Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 9, September 2015, pg.350 – 355

RESEARCH ARTICLE

Unintellectual Accuracy Verification and Data Access for Named Data Networking

Soumya M J, Dhanya M
Computer Science and Engineering, India
soumyamj.07@gmail.com, dhanyamohanshenoi@gmail.com

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.

To overcome the drawbacks of IP network that are mentioned above a new concept called as NAMED DATA NETWORK (NDN) is used. NDN is one among the five research project that is being carried in America. NDN is termed as future internet architecture. NDN poses several advantages over current IP network. The data packet in NDN is secured by digitally signing it by an entity so that its authenticity and integrity will be easily verified by the users and the network nodes present in NDN. Due to establishing these security concerns NDN design involves few challenges.

Security challenges involved in NDN are listed below-

- Existing algorithm is heavy weight signature generation and verification algorithm. This algorithm is named heavy weight because the universal content verification is difficult to achieve in the network nodes
- Any node in NDN is capable to access the contents without the permission of the Content Provider (CP).

To address the issues of existing algorithm, a new algorithm is leveraged in the network layer with minimum extensions. The proposed Lightweight Integrity Verification algorithm uses an efficient key update management.

The main function of this is that unauthorized nodes and users cannot verify the data packets travelling across the NDN and thus drop those packets in the network. This is achieved by the CP by issuing a status for each content packet regarding the content name and the NDN nodes which request them. Therefore the LIVE ensures that the content access is performed by CP and the CP has all the power over the data which is being transmitted over the NDN.

To establish LIVE architecture we need to face few challenges. The challenges are listed below-

•As mentioned heavy weight algorithm is a traditional algorithm. They introduce runtime and computation overhead in the network which is sometimes not possible to accept by the NDN nodes maintaining the traffic.
•In traditional schemes it would be difficult to withdraw public keys. Due to this it may effect to cancel content verification permissions that are assigned to the nodes as well as users.
•Traditional schemes requires public key management infrastructure used to check the trust chain of the public keys before the mode of verifying the signatures of the data packets.

II. EXISTING SYSTEM

The existing internet architecture is IP network. It is connectionless network heterogeneity.it involves IP datagram and it is network layer protocol. The representation of IP hour glass is shown in Fig. 1-

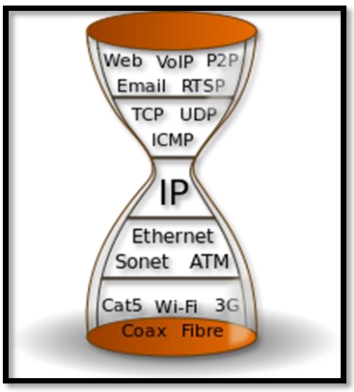

Fig. 1 Representation of IP hour glass

Limitation of IP network is as below-

- In IP network, intelligence is present only at host side of the network
- Routing establishes only connectivity and provides one kind of service like best effort datagram

Heavy weight signature generation and verification algorithms involves drawbacks which are listed below-

- They introduce runtime and computation overhead in the network which is sometimes not possible to accept by the NDN nodes maintaining the traffic.
- In traditional schemes it would be difficult to withdraw public keys. Due to this it mat effect to cancel content verification permissions that are assigned to the nodes as well as users.
- Traditional schemes requires public key management infrastructure used to check the trust chain of the public keys before the mode of verifying the signatures of the data packets.
- Routers present in the network have limited computation resources that are specifically used for content routing and forwarding of the data packets.

III.PROPOSED SYSTEM

- Every data packet in NDN is digitally signed by an entity so that its authenticity and integrity is verified by the network nodes and the users irrespective where the data packet is retrieved.
- The routers have control over verification capability of content integrity and authenticity for NDN nodes through efficient key update mechanism so that unauthorized users cannot access the data packets. And finally drop them in NDN.
- Proposed solution enables that that content access performed by each of the NDN node is under the CP's control since NDN nodes cannot access corrupted contents in the network.

Advantages of proposed LIVE architecture is as below-

- The name light weight for LIVE architecture is due to the usage of light weight hash functions that are used in here. They are lightweight enough for NDN nodes to verify signatures of the data packets and content integrity in NDN.
- The practical advantage of LIVE is content caching can be easily cancelled by CPs by changing tokens used to sign contents in NDN.
- Simplicity part of LIVE is tokens are easily generated by CP and flexibly distributed by CPs with a flat architecture that does not require "trust chain" among different tokens used in the network

A. *Fundamental principles of NDN*

- The binding principles of TCP/IP is included in the "thin waist" at network layer of OSI model. This helps in promoting the self-sustaining innovation and also to provide end to end control where required in the network
- Consider the evolution of network usage and generalize the thin waist so that to allow packets to name the content which is being carried out.
- Integration of fundamental architectural primordia's of TCP/IP such as every single data packet is cryptographically authenticated, derive the traffic flow control, forwarding capabilities and adaptive routing.

B. *Architecture of NDN*

The communication in NDN is mainly operated by the receivers. Receivers are also referred as data consumers. Receivers communicate with the help of two types of packets, namely Interest and Data. Both of them Interest and Data carry a name that indicates a portion of the data that is broadcasted in any of the Data packet.

A data consumer places the name of required portion of data into Interest packet and forward that Interest packet into the network. The network routers make use of this name to direct the Interest to data producer. Once the Interest packet arrive at network node that poses a requested data in it, then that particular node returns a Data packet which includes name and content along with a signature by producers key that wraps the two. This is represented in below figure. The packets in NDN architecture is represented in Fig. 2-

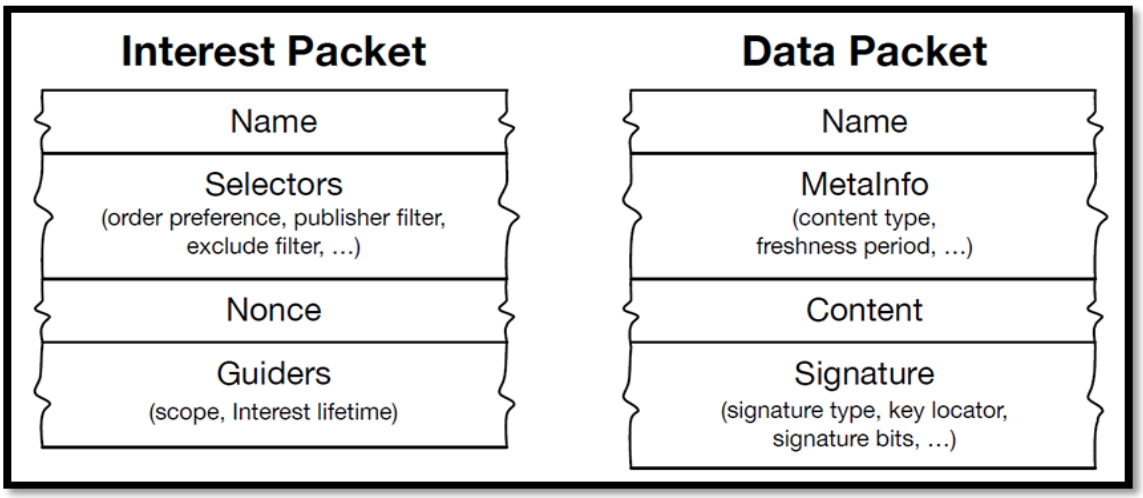

Fig. 2 Packets in NDN

There is enormous support coming from networking community to enlarge in the process of NDN design and its development. All this wrapped together is enforcing to a new architecture called Named Data Networking. Below Fig. 3 represents a NDN testbed that is being carried out as a project in America.

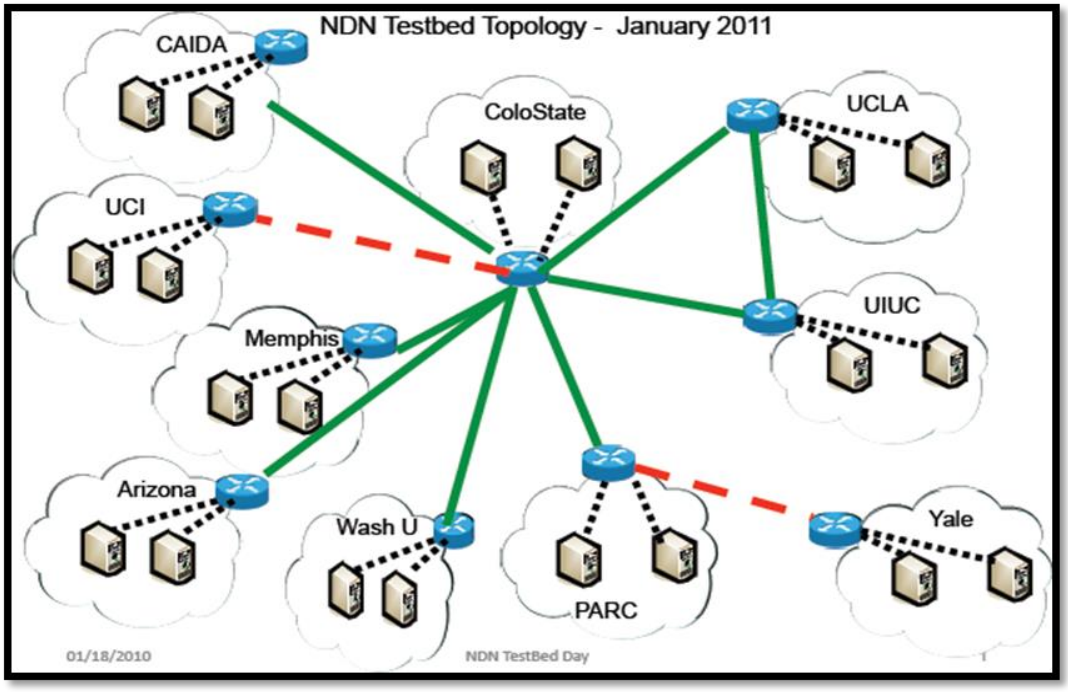

Fig.3 Testbed topology

The Data packet in the network follows in direction opposite to Interest packet and finally arrives at requesting consumer.

To follow up with the forwarding process of Interest and Data packets in the network, each of the individual NDN routers in network support three data structures-

- Pending Interest Table (PIT)
- Forwarding Information Base (FIB)
- Content Store (CS)
- Forwarding Strategy Module

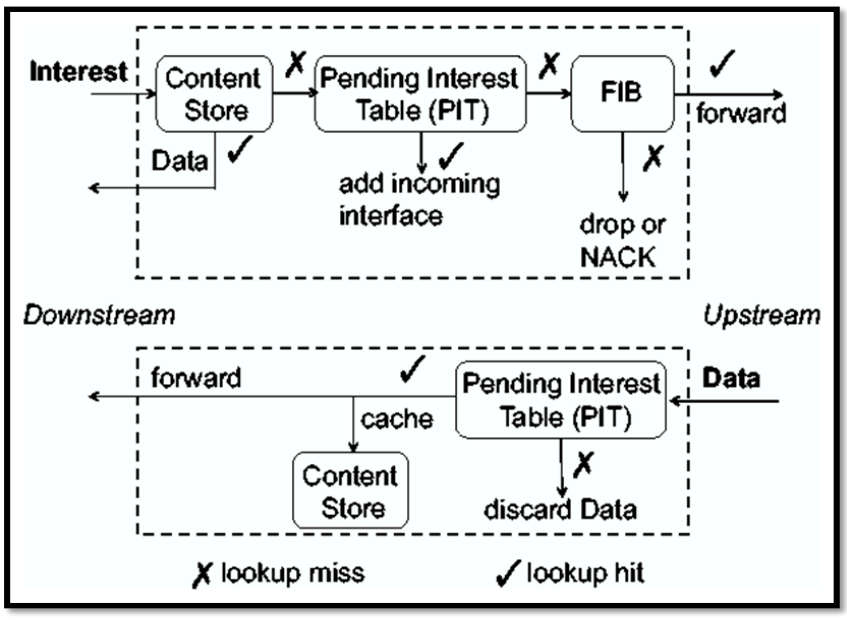

Fig. 4 Communication in NDN

The communication procedure that is carried out in NDN can be illustrated in Fig. 4 shown above. The PIT is used to accumulate Interests packets which are forwarded by the network routers and those packets which are

not satisfied. PIT records all the information of the packets both incoming and outgoing. Whenever a packet comes, first the router checks with content store for matching data. If data is found then it returns from that content store otherwise it will forward to data producer directly. Content Store can be regarded as a temporary storage of the data packets. Both type of packets, Interest or Data do not specify host address rather name is specified and accordingly they are transmitted in the NDN. This will banish the requirement of source or the destination nodes during delivery of the data which is just reverse as in IP's end to end delivery of data packets.

The design of NDN is such that the NDN names are non-transparent to the network. This facilitates any application to have its own kind of naming context scheme that fits its need and requirement. This specifies that naming scheme is independent and can be evolved according to the needs of a network. The naming design is of hierarchical structure which is shown with an example as shown below. Consider a video created by VTU, so the naming design would be as- /vtu/videos/test.mpg, where '/' indicates name components in the format of text depiction. This is almost similar to the way URLs are depicted.

In TCP/IP, the security is distributed across the endpoints in the network. Whereas in NDN the security is established by the data producers in the NDN. This is achieved in a way that the data producers will apply cryptographic functions on each data packet and sign them.

In MD5 algorithm any message is divided into number of pieces of 512-bit blocks. Next the message is padded so that the message length is divisible by 512.

C. *NDN Architecture Development*

The NDN requires a standard process for the way Interest and Data packets transmit around the network. And a description of the functions that exist in network layer of the OSI. There is also a need to support naming procedure, high rating of forwarding and routing procedure, trust management and forwarding strategy. This is supported by software libraries which are not embedded in NDN but explicitly support in maintaining all the activities.

NDN is in development stage in many applications. These applications and their implementation stage is described below-

- Video streaming – this application is the first one to demonstrate the nature of NDN data delivery nature.
- Real time conferencing – this application is demonstrated via an application called ChronoChat which is a multi-user chat application. This supports encrypting of the data being received by end user.
- Building automation system – ideal are where this application is viewed is in enterprise building automation and management systems. NDN research is being carried on this field.
- Vehicular networking – this application illustrates the process of enabling location based content retrieval and discovering new support models to support the communication in NDN.
- Other applications – the existing NDN software platform enables students and interested people to research on the methods and implementations of NDN.

Hardware system configuration

- System processor - Pentium IV
- Hard disk - 40 GB
- RAM - 1GB
- Speed - 2.4 GHz

Software system configuration

- Operating System -Windows 7 / 8
- Coding language - JAVA

- Front end - JAVA SWINGS
- Database - MySQL
- Database connectivity - JDBC

IV. CONCLUSIONS

The proposed LIVE project establishes integrity and authenticity in the communication network. Light weight hash functions are used in generating the signature for the packets, hence the name Light Weight for the project. The LIVE also establishes access control over the contents in the network which makes content provider to have control over the data being exchanged in NDN.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity,Unlinkability, Unobservability, Pseudonymity, and Identity Managementa Consolidated Proposal for Terminology, Version 0.31,"technical report, 2005.

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "AnAnonymous On-Demand Position-Based Routing in MobileAd Hoc Networks," Proc. Int'l Symp. Applications on Internet(SAINT), 2006.

[3] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l WorkshopMobile Distributed Computing (ICDCSW), 2005.

[4] V. Pathak, D. Yao, and L. Iftode, "Securing Location AwareServices over VANET Using Geographical Secure Path Routing,"

[5] Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008. K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2007.

