Towards Content-Oriented Orchestration for virtual Information Centric Networking

Guillaume DOYEN, on behalf of the Doctor consortium
Troyes University of Technology – Charles Delaunay Institute
Contact: guillaume.doyen@utt.fr
Web: http://www.doctor-project.org

ICNRC – IETF meeting #101 – London – March 20, 2018
Outline

- Context
  - Locks for an ICN deployment

- Leveraging NFV as an ICN enabler
  - Opportunities and challenges
  - NDN Monitoring and Security
  - NDN Management and Orchestration

- Current results
  - Overall deployment and attack scenario
  - Monitoring evaluation
  - Orchestration evaluation

- Conclusion and perspectives
Outline

- **Context**
  - Locks for an ICN deployment

- **Leveraging NFV as an ICN enabler**
  - Opportunities and challenges
  - NDN Monitoring and Security
  - NDN Management and Orchestration

- **Current results**
  - Overall deployment and attack scenario
  - Monitoring evaluation
  - Orchestration evaluation

- **Conclusion and perspectives**
Locks for an ICN deployment

- A decade of research and development
  - Fundamental research topics covered
  - A set of operational implementations

- A pragmatic deployment approach
  - A progressive migration performed according to opportunities
    - Services that would benefit from an ICN stack at most
    - Topological locations (access, edge, core) that best fit with ICN Traffic Engineering features (e.g. symmetric routing, caching)
  - Management and security frameworks are required
  - Cohabitation with IP must be handled
  - This is the position of the 2014-2018 Doctor Project
    - Funded by the (French) National Research Agency (ANR)
    - Selected NDN as a target ICN technology
Outline

- **Context**
  - Locks for an ICN deployment

- **Leveraging NFV as an ICN enabler**
  - Opportunities and challenges
  - NDN Monitoring and Security
  - NDN Management and Orchestration

- **Current results**
  - Overall deployment and attack scenario
  - Monitoring evaluation
  - Orchestration evaluation

- **Conclusion and perspectives**
Where and how ICN stacks can be deployed?

- **Coupling ICN and IP**
  - Mixing protocol stacks (see CISCO H-ICN)
  - Leveraging Software Defined Networking [1-6]
  - Beyond : data-plane programmability for ICN pipelines through P4 [7]

- **Isolating ICN and IP**
  - Parallel combination with dual stacks nodes and end-hosts
  - Serial combination with dedicated gateways

- **Contribution of the Doctor project**
  - Cohabitation with IP can be handled with NFV
NFV: opportunities and challenges

The promise

- By leveraging the isolation property of virtualisation, an ICN stack can be deployed independently from any other networking stack.
- Tenant domains and infrastructure domains are decoupled.
  - ICN is a tenant domain protocol stack in a virtual L2.
  - In the infrastructure domain, IP still remains the networking substrate carrying all Internet traffic.
- NFV aims at reducing CAPEX by enabling commodity servers to host softwarized network functions.

The challenges

- Efficient Virtual Network Functions must be designed and implemented.
  - The stateful and CPU intensive nature of an ICN data-plane is hardly compatible with operations on the fly (spawn, migration, etc.).
- Novel Management and Orchestration solutions for virtual ICN network stacks must be entirely designed and implemented.
Content-Oriented MANO - PoC

Diagram showing components and interactions:

- Tenant Network Controller
- EM: NFV Agent, MMT Probe
- iGW, eGW
- Virtual Computing, Virtual Storage, Virtual Network
- Virtualisation Layer
- Virtualised Infrastructure Manager
- NFVI
- NFD Agent, MMT Probe
- Or-VnfM
- Ve-Vnf-em
- Or-Vi
- Or-Vnf
- NFV Orchestrator
- Orchestration engine
- TOSCA PROCESSOR
- TOSCA Descriptors
- TOSCA Parser
- Cyber CAPTOR
- NFD Agent, MMT Probe
- VNF Manager
- MMT Operator
- NFV Instances
- NFVI Resources
- NS Catalogue
- VNF Catalogue
- VNFM
- vnf-em
<table>
<thead>
<tr>
<th>Component</th>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faces</td>
<td>In Interest</td>
<td>Periodic number of incoming Interests</td>
</tr>
<tr>
<td></td>
<td>In Data</td>
<td>Periodic number of incoming Data</td>
</tr>
<tr>
<td></td>
<td>In NACK</td>
<td>Periodic number of incoming NACK</td>
</tr>
<tr>
<td></td>
<td>Out Interest</td>
<td>Periodic number of outgoing Interests</td>
</tr>
<tr>
<td></td>
<td>Out Data</td>
<td>Periodic number of outgoing Data</td>
</tr>
<tr>
<td></td>
<td>Out NACK</td>
<td>Periodic number of outgoing NACK</td>
</tr>
<tr>
<td></td>
<td>Drop Interest</td>
<td>Periodic number of dropped Interests</td>
</tr>
<tr>
<td></td>
<td>Drop Data</td>
<td>Periodic number of dropped Data</td>
</tr>
<tr>
<td></td>
<td>Drop NACK</td>
<td>Periodic number of dropped NACK</td>
</tr>
<tr>
<td>Content Store</td>
<td>CS Insert</td>
<td>Periodic number of Data insert in CS</td>
</tr>
<tr>
<td></td>
<td>CS Miss</td>
<td>Periodic number of cache miss in CS</td>
</tr>
<tr>
<td></td>
<td>CS Hit</td>
<td>Periodic number of cache hit in CS</td>
</tr>
<tr>
<td>Pending Interest Table</td>
<td>PIT Create</td>
<td>Periodic number of PIT entries created</td>
</tr>
<tr>
<td></td>
<td>PIT Update</td>
<td>Periodic number of updates in PIT</td>
</tr>
<tr>
<td></td>
<td>PIT Delete</td>
<td>Periodic number of PIT entries deleted</td>
</tr>
<tr>
<td></td>
<td>PIT unsatisfied</td>
<td>Periodic number of PIT entries unsatisfied</td>
</tr>
<tr>
<td></td>
<td><strong>PIT Size</strong></td>
<td><strong>Periodic number of PIT entries</strong></td>
</tr>
<tr>
<td></td>
<td>PIT Entries time</td>
<td>Average time in PIT for entries</td>
</tr>
</tbody>
</table>
Understanding NFD pipelines for anomaly detection

Correlating events
A TOSCA extension for ICN (1)

- **Virtual Deployment Unit (VDU)**
  - Abstraction describing the virtual resources over which a VNF is executed
- **Virtual Link (VL)**
  - Resources required to link two VDUs
- **Connection Point (CP)**
  - The connection capability which associates a VDU to a virtual link
- **Virtual Network Function (VNF)**
  - The piece of software that will be executed on a VDU
  - NDN router, ingress and egress HTTP gateways and NDN firewall
- **Forwarding Path and Graph**
  - a list of VNFs that a particular set of NDN packets must follow
  - Uses content prefixes instead of L2/L3 flow specifications
- **Policies**
  - Event-Condition-Action rules to apply dynamically
  - Upscaling, signature verification, firewall updates
NDN Orchestration

- Python code + REST APIs: implemented from scratch
- NFVO Core
  - Initial deployment of a NDN service
    - Deploy virtual networks -> Deploy virtual units -> Connect virtual units to virtual networks
    - Retrieve VDU and networks configurations -> Engage VNFs configuration (NDN Engine)
    - Make sure that VNFs are in a correct state -> Start monitoring probes and event correlators
- NDN Engine
  - Generates the appropriate NDN configuration for each VNF
    - NDN forwarding paths + NFVI information (IP addresses, identifiers, etc.) -> FIB entries
- VNF Manager
  - Responsible for the life-cycle management of NDN VNFs
  - VNF <-> VNFM <-> NFVO
    - Receives initial configurations and dynamic reconfigurations from NFVO and pushes them into VNFs
    - Gets notifications (security alerts) from VNF and send them the NFVO
Outline

- Context
  - On the maturity of the ICN paradigm

- Leveraging NFV as an ICN enabler
  - Opportunities and challenges
  - NDN Monitoring and Security
  - NDN Management and Orchestration

- Current results
  - Overall deployment and attack scenario
  - Monitoring evaluation
  - Orchestration evaluation

- Conclusion and perspectives
Evaluation context

- **European telco topology**
  - ClaraNet (4 PoP part of)
  - Points of Presence (PoP) made available through the Internet Zoo Topology Dataset

- **Different NDN VNFs**
  - NDN routers
  - Signature verification module
  - NDN Firewall

- **The whole network is deployed through virtualized means**
  - 1 PoP in 1 Openstack VM

By claranet (claranet) [CC0], via Wikimedia Commons
Evaluation topology
TOSCA VNF and VDU specifications

**router_2:**
- type: tosca.nodes.nfv.doctor.VNF
- properties:
  - id: 2
  - vendor: orange
  - version: 1.0
- requirements:
  - VDU: VDU2

**firewall_1:**
- type: tosca.nodes.nfv.doctor.VNF.firewall
- properties:
  - id: 6
  - vendor: orange
  - version: 1.0
  - configuration:
    - mode: accept
    - rules:
      - action: append-drop
      - prefix: [/foo]
- requirements:
  - VDU: VDU4

**VDU2:**
- type: tosca.nodes.nfv.doctor.VDU
- properties:
  - name: VDU2
  - sw_image: maouadj/ndn_router:v1
  - config: /doctor/launch_nfd_router.sh
  - flavor: medium
  - placement_policy: ['popLocation==uk']

**VDU4:**
- type: tosca.nodes.nfv.doctor.VDU
- properties:
  - name: VDU4
  - sw_image: maouadj/ndn_firewall:v1
  - config: /doctor/launch_ndn_firewall.sh
  - flavor: medium
  - placement_policy:
    - popLocation==netherlands
http_from_r2_to_as1:
  type: tosca.nodes.nfv.doctor.FP
  description: creates path for /http from r2 to as1
  properties:
    id: 2
    policy:
      type: NDN
      prefix: [/com/google]
    path:
      - forwarder: router_2
        capability: VDU2_VL10_CP
      - forwarder: router_x
        capability: VDUX_VL10_CP
      - forwarder: router_x
        capability: VDUX_VL2_CP
      - forwarder: router_4
        capability: VDU3_VL2_CP
      - forwarder: router_4
        capability: VDU3_VL3_CP
      - forwarder: firewall_1
        capability: VDU4_VL3_CP
      - forwarder: firewall_1
        capability: VDU4_VL4_CP
      - forwarder: peering_router_1
        capability: VDU5_VL4_CP
TOSCA mitigation policies specifications

- Starts the signature verification enforcement if a CPA alert is raised

  policies:
  - CPA_countermeasure:
    type: tosca.policies.nfv.doctor.security.signature_verification
    targets: [router_4, router_5]
    triggers:

      peeringPoint1_verification:
      event_type: tosca.nfv.doctor.security.alert.cpa
      condition:
      constraint: triggered_by router_2
      action:
      action_type: update_router_mode
      mode: signing
      target_router: router_4

- Updates the firewall black list with prefixes whose signature is invalid

- Spawn NDN routers to cope with the resource exhaustion due to signature verification
Monitoring and detection results

Relevance of the Bayesian Network Classifier (BNC) [NOMS 2018]

Guarantee of prescribed PFA for micro-detectors

Learning curve of the proposed BNC
Orchestration and mitigation

- Delay for the mitigation policy enforcement [ongoing work]

Weak attack footprint (8 Interests/s)  
Strong attack footprint (128 Interests/s)
Orchestration and mitigation

- **Overall mitigation evaluation** [ongoing work]

![Graph 1: Average mitigation delay according to the attack rate](image1)

![Graph 2: Mitigation efficiency (bad/good packets ratio) according to the attack rate](image2)

Average mitigation delay according to the attack rate

Mitigation efficiency (bad/good packets ratio) according to the attack rate

21
Outline

- Context
  - Locks for an ICN deployment

- Leveraging NFV as an ICN enabler
  - Opportunities and challenges
  - NDN Monitoring and Security
  - NDN Management and Orchestration

- Current results
  - Overall deployment ant attack scenario
  - Monitoring evaluation
  - Orchestration evaluation

- Conclusion and perspectives
Conclusion and perspectives

- An ongoing work toward the design and implementation of NFV-MANO components for NDN
  - A proof of concept of the whole architecture
  - (Part of) code availability
    - https://github.com/DOCTOR-ANR
    - Some components are still under development

- Doctor and ICNRG
  - Doctor is open to serve ICNRG efforts to push forward the deployment and standardization of this network paradigm
  - Toward a standardized management plane for ICN?

- Future work
  - Evaluate the benefits of an NDN virtual network carrying web traffic with real end-users
  - Further explore the content orchestration
  - Explore micro-services orchestration for NDN
Questions ?
References


Related Project publications


