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

ICNRG – 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

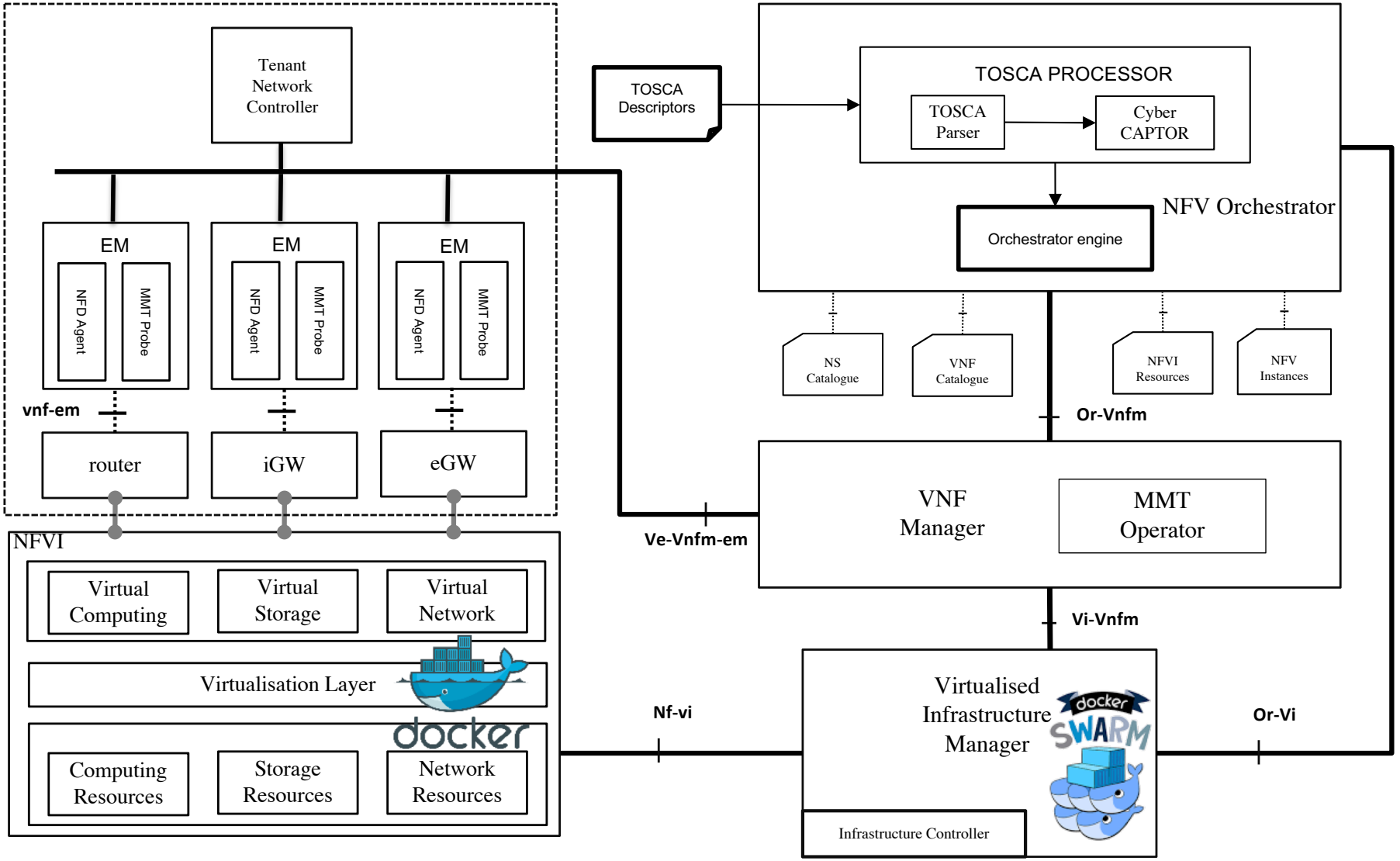
Where and how ICN stacks can be deployed?

- 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

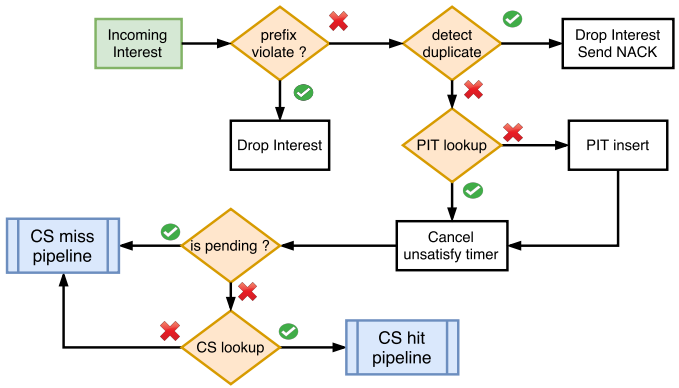


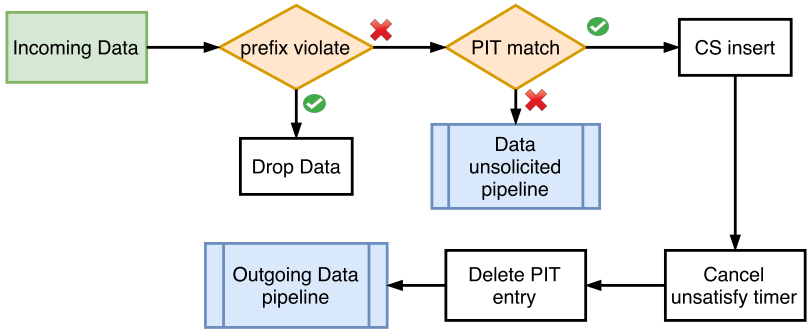
NFD Monitoring [NOMS 2018]

Component	Metric	Description
Faces	In Interest	Periodic number of incoming Interests
	In Data	Periodic number of incoming Data
	In NACK	Periodic number of incoming NACK
	Out Interest	Periodic number of outgoing Interests
	Out Data	Periodic number of outgoing Data
	Out NACK	Periodic number of outgoing NACK
	Drop Interest	Periodic number of dropped Interests
	Drop Data	Periodic number of dropped Data
	Drop NACK	Periodic number of dropped NACK
Content Store	CS Insert	Periodic number of Data insert in CS
	CS Miss	Periodic number of cache miss in CS
	CS Hit	Periodic number of cache hit in CS
Pending Interest Table	PIT Create	Periodic number of PIT entries created
	PIT Update	Periodic number of updates in PIT
	PIT Delete	Periodic number of PIT entries deleted
	PIT unsatisfied	Periodic number of PIT entries unsatisfied
	PIT Size	**Periodic number of PIT entries**
	PIT Entries time	Average time in PIT for entries

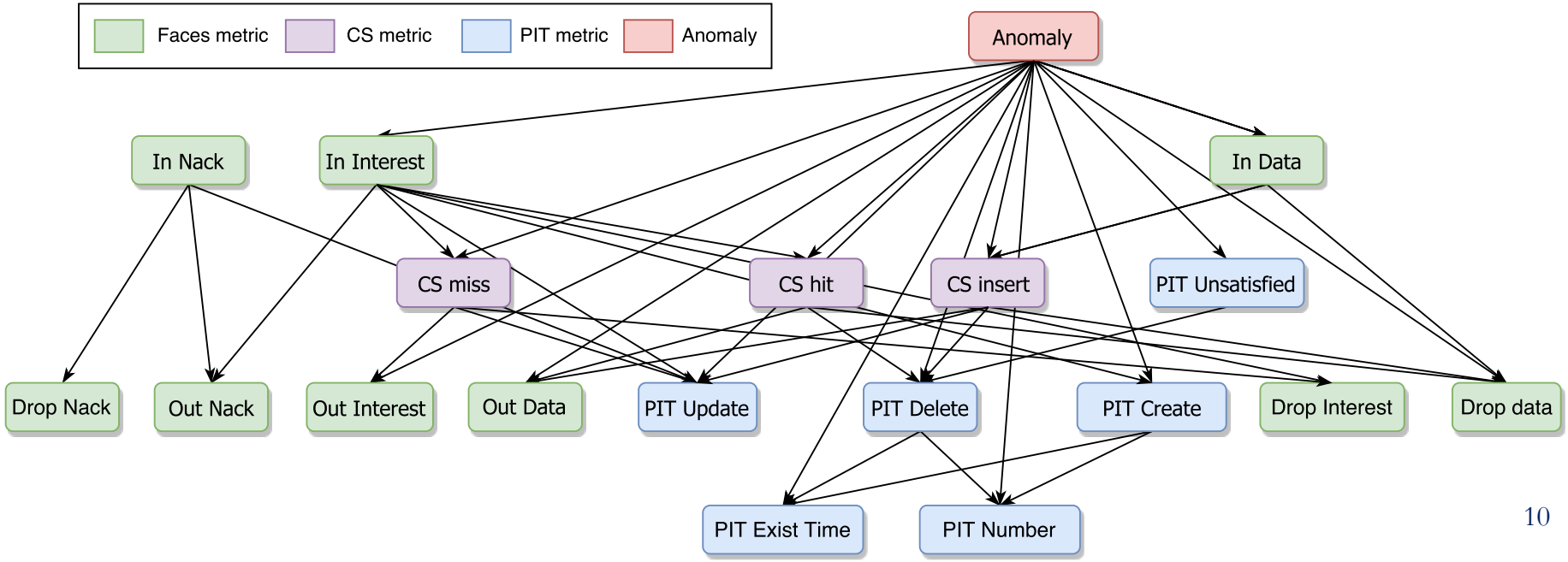
NDN Event Management [NOMS 2018]

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

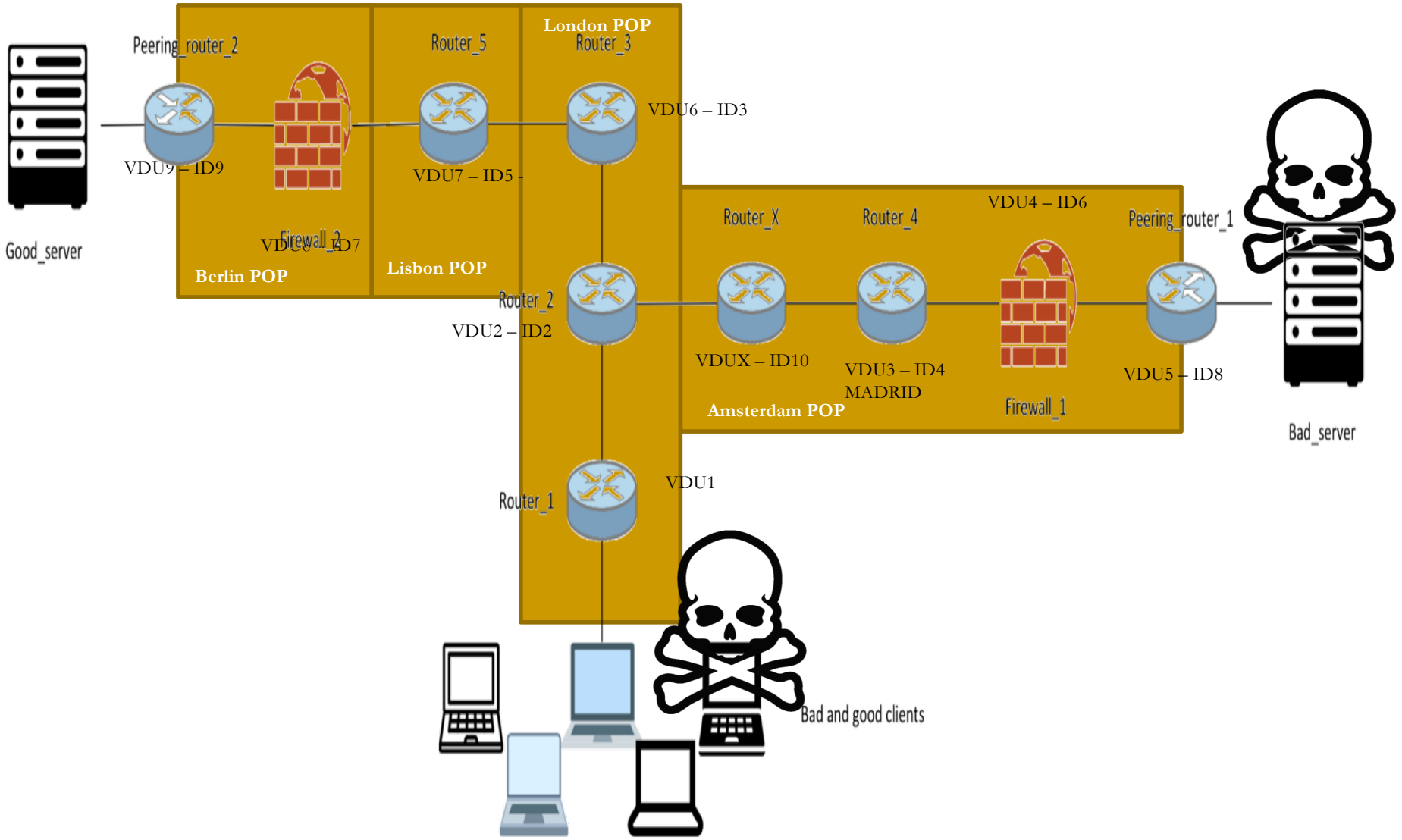
- Context
  - On the maturity of the ICN paradigm
- Leveraging NFV as an ICN enabler
  - Opportunities and challenges
  - NDN Monitoring and Security
  - NDN Management and Orchestration
- Current results
  - Overall deployment and attack scenario
  - Monitoring evaluation
  - Orchestration evaluation
- 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']
```

TOSCA Forwarding Path Specification

```
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

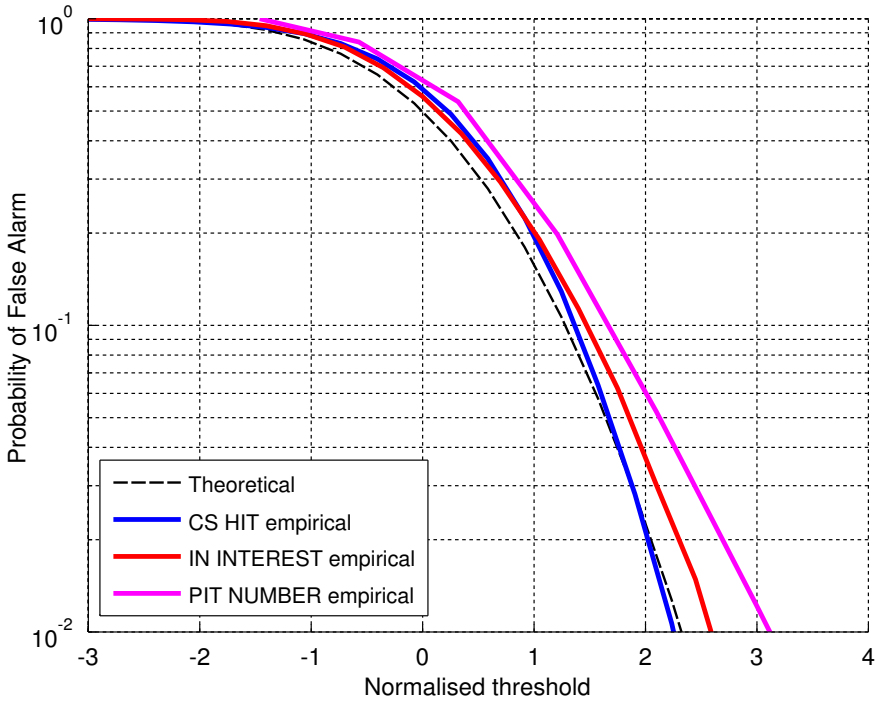
```
policies:
  - CPA_countermeasure:
    type: tosca.policies.nfv.doctor.security.signature_verification
    targets: [router_4, router_5]
    triggers:

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

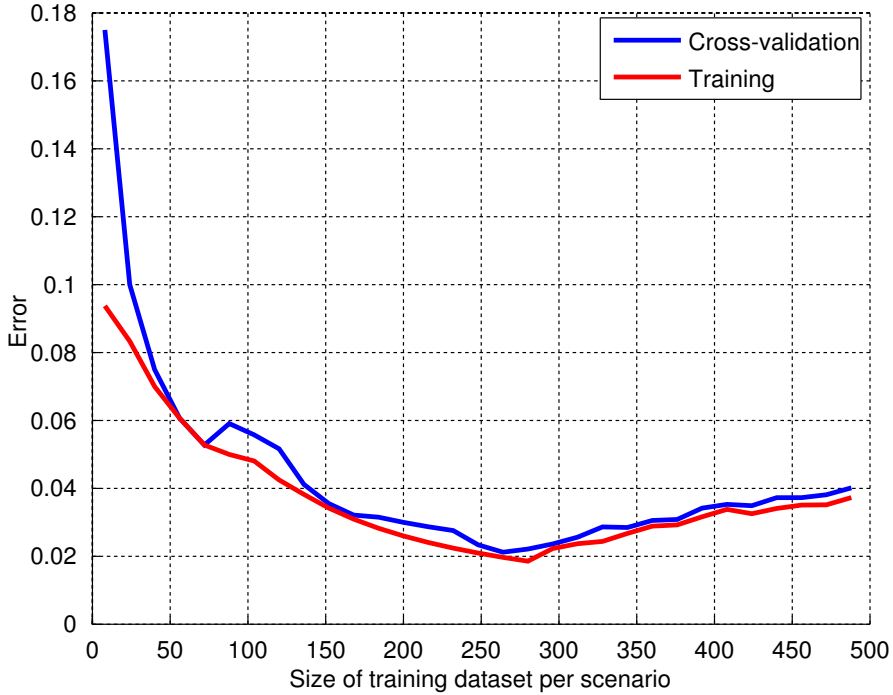
- Updates the firewall black list with prefixes whose signature is invalid
- Spawn NDN routers to cope with the resource exhaustion due to signature verification

Monitoring and detection results

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



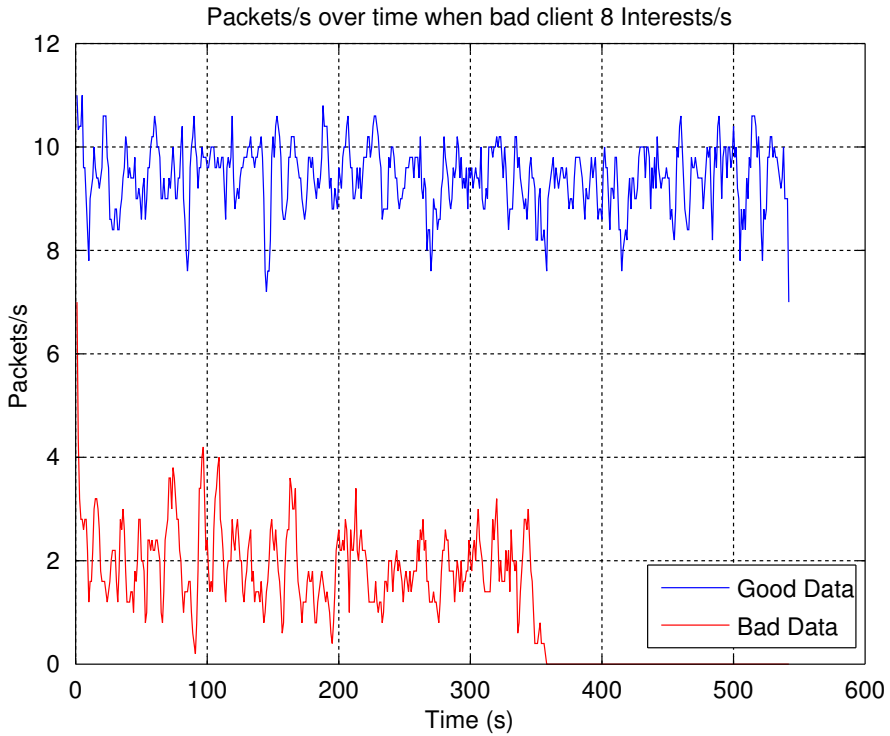
Guarantee of prescribed PFA for micro-detectors



Learning curve of the proposed BNC

Orchestration and mitigation

- Delay for the mitigation policy enforcement [ongoing work]

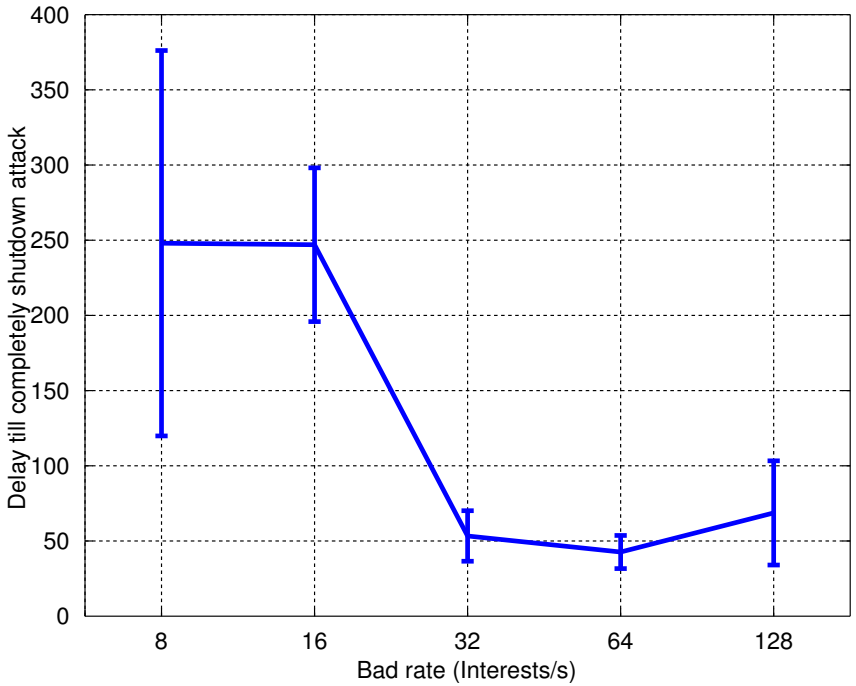


Weak attack footprint (8 Interests/s)

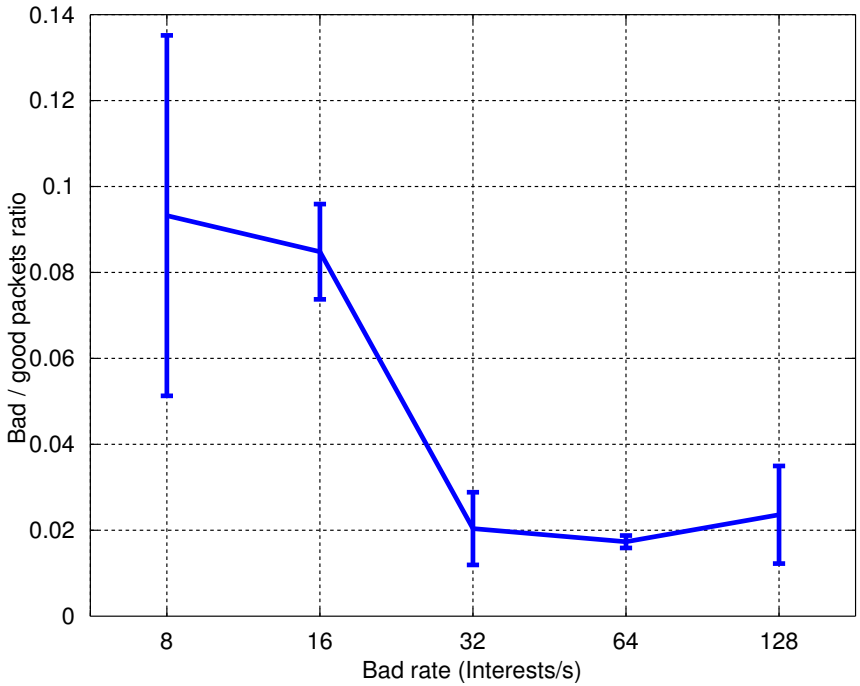
Strong attack footprint (128 Interests/s)

Orchestration and mitigation

- Overall mitigation evaluation [ongoing work]



Average mitigation delay according to the attack rate



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

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

Systematic
Paris Region Systems & ICT Cluster

Agence Nationale de la Recherche
ANR

Questions ?

orange™

THALES

montimage

Loria
Laboratoire lorrain de recherche en informatique et ses applications

utt
université de technologie Troyes

References

1. M. Vahlenkamp, F. Schneider, D. Kutscher and J. Seedorf, "Enabling Information Centric Networking in IP Networks Using SDN," *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Trento, 2013, pp. 1-6.
2. S. Salsano, N. Blefari-Melazzi, A. Detti, G. Morabito, L. Veltri, "Information centric networking over SDN and OpenFlow: Architectural aspects and experiments on the OFELIA testbed", Computer Networks, Volume 57, Issue 16, 13 November 2013, Pages 3207-3221, ISSN 1389-1286
3. N. L. M. van Adrichem and F. A. Kuipers, "NDNFlow: Software-defined Named Data Networking," *Network Softwarization (NetSoft), 2015 1st IEEE Conference on*, London, 2015, pp. 1-5.
4. X. N. Nguyen, D. Saucez and T. Turletti, "Efficient caching in content-centric networks using OpenFlow," *INFOCOM, 2013 Proceedings IEEE*, Turin, 2013, pp. 1-2.
5. Peyman TalebiFard, Ravishankar Ravindran, Asit Chakraborti, Jianli Pan, Anu Mercian, Guoqiang Wang, Victor C.M. Leung, "An Information Centric Networking approach towards contextualized edge service," *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, 2015, pp. 250-255.
6. Pedro Henrique V. Guimaraes, Lyno Henrique G. Ferraz, Joao Vitor Torres, Diogo M. F. Mattos, Andres F. Murillo P., Martin E. Andreoni L., Igor D. Alvarenga, Claudia S. C. Rodrigues, Otto Carlos M. B. Duarte, “Experimenting Content-Centric Networks in the Future Internet Testbed Environment”, ICC 2013 Workshops, IEEE, 2013.
7. Salvatore Signorello, Radu State, Jérôme François, Olivier Festor:NDN.p4: Programming information-centric data-planes. NetSoft 2016: 384-389

Related Project publications

[NOMS 2018] Hoang Long Mai, Tan Nguyen, Guillaume Doyen, Rémi Cogranne, Wissam Mallouli, Edgardo Montes de Oca, Olivier Festor. Towards a Security Monitoring Plane for Named Data Networking and its Application against Content Poisoning Attack. To appear in NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium

[IM 2017] Tan N. Nguyen, Xavier Marchal, Guillaume Doyen, Thibault Cholez, Rémi Cogranne. Content Poisoning in Named Data Networking: Comprehensive characterization of real deployment. IM 2017: 72-80

[ICN 2016] 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. ICN 2016: 225-226

[IM 2015] Tan N. Nguyen, Rémi Cogranne, Guillaume Doyen. An optimal statistical test for robust detection against interest flooding attacks in CCN. IM 2015: 252-260

[WIFS 2015] Tan N. Nguyen, Rémi Cogranne, Guillaume Doyen, Florent Retraint: Detection of interest flooding attacks in Named Data Networking using hypothesis testing. WIFS 2015: 1-6