An Efficient and Secure Content Access Control in Named Data Networking

Rashmi M
M.Tech, CSE, VTU
Department of Computer Science & Engineering
Don Bosco Institute of Technology Bangalore, India

Shwetha Rani K P
Assistant Professor
Department of Computer Science & Engineering
Don Bosco Institute of Technology Bangalore, India

***Abstract*—The next generation future Internet architecture is believed to be changed. This is because there are vast researches and experiments going, to improve the current Internet architecture. This has led to a new Internet architecture named as Named Data Networking (NDN) .It is believed that the current IP architecture will be replaced with this new Internet architecture).The data packets in NDN will carry information of the contents being used in the network rather than carrying the IP address of the source and destination port addresses of a network. The main strength of NDN is that the data packets have a built-in security embedded with it. This eradicates many issues related to Internet security .For this purpose a concept called Lightweight Integrity Verification (LIVE) architecture is proposed which will resolve the current issues related to the Internet architecture.**

***Keywords*—NDN, IP network, data packets, security, LIVE**

I.INTRODUCTION

IP network is the current Internet architecture that is being used worldwide. The main task of IP network is to transmit data packets from source node to destination node based on the IP address that are present in the packet headers. This IP network is also referred as TCP/IP. Although IP network poses several advantages like security issues, self-containment it also induces many drawbacks.

Today's Internet was designed as a means of communication between two remote hosts. This was envisioned in 1970-s and early 1980-s as the predominant paradigm for resource sharing. Today, common Internet usage scenarios have changed significantly and include: large-scale content distribution, delay-tolerant networking, swarms of wireless devices producing and consuming data as well as mobile computing. Named-Data Networking (NDN) [30] is one such effort.

NDN is part of a field typically called Information-Centric Networking (ICN) [18], [26] – consisting of networking paradigms designed for efficient data distribution [22]. Related prominent efforts are PARC's Content-Centric Networking (CCN), whose open source software CCNx is used as a reference implementation for the work described below. In NDN, named data – rather than a named host or an interface address – is a first-class entity. Data is directly addressable, regardless on what host distributes it, and is returned in response to explicit requests from consumers, and is never sent unsolicited, i.e., NDN is a "pull" architecture.

NDN also stipulates that each piece of data must be signed by its producer. This allows decoupling of trust in data from trust in the entity that store and/or disseminates that data. NDN's long-term goal is to replace the current TCP/IPbased Internet architecture [12]. In order to succeed, it must be shown that NDN can support all major types of communication performed today and envisaged for the near future. Recent work focused on implementing telephony [21], video conferencing [40], smart meters [24], and control systems [4], [34] over NDN.

This paper provides further evidence of NDN's suitability for communication other than data distribution. Specifically, we explore the use of NDN for secure sensing applications. Sensors play a central role in the Internet of Things (IoT) [8]. Smart objects, which represent the building blocks of IoT, provide a bridge between physical (analog) and digital (cyber) worlds, through sensing. The use of sensors in IoT research builds on research of the embedded and wireless sensing community [2] and more recent efforts in sensing using general purpose mobile devices [5].

Related research in sensing and control by the NDN team, which motivates the work described here, has focused on the context of building automation systems (BAS). BAS are a traditional application of industrial control systems to managing the various systems of buildings, including heating, ventilation and air conditioning (HVAC), electrical distribution, water monitoring, fire detection and suppression, intrusion detection, and access control. The IP protocol suite is increasingly used to network their components and as such is now a fundamental substrate of new buildings [17].

In both BAS and IoT scenarios, the main purpose of a typical network-enabled sensor is to collect data and allow other devices and applications to access it remotely. Such sensors tend to be part of resource-constrained devices, for example being either battery-operated or energy-limited for sustainability reasons, with computing resources sufficient to perform data gathering and reporting. In order to save power, sensors can choose to sleep or hibernate whenever possible.

Therefore, any general approach to secure sensing must offer availability, integrity, origin authentication and access control (data privacy). Also, due to sensors' limited resources, a common DoS attack vector is to attempt to overwhelm the target sensor(s) with malicious requests. Thus, DoS mitigation is an important requirement All of the above, coupled with scalability, represent a major challenge in the context of any Internet architecture, including NDN. BAS and other industrial control systems have in the past

typically employed physical or logical isolation of the network as a primary security measure, and can likely do so no longer [25].

Our approach to sensing security must necessarily be more sophisticated. The rest of this paper is structured as follows: We proceed with an overview of related work in Section II. Then, Section III introduces our security framework, which provides foundation for the sensing protocols, presented in Section IV. The paper concludes in Section V.

II. RELATED STUDY

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.

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.

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.

III. SYSTEM DESIGN

A. Packet types

i. 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.

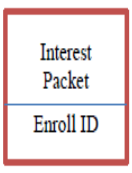

Fig.1.Int. packet Format

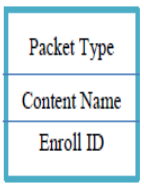

Fig.2.Validation Request Format

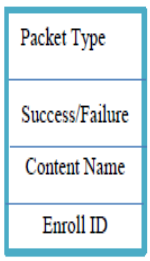

Fig.3.Validation Response Format

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 1.1 Access Table

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

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

Content Name	ID
/ndn/edu/sbu/me/calendar.pdf	/gce/cse/1563, /edu/sbu/1326
/ndn/org/caida/demo.mp4	/org/caido/25780
/ndn/edu/colostate/techmeet_video.mpeg	/org/caido/25780
/ndn/edu/arizona/network_lecture.ppt	/edu/annauniv/2914
/ndn/com/orange/new_tariff.xlsx	/com/airtel/2143

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.

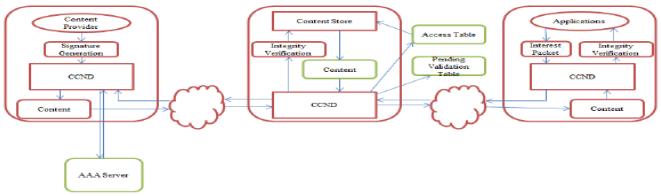

Fig.4. Proposed design for Role based Content Access Control

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.

Algorithm 1: Interest Validation Algorithm in NDN Routers

```
Input: Interest Packet (IntPacket)
if (IntPacket.ContentName exists in ContentStore) then
   EnrollID := IntPacket.EnrollID;
   if(enrollID exists in AccessTable) then
   //Check the acess 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
end if
if(validationResponsePacket == true) then
   remove contentName, enrollID in PVT;
   Update the entry in AccessTable;
   send contentPacket to ContentRequestor;
end if
```

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 enrolls 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.

Algorithm2: 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
```

V. PERFORMANCE EVALUATION

We use our prototype to determine the performance of LIVE. Since content access delay incurred by verification is proportional to length of content packet delivery, for simplicity, we only evaluate the delay of two-hop content forwarding with and without caching. Figure 5 shows the testbed of our experiments, including one user node *R*1 and one CP node *R*4.

Also, it includes two machines acting as NDN routers: *R*2 is a CR of the CP and can cache the contents from the CP, and *R*3 is the normal router that cannot cache the contents from CP. *R*3 forwards content requests received from *R*1 to *R*4.

We evaluate the performance of LIVE at *R*1 and *R*4 using Mac laptops with 2.53 GHz Intel CPU, 4GB RAM, and Mac OS 10.6.8. We investigate the token generation performance in the CP and measure the computation and content delivery delays introduced by LIVE in the user node R1.

Also, since LIVE increases the content packet size by piggybacking signatures, we measure the communication overhead incurred by LIVE. We evaluate the LIVE performance with different content sizes range from 150 bytes to 1480 bytes. To demonstrate the benefits of lightweight signatures in LIVE, we also implement a signing and verification library with the RSA algorithm with 1024-bit RSA keys by extending the OpenSSL library (OpenSSL-1.0.1c) [17].

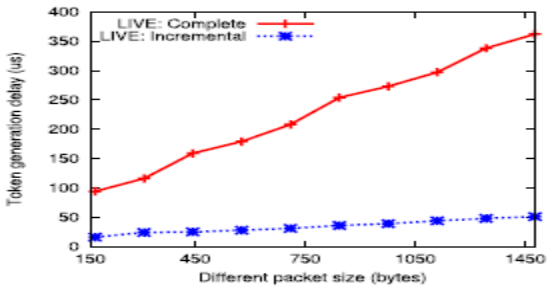

Fig 5: Performance of Token Generation

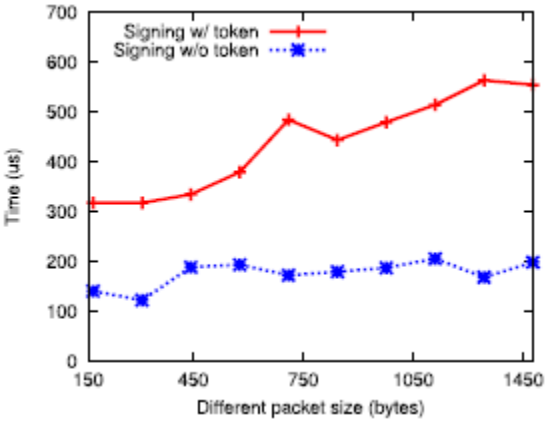

Fig 5: Content Signing Performance

VI. CONCLUSION

With the advent of the IoT and its convergence with critical infrastructure such as building automation systems (BAS), secure connectivity of resources constrained devices is becoming increasingly important. This paper focused on the design of a secure and efficient framework for connecting sensors with applications over NDN. Our framework includes a trust model that allows parties to authenticate sensor data, and fine-grained access control mechanisms based on data encryption as well as key attributes. We considered three types of sensors and constructed corresponding communication protocols tailored for NDN.

REFERENCES

[1] K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, 3, 2005.
[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. Computer Networks, 38, 2002.
[3] J. Al-karaki and A. Kamal. Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications, 11, 2004.
[4] J. Burke, P. Gasti, N. Nathan, and G. Tsudik. Securing instrumented environments over content-centric networking: the case of lighting control and NDN. In INFOCOM NOMEN, 2013.
[5] J. A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava. Participatory sensing. In World Sensor Web Workshop, ACM Sensys 2006, 2006.
[6] S. Camtepe and B. Yener. Key distribution mechanisms for wireless sensor networks: a survey. Technical report, 2005.
[7] Content centric networking (CCNx) project. http://www.ccnx.org.
[8] M. Chui, M. L¨offler, and R. Roberts. The internet of things. McKinsey Quarterly, 2:1–9, 2010.
[9] A. Compagno, M. Conti, P. Gasti, and G. Tsudik. Poseidon: mitigating interest flooding ddos attacks in named data networking. In LCN, 2013.

[10] S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun. ANDaNA: Anonymous named data networking application. In NDSS, 2012.
[11] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In CCS. ACM, 2002.
[12] National science foundation (NSF) future of internet architecture (FIA) program. http://www.nets-fia.net/.
[13] A. Fiat and M. Naor. Broadcast encryption. In CRYPTO, 1993.
[14] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In CRYPTO, 1999.
[15] P. Gasti and A. Merlo. On re-use of randomness in broadcast encryption. In PST, 2011.
[16] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang. DoS & DDoS in Named-Data Networking. In ICCCN NACSD, 2012.
[17] W. Granzer, D. Lechner, F. Praus, and W. Kastner. Securing ip backbones in building automation networks. In Industrial Informatics,2009. INDIN 2009. 7th IEEE International Conference on, pages 410–415. IEEE, 2009.
[18] M. Gritter and D. Cheriton. An architecture for content routing support in the internet. In USENIX USITS, 2001.
[19] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energyefficient communication protocol for wireless microsensor networks. In HICSS, 2000.
[20] C. Intanagonwiwat, R. Govindan, D. Estrin, J. S. Heidemann, and F. Silva. Directed diffusion for wireless sensor networking. IEEE/ACM Trans. Netw., 11(1):2–16, 2003.
[21] V. Jacobson, D. Smetters, N. Briggs, M. Plass, J. Thornton, and R. Braynard. VoCCN: Voice-over content centric networks. In ReArch, 2009.
[22] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, and R. Braynard. Networking named content. In ACM CoNEXT, 2009.
[23] C. Jones and K. Sivalingam. A survey of energy efficient network protocols for wireless networks. Wireless Networks, 7, 2001.
[24] K. Katsaros, W. Chai, N. Wang, G. Pavlou, H. Bontius, and M. Paolone. Information-centric networking for machine-to-machine data delivery: a case study in smart grid applications. Network, IEEE, 28(3), May 2014.
[25] E. D. Knapp. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress, 2011.
[26] T. Koponen, M. Chawla, B. Chun, A. Ermolinskiy, K. Kim, S. Shenker, and I. Stoica. A data-oriented (and beyond) network architecture. In ACM SIGCOMM, volume 37, pages 181–192. ACM, 2007.
[27] S. Kumar, V. Raghavan, and J. Deng. Medium access control protocols for ad hoc wireless networks: a survey. Ad Hoc Networks, 4:326–358, 2006.
[28] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In CCS. ACM, 2003.
[29] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson. Wireless sensor networks for habitat monitoring. In ACM WSNA, 2002.
[30] Named data networking project (NDN). http://named-data.org. Retrieved Mar. 2013.