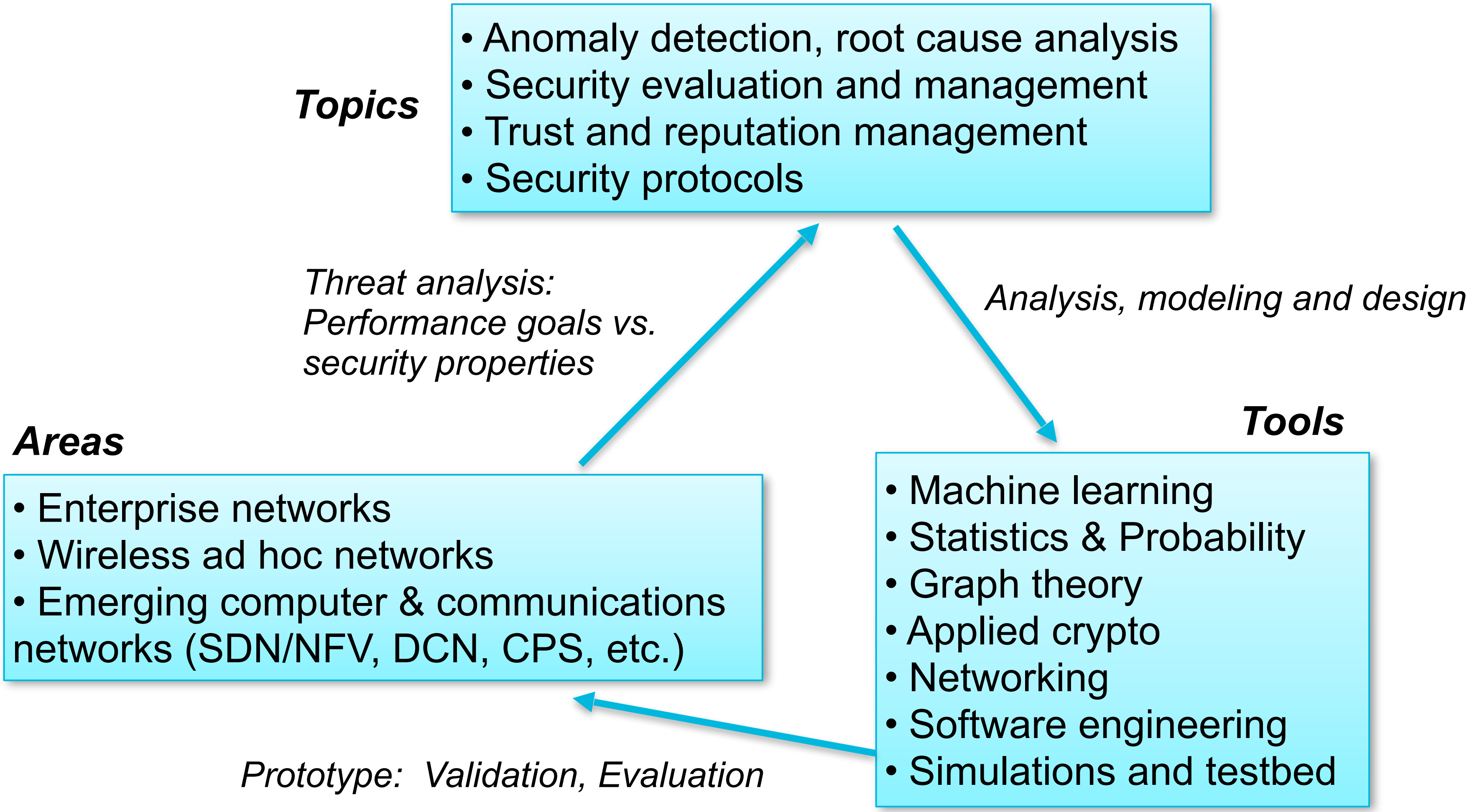
Institut Mines-Télécom

Leveraging SDN & NFV to Achieve Software-Defined Security

Zonghua Zhang

@imt-lille-douai.fr

NEtwork **P**erformance and **S**ecurity **G**roup: **NEPS**



Topics

- Anomaly detection, root cause analysis
- Security evaluation and management
- Trust and reputation management
- Security protocols

Threat analysis: Performance goals vs. security properties

Analysis, modeling and design

Areas

- Enterprise networks
- Wireless ad hoc networks
- Emerging computer & communications networks (SDN/NFV, DCN, CPS, etc.)

Tools

- Machine learning
- Statistics & Probability
- Graph theory
- Applied crypto
- Networking
- Software engineering
- Simulations and testbed

Prototype: Validation, Evaluation

Institut Mines-Télécom

s@movar UMR 5157

IMT Lille Douai
École Mines-Télécom
IMT-Université de Lille

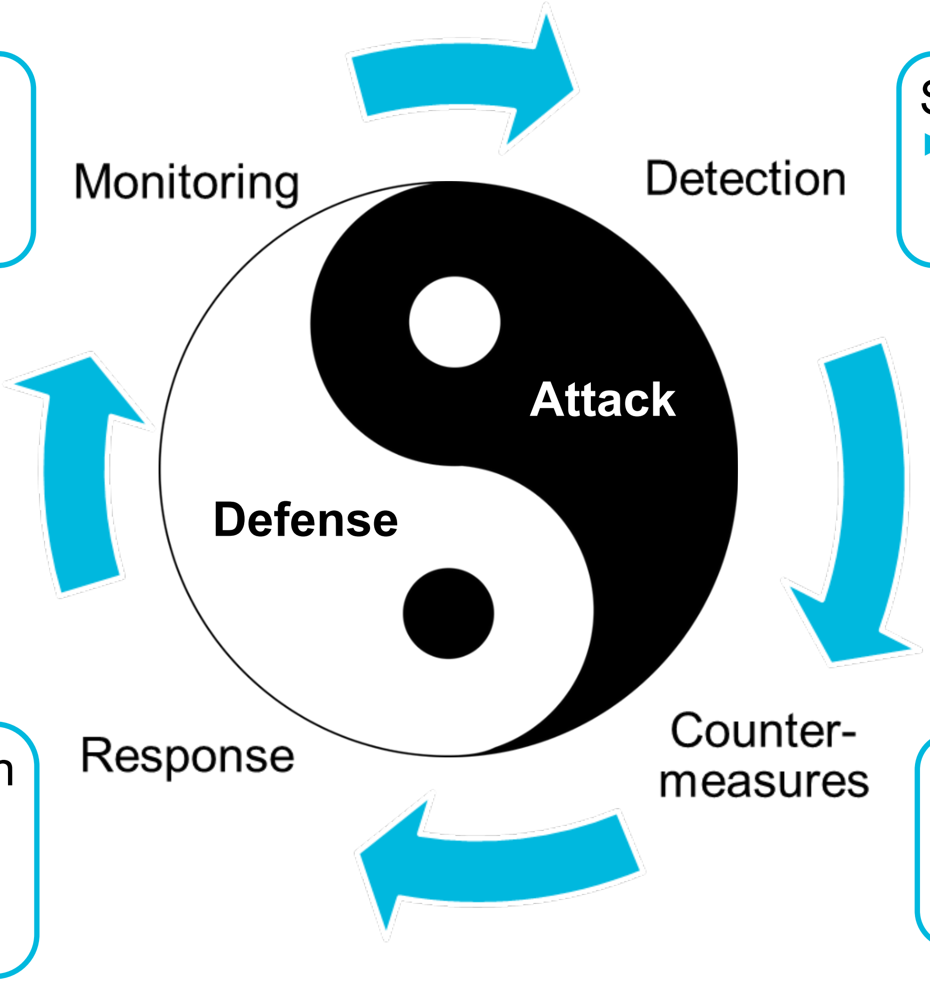
Autonomic Cyberdefense: Mission Impossible ?

Self-Protection

- ▶ Security protocols
- ▶ Trust and reputation system

Self-Optimization

- ▶ Cost-effective security hardening or response



Self-Configuration

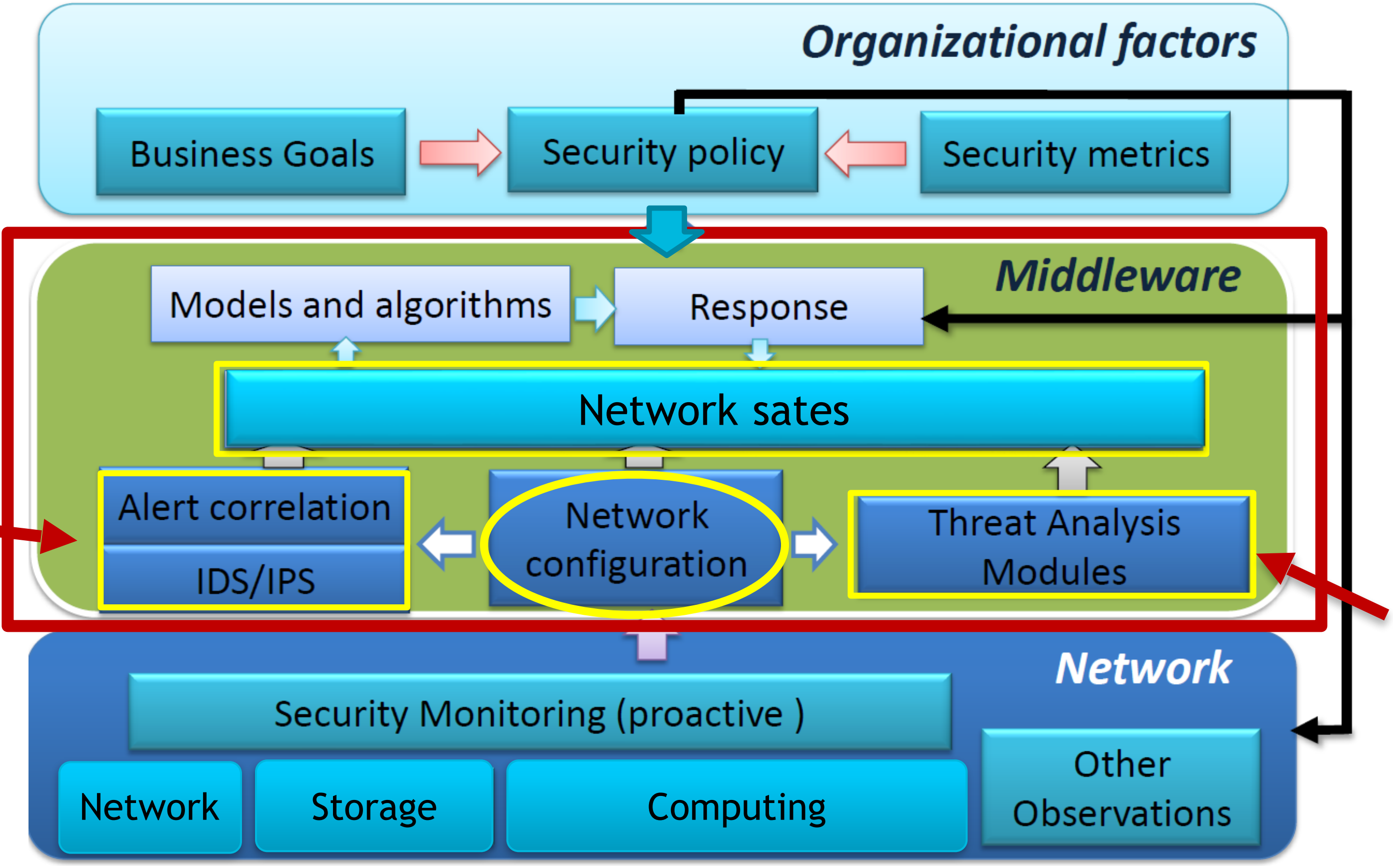
- ▶ Adaptive security policy
- ▶ Self-adaptive software
- ▶ Software-Defined Networking (SDN)

Self-Healing

- ▶ Automated vulnerability analysis and patching

Cost-Effective Security Hardening

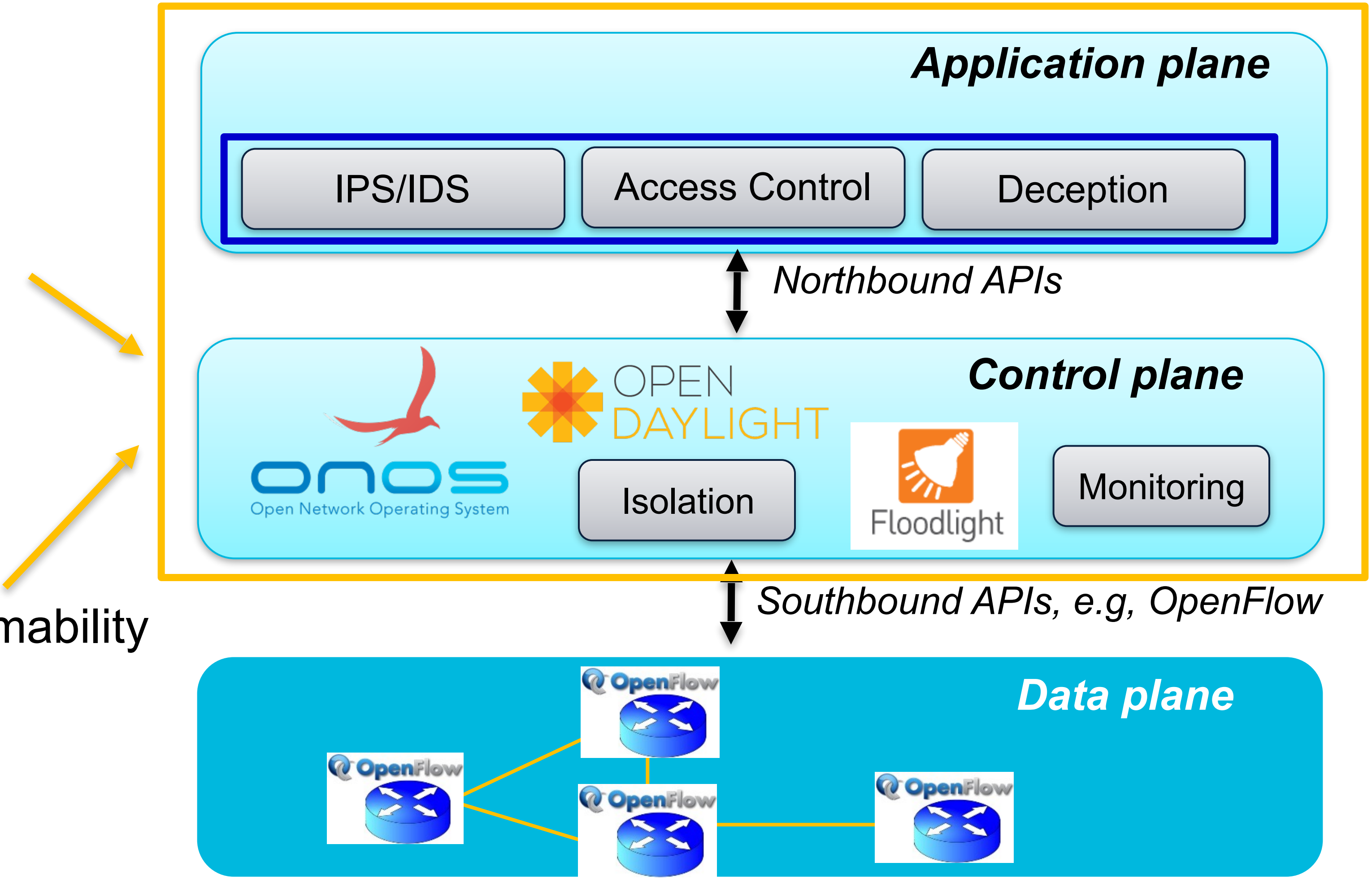
Partially
Observable
Markov
Decision
Process



Attack
Graph
&
Hidden
Markov
Model

- "Exploring attack graph for cost-benefit security hardening: A probabilistic approach," by Shuzhen Wang, Zonghua Zhang, and Youki Kadobayashi, *Computers & Security* 32: 158-169 (2013)
- "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach," by Zonghua Zhang, Pin-Han Ho, Liwen He, *Computers & Security* 28(7): 605-614 (2009)

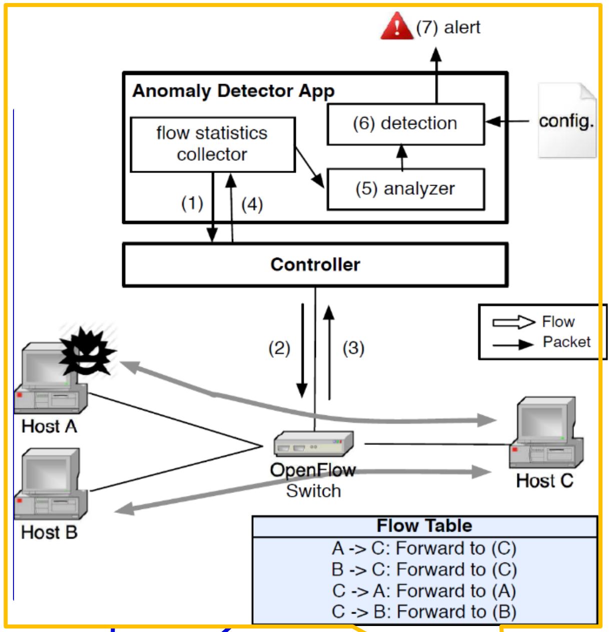
SDN Based Security Management



Global visibility

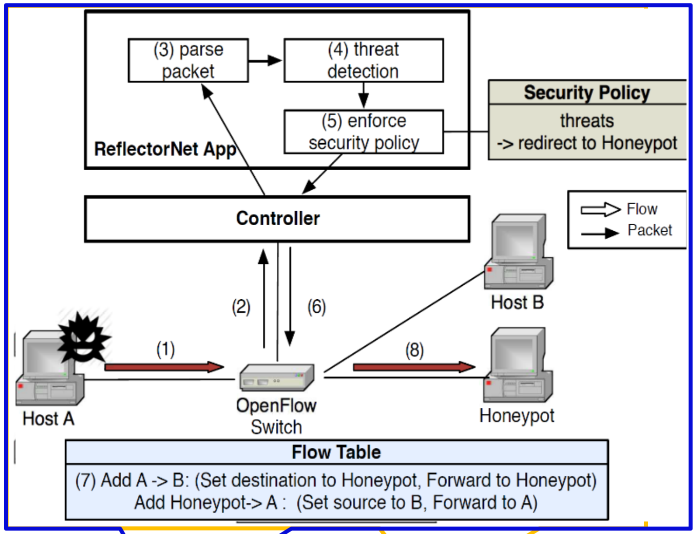
Programmability

SDN Based Security Functions



Flow Table

A -> C: Forward to (C)
B -> C: Forward to (C)
C -> A: Forward to (A)
C -> B: Forward to (B)



Flow Table

(7) Add A -> B: (Set destination to Honeypot, Forward to Honeypot)
Add Honeypot-> A : (Set source to B, Forward to A)

NIPS

Anomaly detector

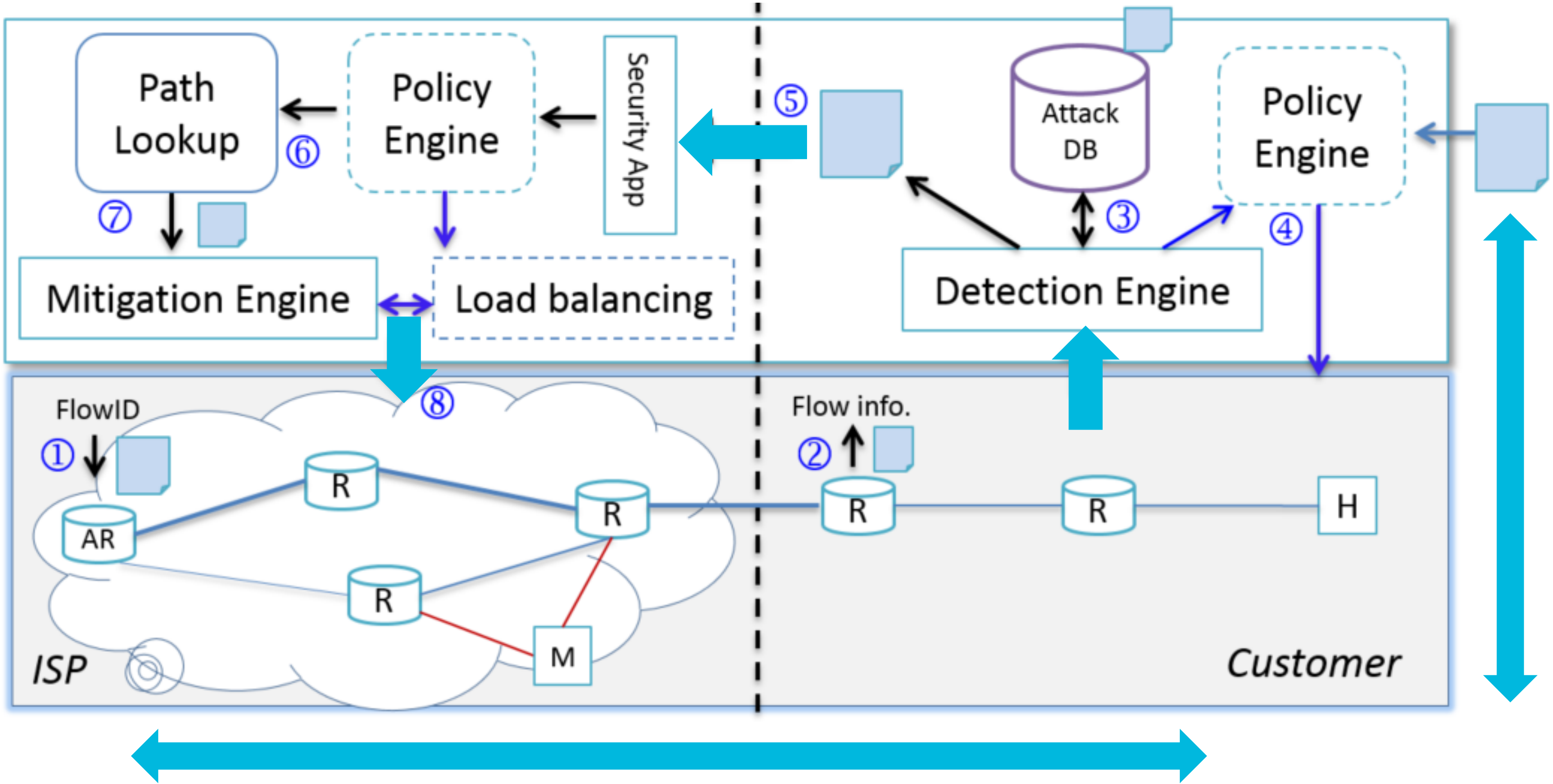
Honeynet

Stateful firewall

- Hardware matters (e.g., multi-port-forwarding, picket header modification)
- Performance bottleneck is due to control messages (packet-in)
- Data plane has a rich set of network status information (SDN as database)

- “Enabling security functions with SDN: A feasibility study,” by Changhoon Yoon, Taejune Park, Seungsoo Lee, Heedo Kang, Seungwon Shin, and Zonghua Zhang, *Computer Networks* 85: 19-35 (2015)

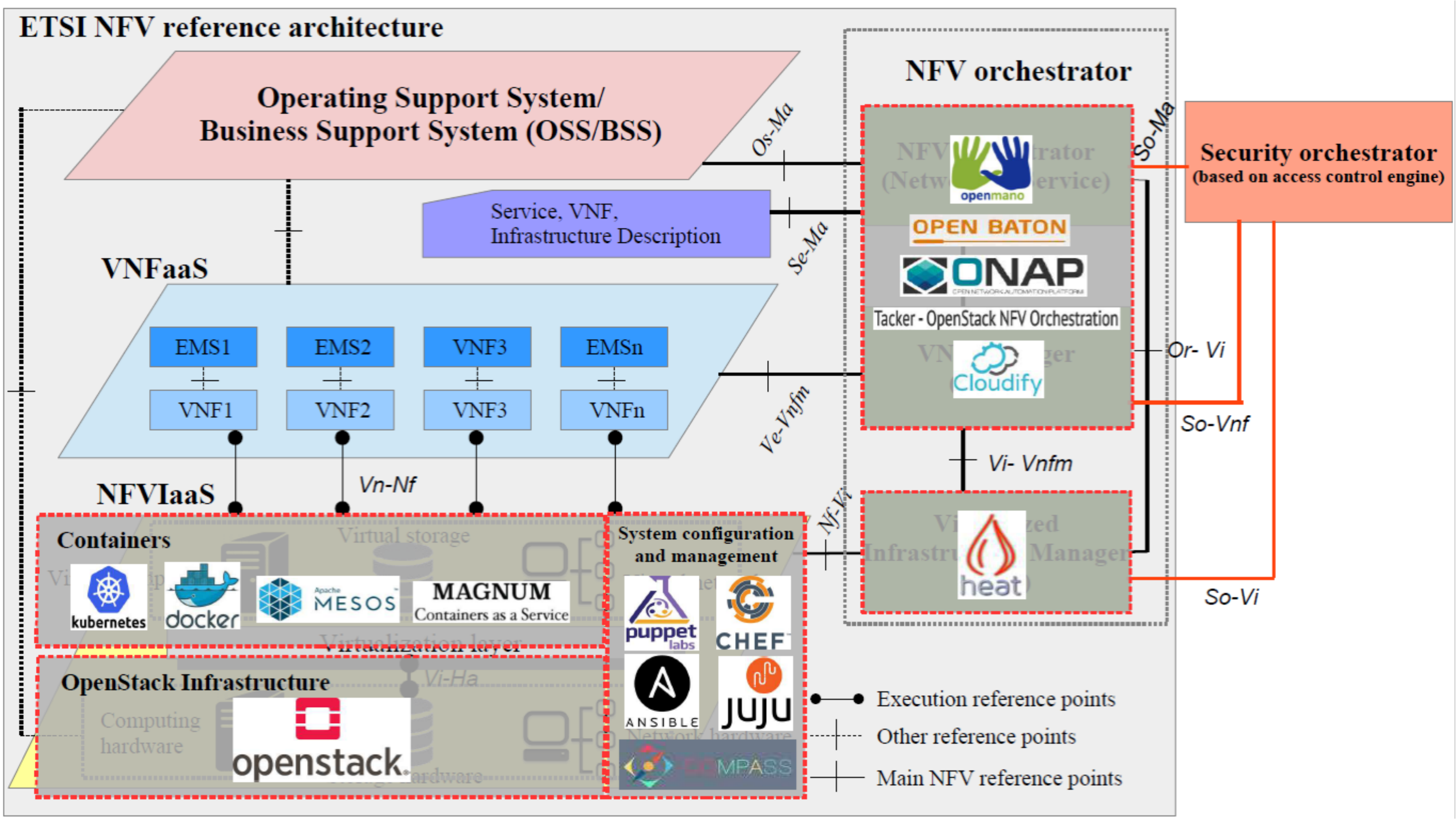
SDN Based DDoS Mitigation



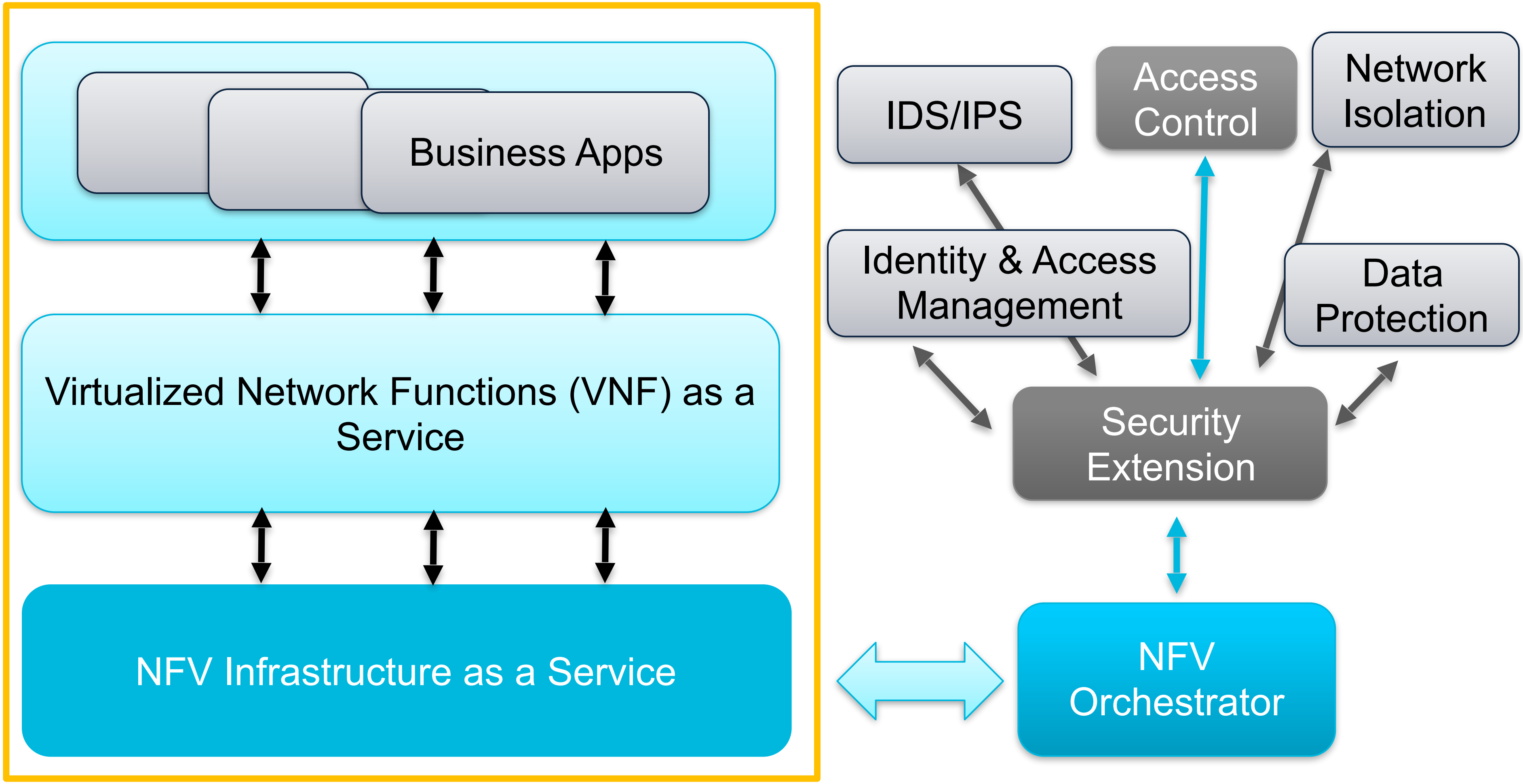
- Collaborative
- On-demand

- "ArOMA: An SDN based autonomic DDoS mitigation framework," by Rishikesh Sahay, Gregory Blanc, Zonghua Zhang, and Hervé Debar, *Computers & Security* 70: 482-499 (2017)

NFV based Security Management and Orchestration

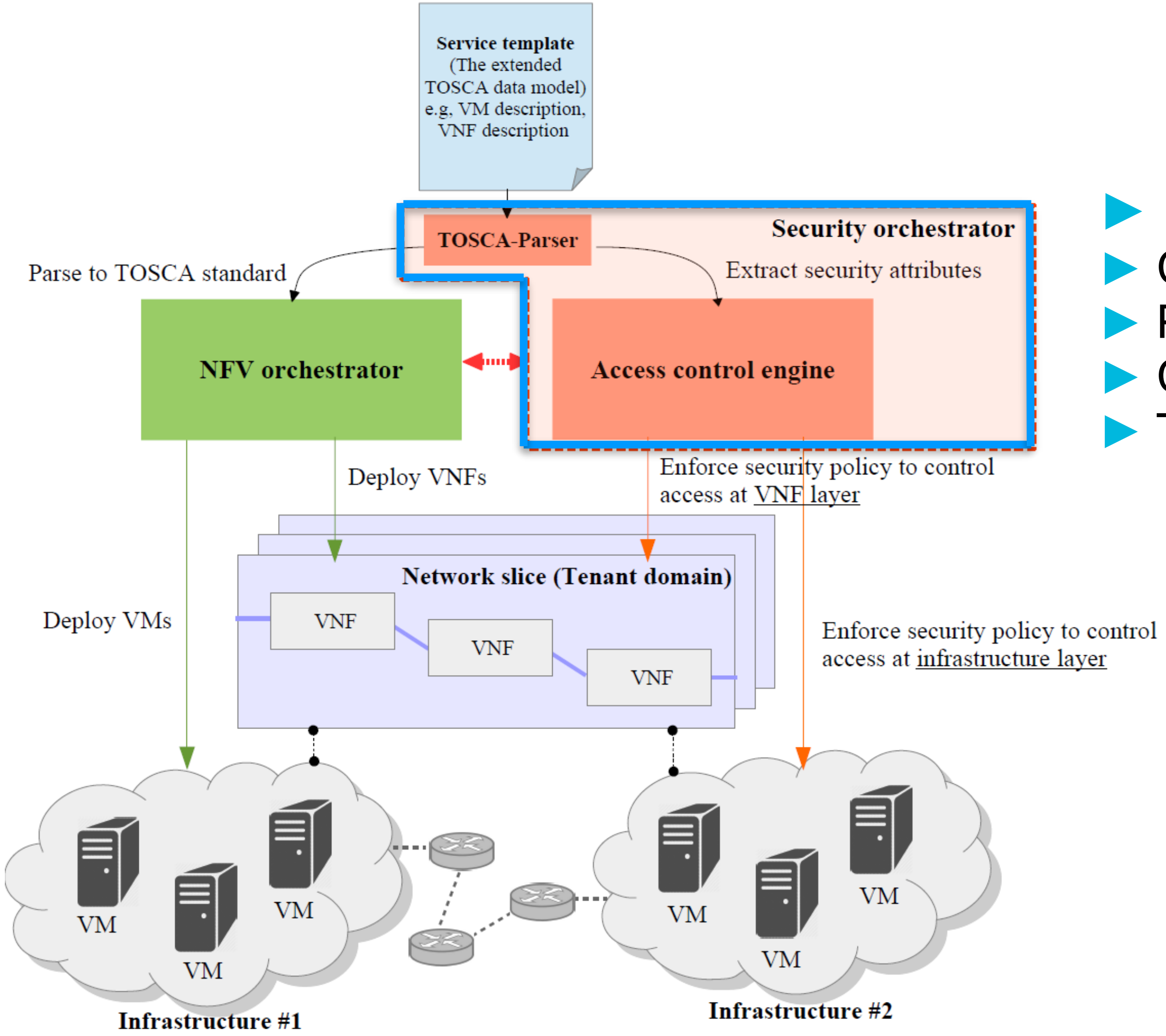


NFV based Security Management and Orchestration


Business Apps
Virtualized Network Functions (VNF) as a Service
NFV Infrastructure as a Service
IDS/IPS
Access Control
Network Isolation
Identity & Access Management
Data Protection
Security Extension
NFV Orchestrator

- **Project SecMANO**: NFV based Security Management and Orchestration, CRE of Orange Labs

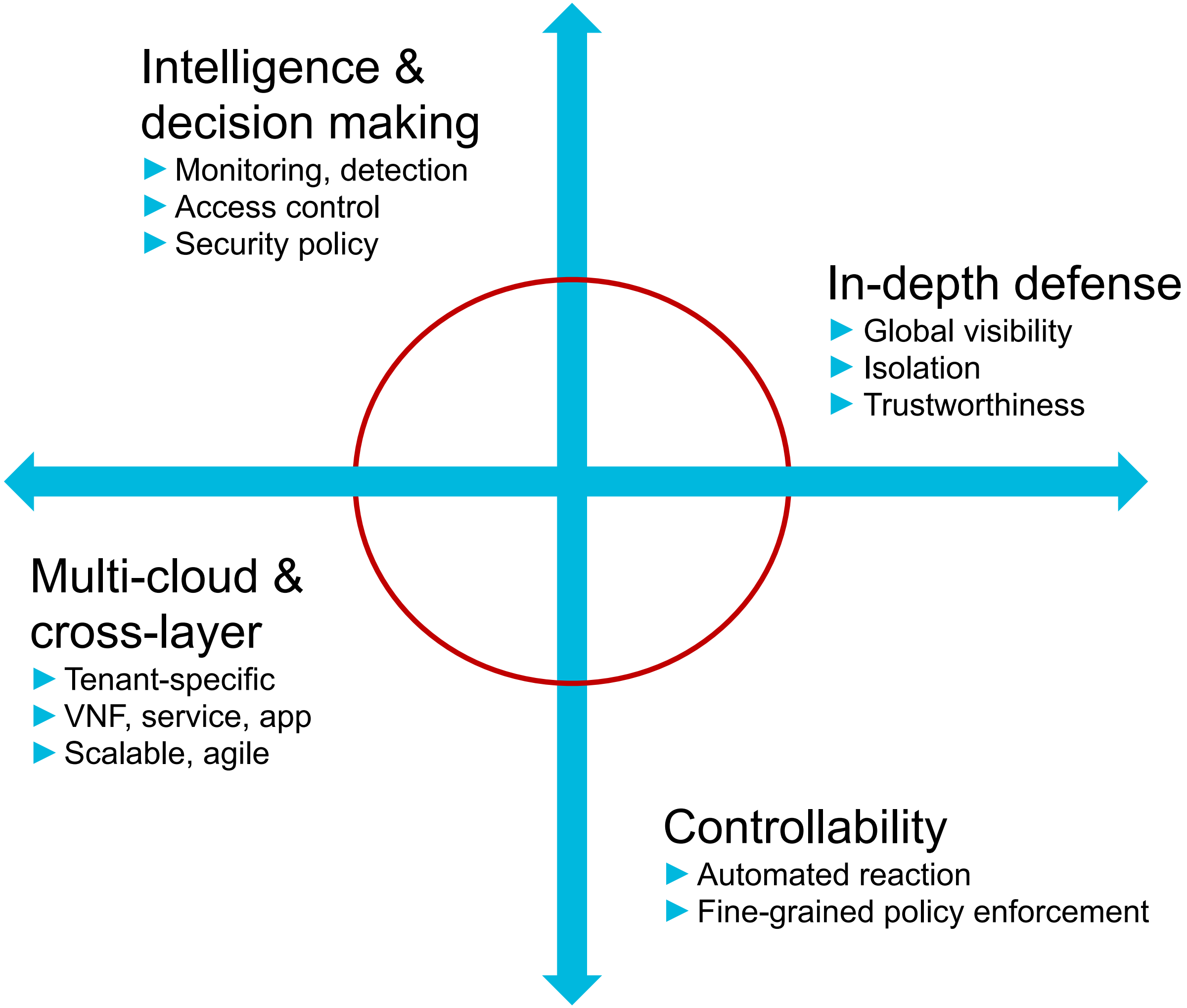
Security Orchestrator



- Policy-driven
- Centralized control
- Programmable
- Cross-layer
- Tenant-specific

- “A First Step Towards Security Extension for NFV Orchestrator,” by Montida Pattaranantakul, Yuchia Tseng, Ruan He, Zonghua Zhang, Ahmed Meddahi, *ACM 2nd Workshop on SDN-NFV Security* (Best paper), March 2017
- “SoDAC: A New Software-Defined Access Control Paradigm for Cloud-based Systems,” by Ruan He, Montida Pattaranantakul, Zonghua Zhang, Thomas Duval, *the 19th international Conference on Information and Communications Security (ICICS)*, Dec. 2017

Perspectives



Intelligence & decision making

- Monitoring, detection
- Access control
- Security policy

In-depth defense

- Global visibility
- Isolation
- Trustworthiness

Multi-cloud & cross-layer

- Tenant-specific
- VNF, service, app
- Scalable, agile

Controllability

- Automated reaction
- Fine-grained policy enforcement

- Open Security Controller, by Huawei, Intel, McAfee etc., https://www.opensecuritycontroller.org/

Institut Mines-Télécom

IMT Lille Douai
École Mines-Télécom
IMT-Université de Lille

Institut Mines-Télécom

Thanks !

Zonghua Zhang

@imt-lille-douai.fr