TELECOM SudParis

Une école de l'IMT

Building Security Services on top of SDN

Gregory Blanc
Télécom SudParis, IMT

3rd FR-JP Meeting on Cybersecurity – WG7
April 25th, 2017 – Keio University Mita Campus, Tokyo

Table of Contents

1 SDN and NFV as 5G Enablers

2 SDN-based Security

3 Challenges

4 IMT Cybersecurity Platform

Table of Contents

1 SDN and NFV as 5G Enablers

2 SDN-based Security

3 Challenges

4 IMT Cybersecurity Platform

5G: New Generation Mobile Networks

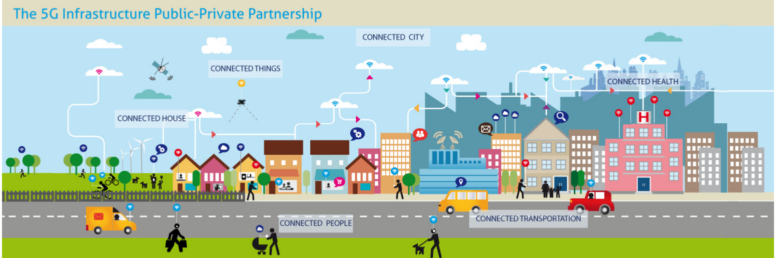
As per the 5G Infrastructure PPP Vision [1], 5G capabilities will provide:

- wide range of applications and services
- increased resilience and continuity
- much higher resource efficiency
- security and privacy protection
- enormous capacity improvements
- user data rates boost

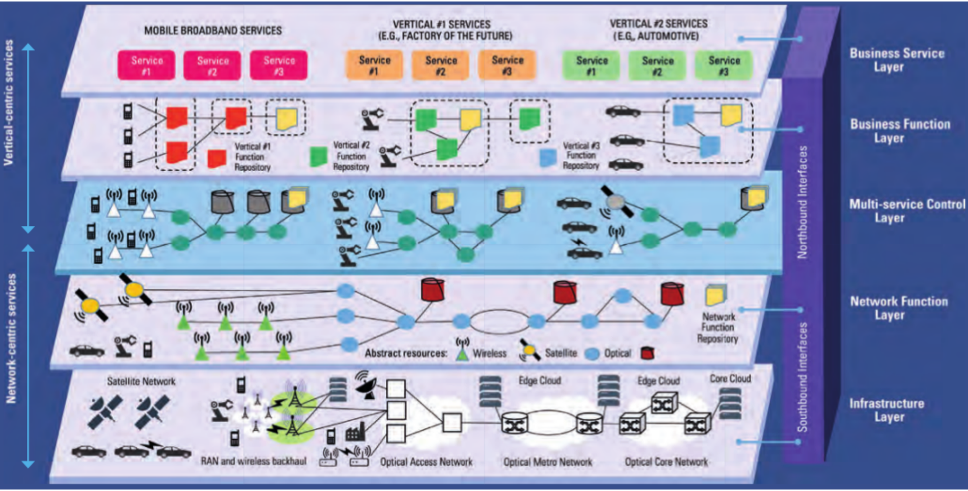
5G: Empowering Vertical Markets

5G vertical sectors (Automotive, eHealt, Energy, Factories, Media & Entertainment) require additional capabilities [2]:

- **Data rate:** in the order of Gb/s
- **Mobility (speed):** in the order of 500km/h
- **E2E latency:** minimum values of 100μs to 10ms
- **Density (number of devices):** up to 100 per m^2
- **Reliability:** up to 99.99999%
- **Position accuracy (location):** in the order of 0.3m



5G: Integrated Architecture [2]



Softwarization/Virtualization: Key Enabler

Software-Defined Networking (SDN)

- proposes logical centralization of control functions
- relies on advances in server scale out and cloud technologies

Network Functions Virtualization (NFV)

- leverages recent advances in server and enterprise IT virtualization

Softwarization/Virtualization: Key Enabler

Software-Defined Networking (SDN)

- proposes logical centralization of control functions
- relies on advances in server scale out and cloud technologies

Network Functions Virtualization (NFV)

- leverages recent advances in server and enterprise IT virtualization

- More flexibility and tighter integration with infrastructure layers

Softwarization/Virtualization: Key Enabler

Software-Defined Networking (SDN)

- proposes logical centralization of control functions
- relies on advances in server scale out and cloud technologies

Network Functions Virtualization (NFV)

- leverages recent advances in server and enterprise IT virtualization

- More flexibility and tighter integration with infrastructure layers
- Further investigation needed in terms of performance and scalability

Softwarization/Virtualization: Key Enabler

Software-Defined Networking (SDN)

- proposes logical centralization of control functions
- relies on advances in server scale out and cloud technologies

Network Functions Virtualization (NFV)

- leverages recent advances in server and enterprise IT virtualization

- More flexibility and tighter integration with infrastructure layers
- Further investigation needed in terms of performance and scalability
- Essentially not networking technologies

Softwarization/Virtualization: Key Enabler

Software-Defined Networking (SDN)

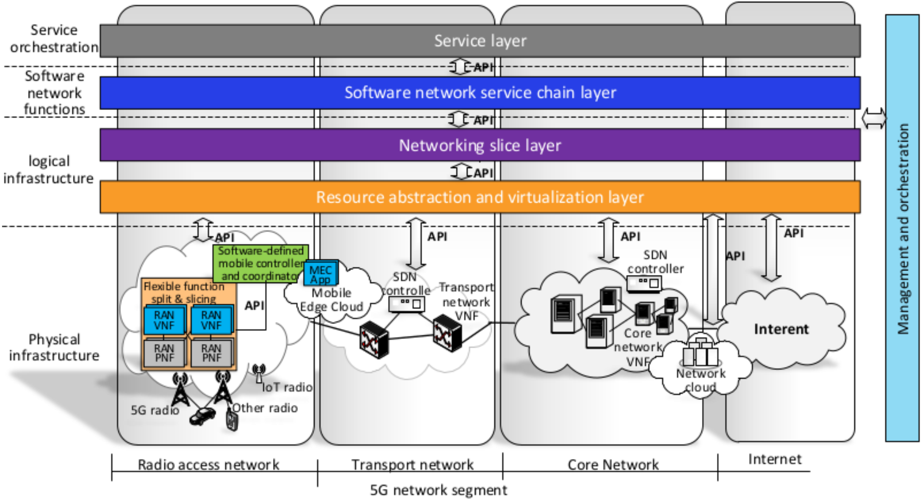
- proposes logical centralization of control functions
- relies on advances in server scale out and cloud technologies

Network Functions Virtualization (NFV)

- leverages recent advances in server and enterprise IT virtualization

- More flexibility and tighter integration with infrastructure layers
- Further investigation needed in terms of performance and scalability
- Essentially not networking technologies
- Need for a unified control for multi-tenant networks and services

Softwarization in 5G [3]



Virtualized (Security) Functions

Security services being brought up thanks to (virtualized) functions.

Replacing the dedicated physical middlebox to which traffic was steered:

1. an on-demand cloud service to which traffic is steered
2. a virtualized network function instantiated on the path
3. an SDN application on top of the SDN controller
4. flow rules to be distributed to the SDN switch

Table of Contents

1 SDN and NFV as 5G Enablers

2 SDN-based Security

3 Challenges

4 IMT Cybersecurity Platform

Leveraging SDN Features to Build Security Functions

Mainly, decoupling the control plane from the data plane introduced flexibility and granularity in dealing with policy enforcement

A few other features allow to easily integrate security in the network where access control and routing are now distinct:

1. built-in monitoring features allow to assess the network status
2. centralized visibility could be utilized for event correlation
3. northbound interface enables network control for security functions
4. data plane programmability enables reconfiguration to enhance resilience

Further developments are still needed to achieve autonomic security and policy-based network management.

Building SDN-based Security Functions: Feasibility [4]

Goal: break out from inflexible middleboxes' constraints.

Requirements and challenges include:

- avoid adding a third-party device
- reduce collateral damage (CPU/memory overhead at data plane)
- avoid security inherent to SDNs

Major insights

1. Need to reduce control messages overhead
2. Possibility to implement applications that leverage network status
3. Take into account data plane capacities when designing functions
4. Security often impacts SDN performance
5. Some functions may benefit from hardware-based processing
6. NFV is recommended for hardware-independent security functions

Autonomous Security: DDoS mitigation [5]

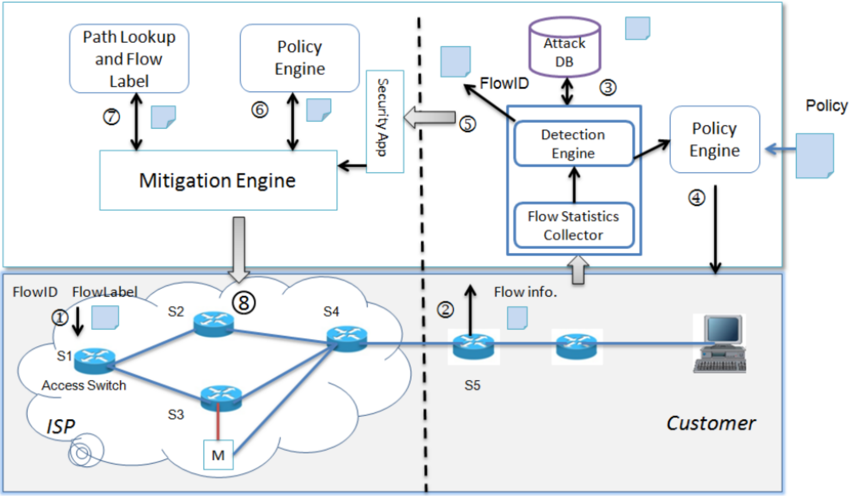


Table of Contents

1 SDN and NFV as 5G Enablers

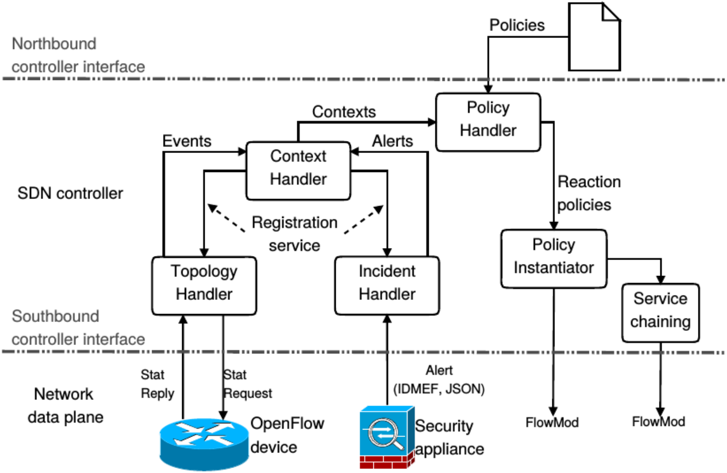
2 SDN-based Security

3 Challenges

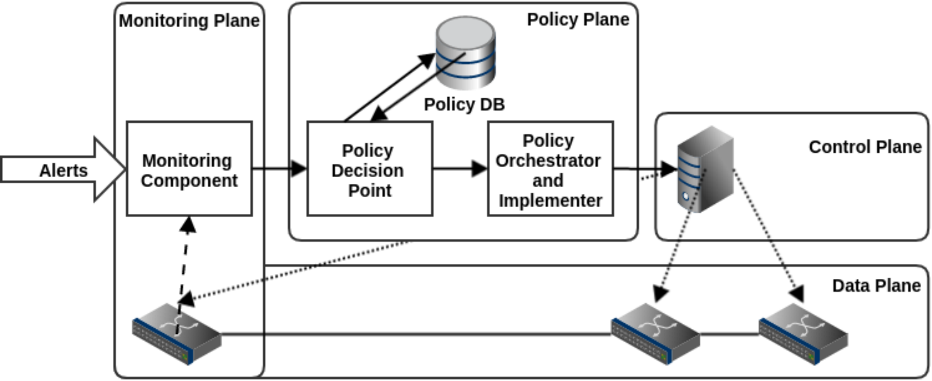
4 IMT Cybersecurity Platform

Network Security Monitoring

Courtesy of N. Kheir



Autonomous Context-Aware Policy Management [6]



Isolation and Secure Migration of Network Topologies [7]

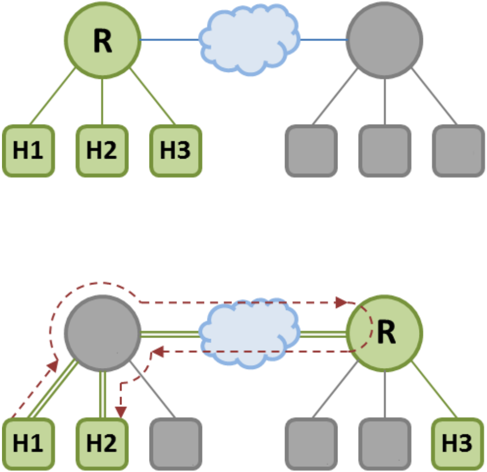


Table of Contents

1 SDN and NFV as 5G Enablers

2 SDN-based Security

3 Challenges

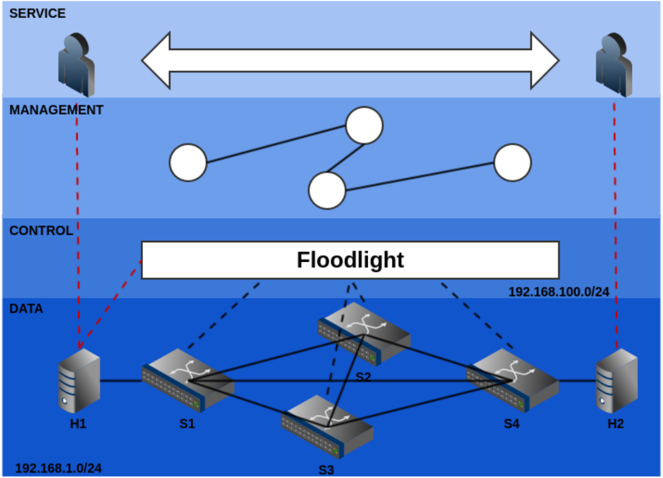
4 IMT Cybersecurity Platform

Testbed Resources

The testbed is a virtualization platform that incorporates:

- a switching fabric: 9 OpenFlow switches with 24 to 48 GbE ports
  - organized in a mesh network
  - highly connected with the VM hosting cluster
  - instantiating one or many logical switches
- a VM hosting cluster: 10 hosts powered with 8-core 2.9GHz CPUs, at least 16GB RAM and 10GbE NICs
  - controlled by VMWare vSphere through ESXi clients
  - accessible through vSphere clients (either local or Web-based)
  - able to instantiate a number of machines, either for network control or service provision

Testbed Actual Deployment



Towards an SDN-based Security Testbed

Ongoing improvements:

- deployment of secure access technologies
- migration to opensource software (OpenStack, ONOS, ODL)
- integration of compute/storage orchestration (OpenStack) with network control (ONOS/ODL)

Foreseen improvements:

- design and implementation of a newtork hypervisor to provide virtual SDNs

Let’s discuss!

Thank you for your attention!

Contact: gregory.blanc@telecom-sudparis.eu

References I

[1] 5G Vision.
Technical report, 5G PPP, 2015.
Available at: http://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf.

[2] 5G empowering vertical industries.
Technical report, 5G PPP, 2016.
Available at: https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf.

[3] View on 5G Architecture.
Technical report, 5G PPP, 2016.
Available at: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-July-2016.pdf.

[4] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, and Z. Zhang.
Enabling security functions with SDN: A feasibility study.
Computer Networks, 85:19–35, 2015.

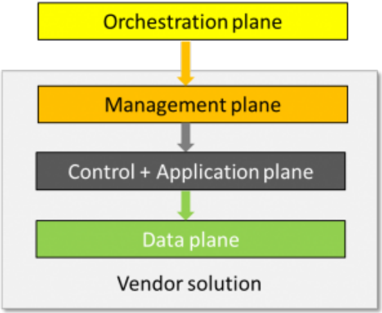
References II

[5] R. Sahay, G. Blanc, Z. Zhang and H. Debar.
Towards Autonomic DDoS Mitigation using Software Defined Networking.
In *2015 NDSS Workshop on Security of Emerging Network Technologies*, 2015.

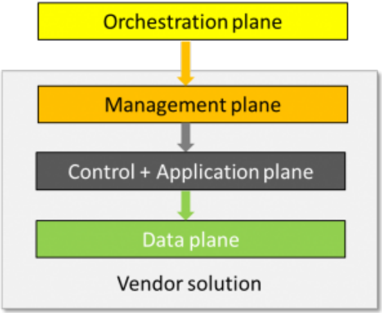
[6] R. Sahay, G. Blanc, Z. Zhang, K. Toumi and H. Debar.
Adaptive Policy-driven Attack Mitigation in SDN.
In *Workshop on Security and Dependability of Multi-Domain Infrastructures*, 2017.

[7] S. Ghorbani, C. Schlesinger, M. Monaco, E. Keller, M. Caesar, J. Rexford and D. Walker.
Transparent, Live Migration of a Software-Defined Network.
In *5th ACM Symposium on cloud Computing*, 2014.

Software-Defined Networking

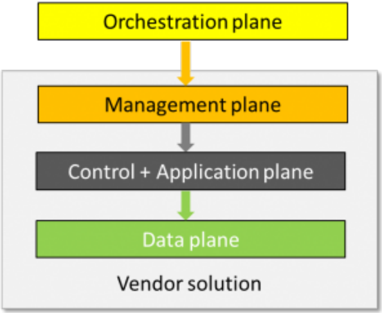


Software-Defined Networking



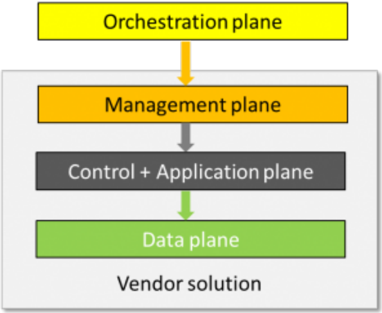
- segregation of the data plane and the control plane

Software-Defined Networking



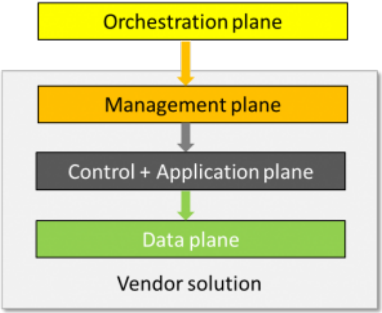
- centralized network control and visibility
- segregation of the data plane and the control plane

Software-Defined Networking



- centralized network control and visibility
- segregation of the data plane and the control plane
- programmability of the network forwarding elements

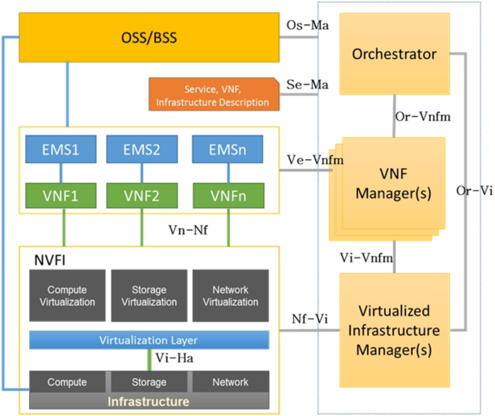
Software-Defined Networking



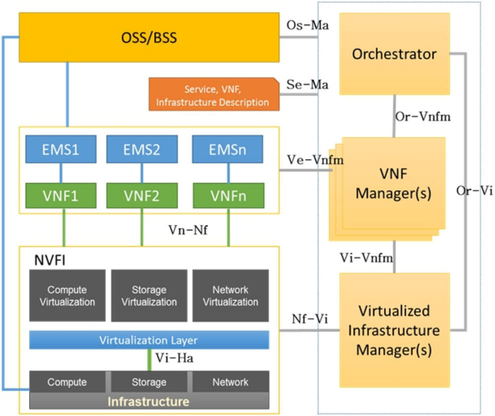
- centralized network control and visibility
- segregation of the data plane and the control plane
- programmability of the network forwarding elements

SDN is not OpenFlow

Network Functions Virtualization



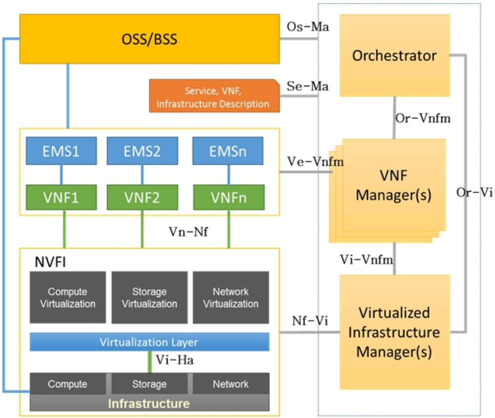
Network Functions Virtualization



Motivation

Reduce deployment costs by reducing reliance on proprietary devices

Network Functions Virtualization



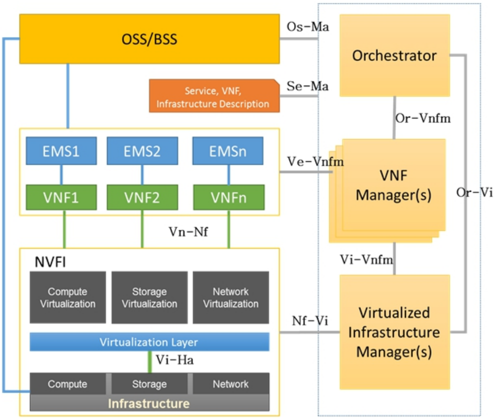
Motivation

Reduce deployment costs by reducing reliance on proprietary devices

Principle

Relocate network functions from dedicated appliances to generic servers

Network Functions Virtualization



Motivation

Reduce deployment costs by reducing reliance on proprietary devices

Principle

Relocate network functions from dedicated appliances to generic servers

Examples of NF: router, gateway, firewall, CDN, WAN accelerator, SLA assurance, etc.