A virtualized and monitored NDN infrastructure featuring a NDN/HTTP gateway

Xavier Marchal, Moustapha El Aoun, Bertrand Mathieu, Wissam Mallouli, Thibault Cholez, Guillaume Doyen, Patrick Truong, Alain Ploix, Edgardo Montes de Oca

A virtualized and monitored NDN infrastructure featuring a NDN/HTTP gateway

Xavier Marchal[1], Moustapha El Aoun[2], Bertrand Mathieu[3], Wissam Mallouli[4], Thibault Cholez[1], Guillaume Doyen[2], Patrick Truong[3], Alain Ploix[2] and Edgardo Montes De Oca[4]

[1]LORIA, UMR 7503
University of Lorraine, CNRS, INRIA
Vandoeuvre-les-Nancy, France

[2]Troyes University of Technology
ICD, UMR CNRS 6281
Troyes, France

[3]Orange Labs
Lannion, France

[4]Montimage
Paris, France

ABSTRACT

We present two practical components to allow real deployment of NDN: a NDN/HTTP gateway that allows to connect a NDN network to the rest of the World Wide Web, and a monitoring solution dedicated to NDN. Following NFV principle, all components of our NDN network are deployed as Virtual Network Functions and run on standard hardware. The whole infrastructure will be shown in a live demo at the conference.

1. INTRODUCTION

Network operators are reluctant to deploy globally Named Data Networking (NDN) because of the huge investment costs required and the uncertainty about the security and the manageability of such disruptive network protocols when deployed in production, while the return of investment is also uncertain. Meanwhile, Network Functions Virtualization (NFV) greatly facilitates the deployment of novel networking architectures by reducing the costs thanks to the usage of commodity hardware in place of dedicated equipments. Consequently, leveraging NFV to ease the deployment of NDN infrastructures appears as a strong mean to incite network operators to adopt this technology. In this context, the challenge we address is to fulfil the requirements needed to move NDN from a solution restricted to labs or tesbeds to a fully operational one by developing NDN-specific Virtual Network Functions (VNF).

In this effort, the first questions which arise are related to (1) the integration of NDN into the existing Internet, and particularly the collocation of NDN with IP and HTTP; and, (2) the capability for a telco-operator to actually monitor a NDN network. Consequently, we proposed and developed early versions of components that provide a solution to these two requirements : a fully-capable NDN/HTTP gateway and a monitoring architecture for NDN. Following NFV principle to gain flexibility and reduce costs, all components are virtualized thanks to Docker and run on standard hardware. We briefly describe these contributions in the following sections.

2. NEWLY DEVELOPED NDN NETWORK COMPONENTS

2.1 NDN/HTTP Gateway

We consider the Web as our use-case since (1) it is known to be the most popular service of the Internet; and, (2) the benefits of transporting web-like traffic is a relevant purpose for the ICN research field. However, since current web clients and servers do not yet implement NDN, we have designed and implemented a dedicated gateway to perform NDN/HTTP translations in order to connect a NDN network to the rest of the the World Wide Web. The gateway is designed as a Virtual Network Function (VNF) that can be deployed when and where required, following VNF principles. The NDN/HTTP translation is actually done using two gateways: (1) the ingress gateway (iGW) is responsible to convert incoming HTTP requests from any client into NDN packets and to reply with the servers' responses by converting the received NDN Data into HTTP replies; and, (2) the egress gateway (eGW), the counterpart of the first one, is responsible to convert NDN packets received from the inside into HTTP requests sent to the right websites, and convert back the HTTP replies to forward NDN Data packets.

More precisely, the communication between the two gateways is done in three steps. First, when receiving a new request, the iGW creates a NDN name suffix from the requested URL that will be used between the two gateways for this data exchange. Then, the iGW sends an Interest to the eGW with a name component that announces a new request for this suffix. The eGW responds with a Data packet that carries a status code. Since Interests should not carry data, the eGW sends in turn an Interest with a name containing the suffix made by the iGW in order to retrieve the full HTTP request. In the last step, the iGW sends Interests to get the HTTP data retrieved by the eGW on the Web. If the content is already present in caches, Interests are directly answered from the NDN network, following NDN principles, without soliciting the eGW.

2.2 MMT monitoring architecture

The monitoring solution proposed in the demonstrator is based on the Montimage Monitoring Tool (MMT) solution. MMT relies on DPI technology and allows, thanks to a dedicated plug-in, to analyse NDN-based traffic and extract different attributes from this protocol stack. MMT also allows computing performance and security indicators at runtime so that the operator can take corrective actions in the case when an incident is detected. The monitoring architecture is composed of several MMT-probes (or agents) deployed in each virtualized network function (here NDN nodes) which communicate with a centralized MMT-operator in the context of a dedicated management network. The MMT-opera-

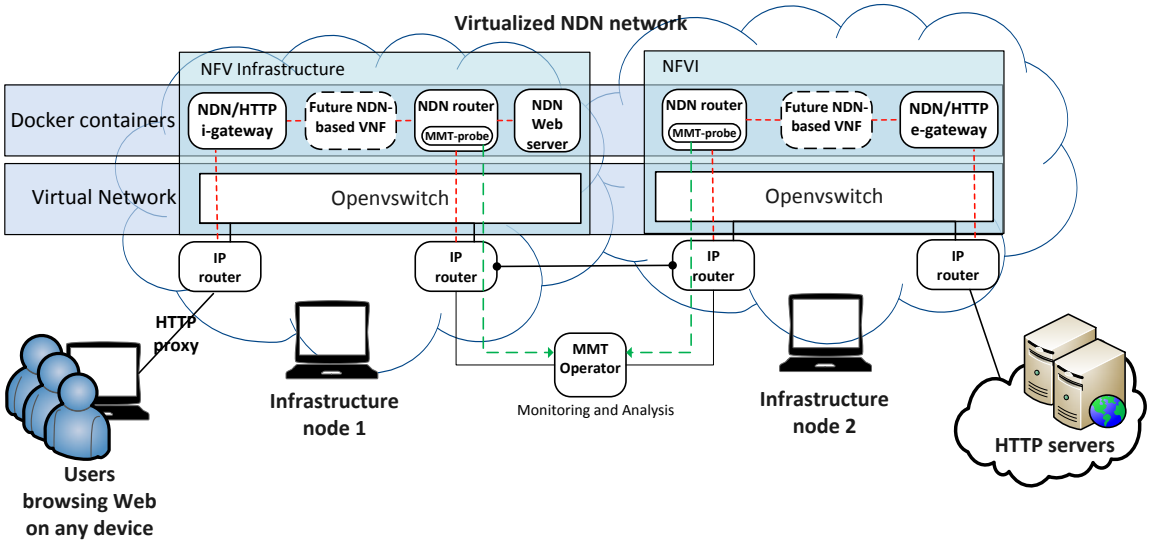

Figure 1: Virtualized NDN network demonstrator

tor, which operates the distributed MMT-probes, intercepts the notifications they send and builds customized Web-based reports to provide a global view of the virtualised NDN network. For example, accounting functions can determine the most visited web sites and security functions can detect potential attacks such as the Interest flooding attacks.

3. VIRTUALIZATION INFRASTRUCTURE AND DEMO SCENARIO

Our methodology to develop a secured virtualized NDN network is incremental. We currently have implemented the network components needed to generate and monitor NDN traffic, while security and orchestration aspects are left for future work. The current demonstrator is composed of five types of components (iGW, eGW, MMT-probe, MMT-operator and NFD) as shown in Figure 1.

3.1 Virtualized NDN architecture

As a computing virtualization framework, we use Docker, which provides lightweight virtualization. Without specific optimization, Docker performs better than other legacy virtualization solutions in terms of network I/O, which is critical when hosting a VNF. First, we "dockerized" the NDN Forwarding Demon as a VNF deployable in our architecture. Then, we developed components to (1) retrieve HTTP requests and convert them in NDN requests and vice-versa; and, (2) monitor NDN traffic with the MMT monitoring solution, by inserting a monitoring agent (MMT-probe) that collects and analyses NDN traffic into each VNF. A virtual network based on OpenvSwitch is deployed to ensure end-to-end network connectivity between all containers. The latter is implemented by VxLAN tunnels, thus enabling our infrastructure to be freely distributed on several telco Points of Presence (PoP) over the Internet. Within the NDN network, the nodes deploy the NDN stack with the latest version of NFD (0.4.1) and NLSR (Named-data Link State Routing Protocol).

3.2 Demonstration scenario

Our demonstration consists in a set up where people can freely navigate on the web, using a classical browser, but through the virtualized NDN network. We use a standard proxy to redirect the regular HTTP/IP-based traffic to the NDN network through the iGW. A native NDN web server will also be directly reachable inside the NDN network, without having to solicit the eGW. Users will thus be able to see in real-time on a web based graphical interface the statistics collected by the MMT-probes related to the NDN traffic they generate while surfing. Some early security analysis of NDN traffic to detect potential flooding attacks will also be displayed by the monitoring solution.

4. CONCLUSION

Deploying NDN as Virtualized Network Functions (VNF) and developing new components that can (1) monitor and secure NDN networks and (2) connect them to the rest of the Internet are important means toward fully-operable NDN solutions. The demo we present shows practical advances in that direction. Our future work will focus on the development and integration of new virtualized NDN components (like a NDN firewall), and on the orchestration of the whole virtualized NDN infrastructure to answer operational needs.

Acknowledgement: This work is partially co-funded by (1) the French National Research Agency (ANR), DOCTOR project under grant <ANR-14-CE28-0001>, and (2) the CRCA and FEDER CyberSec Platform, (D201304601).