the access level for enrollID in AccessTable
      accessAllowed = getAccessLevel(AccessTable, enrollID);
      if(accessAllowed == true) then
         Fetch the contentPacket from contentStore;
         send the contentPacket to contentRequestor;
      else
         Drop the interestPacket;
         Send Denial message;
      end if
   else
      //Check PendingValidationTable
      if(contentName and enrollId exists in PVT) then
         drop interestPacket;
      else
         insert contentName, enrollID in PVT;
         Frame ValidationPacket;
         send validationPacket to contentProvider;
      end if
   end if
else
   //Check PendingValidationTable
   if(contentName and enrollId exists in PVT) then
      drop interestPacket;
   else
      insert contentName, enrollID in PVT;
      Frame ValidationPacket;
      send validationPacket to contentProvider;
   end if
   if(validationResponsePacket == true) then
      remove contentName, enrollID in PVT;
      Update the entry in AccessTable;
      send contentPacket to ContentRequestor;
   end if
end if

E. Validation Procedure

Fig. 4 shows our proposed model for content access control. When user sends an interest packet to content provider, it is first sent to intermediate routers by inserting their enroll ID in the packet. NDN router checks the Content Store for the requested content name. If found then it does access validation by checking the enroll ID in the Access Table. If an entry exists in the table to allow then it allows access. If it has “deny” access then it sends the denial message to the user. Though the requested content exists in the content store, router doesn’t forward the content due to the access restriction which was applied by the content provider.

If there is no entry in the Access table then it creates a validation request packet and sends it to the content provider or to the nearest router. It also adds an entry in PVT (Pending Validation Table) with content name and enroll ID. This helps in reducing the interest flooding in to the network. It also filters the interest packets from the same enroll id for the same content name. If a router receives the validation request packet, it just forwards to another router or to the Content Provider based on the FIB. When the validation request reaches the Content Provider,
it forwards to the AAA server which does actual authentication. The Server responds back with validation response packet saying the success or failure. It then forwards it to the NDN router, which updates its access table with content name; enroll Id and the access level. It removes the entry in the PVT. Then the router sends the content packets to the user.

If the content name is not available in the Content Store, then it forwards the Interest Packet to the content provider or to the neighboring router. Finally, it reaches the Content provider which then sends a validation request to the AAA server. Based on the validation response, the content provider decides whether to send the content packets to the user or to deny the access.

**Algorithm 2: Content Provider Validation algorithm**

```
Input: Interest Packet (IntPacket) / Validation Packet;
Output: ValidationResponse Packet and Content Packets;

validationResult := forward validationPacket to AAA Server;
if (validationResult == true) then
    send validationResponsePacket with success;
    if (interestPacket == true) then
        Generate and send ContentPackets;
    end if
else
    send validationResponsePacket with failure;
end if
```

5. Related Work

Qi Li et. al. [1] proposed a LIVE method in which integrity check mechanism is improved and made very simple for computation whereas it doesn’t support the user authentication and authorization for the content access. Though they do content access control but it is limited to the group and not for an individual.

A. Afanasyev et. al. [3] discusses about the threats and counter measures in Interest Flooding Attacks. They identify the fake interests entering into the Pending interest Table and avoid the flooding attack. But they assume the interest packets with content that doesn’t exists as fake interest which is not true at all the time.

A. Afanasyev et. al. [4] an open forum discussion about the security and privacy issues that prevails in the named data networking.

T. Lauinger et. al. [7] discusses about the privacy risks in NDN. They proposed a selective Caching Mechanism in which only few content packets are cached in Content Store. Since, the cached data integrity verification is not handled, so it is prone to attacks.

M. Nabeel et. al. [6] introduced an efficient privacy preserving mechanism in which the privacy is maintained by handling Content based publishing systems.
Since it uses common brokers for routing messages which is a third party providers, it is their responsibility and we don’t have any control over data.

S. Arianfar et. al. [8] identified available threats on Content Caching and Data Privacy. Also, they proposed solutions for those threats but it is heavy in terms of computation overheads.

6. Conclusion

In this paper, we propose a new model for NDN to improve the security and the content access restriction to the specific users is achieved. Interest Flooding Attack which is a common network attack in NDN is avoided in this model. The performance of the Content Provider is improved thereby it can serve several other users of different locations. In future, a new mechanism for user enrollment in Content Provider’s AAA server will be done and will research more on enhancement and taking up to the security mechanism of TLS based authentication mechanism.

Acknowledgements. We thank ECI Telecom India Pvt. Ltd, Bangalore for financially supporting this paper to be published.

References


Received: November 8, 2015; Published: December 20, 2015