Zürcher Hochschule
für Angewandte Wissenschaften

zh
aw

Smart MTD in Future Networks: Fundamentals, Optimization and Challenges

Dr. Gürkan Gür

Zurich University of Applied Sciences (ZHAW)

May 2025

International Workshop on Applications of Moving Target Defense 2025

Keynote Talk

NATWORK

Co-funded by the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

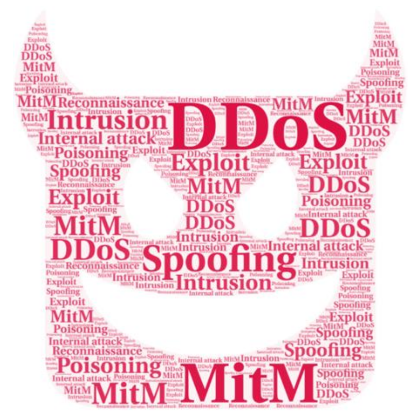
Introduction

The security of communication networks faces challenges

- ❑ Increase in size and complexity
  - Physical and virtual space intersection increase
  - Greater attack surface (*e.g.*, IoT, edge nodes, IaaS)

- ❑ ↑ attack surface ⇒ ↑ attack success probability (*e.g.*, malware propagation, larger botnets)
- ❑ More impactful attacks (*e.g.*, DDoS)

Moving Target Defense (MTD) executed in a smart and efficient way is crucial to tackle these security problems.



Moving Target Defense (MTD) – Basics (1)

MTD aims at modifying (parts of) the infrastructure or their fingerprint to make it hard for an attacker to execute precision strikes on specific vulnerabilities.

↓

Make life much harder for the attacker!

↓

This approach mitigates the asymmetrical advantage of attackers to perform reconnaissance, learn about the targeted systems and exploit related vulnerabilities.

- An additional layer of defense

MTD – Basics (2)

Such parts could be

- **the network** (e.g., its topology to make eavesdropping on specific traffic difficult)

- **technology stack** (e.g., the network equipment that processes a packet to make it hard for an attacker to execute precision strikes on specific vulnerabilities)

- **execution environment** (e.g., randomize the underlying VM technology on which a certain service runs when an instance is started)

- **the software** (e.g., use different implementations of the same functionality)

MTD – Three Main Questions

A decision-making problem:

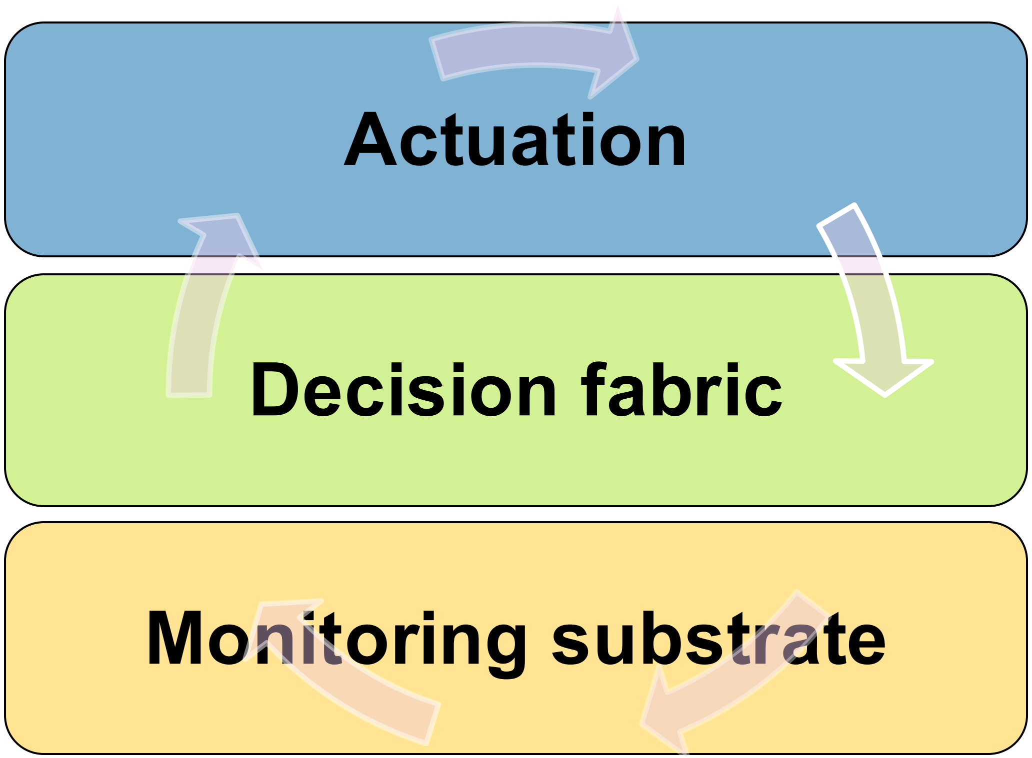
- **What to move**
  - Instruction sets, address space layouts, IP/port numbers, OSs, proxies, ...
- **How to move**
  - Artificial diversity, randomizations
    - Shuffling, redundancy and diversity [11]
- **When to move**
  - Proactive, reactive, hybrid

Cognitive Loop for MTD

- Define a closed-loop key phases, steps, and elements required to manage and enforce MTD actions in a network

[IEEE Comm. Std. Mag. 2021]

Blueprint for MTD



DIVERGENCE -> But Why AI/ML? Benefits

- More effective and efficient security solutions in the cognitive network management;
- Predictive or proactive security functions in the anticipatory networking context;
- Capabilities to cope with a massively increased complexity in 6G (even 5G) network;
- More robust decisions compared to conventional schemes with fewer measurements during inference stages;
- Inherent support for network automation and ZSM from the security perspective.

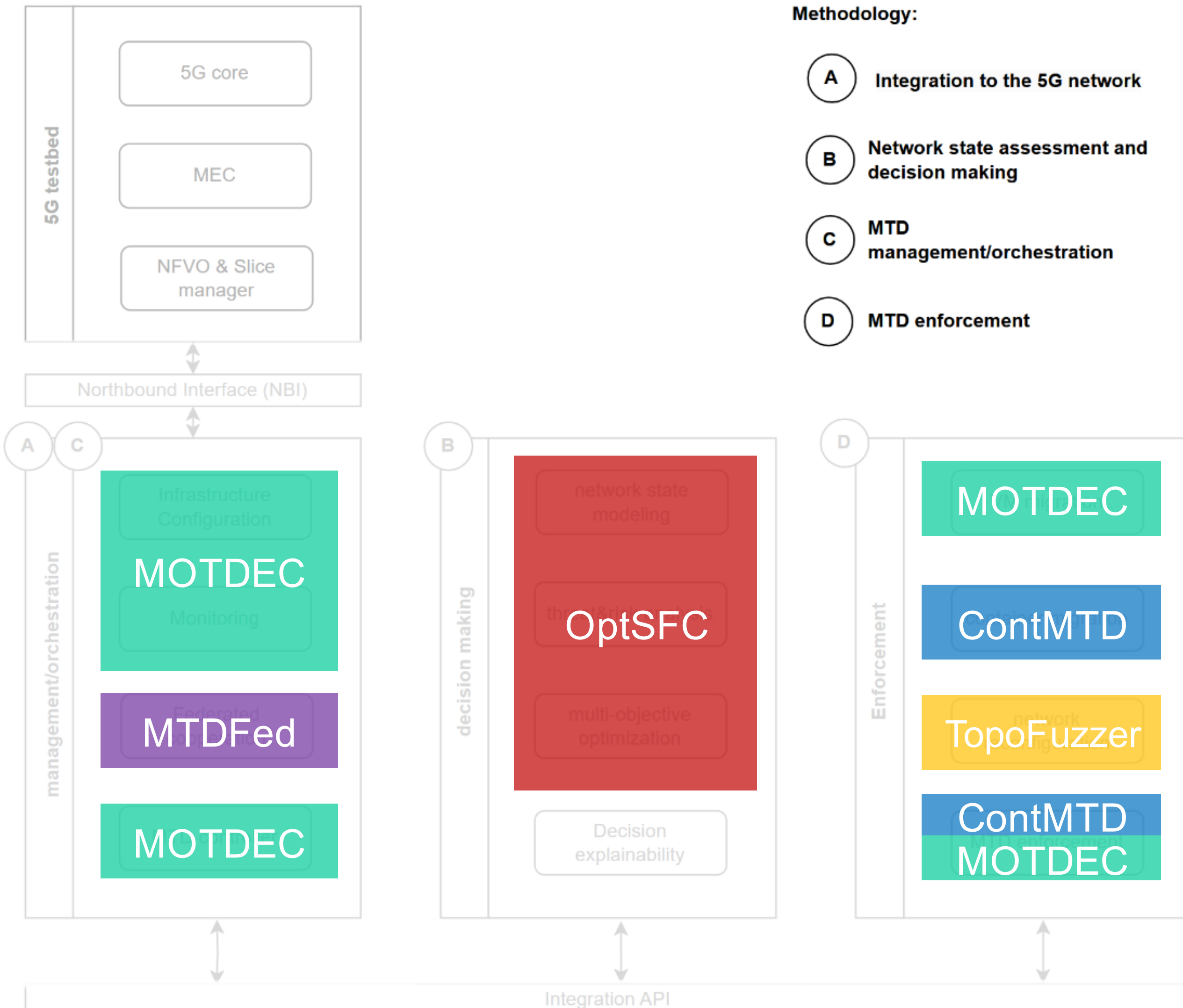
MERLINS

- **MERLINS** defines a pathway for the application of efficient and context-aware MTD actions in Telco Cloud networks
  - A Closed-loop Methodology for MTD enforcement and management
  - High Level Architecture needed to make an MTD framework
  - Integrated solutions designed and developed for MTD enforcement in 5G and MTD strategy optimization

> - **Prevent** & **mitigate** attacks using MTD
> - Exploit **virtualization** and **SDN** for efficient MTD
> - **Optimize** MTD strategies with **AI/ML**

Based on PhD work by W. Soussi (UZH, ZHAW)

MERLINS Framework



Methodology:

- **A** Integration to the 5G network
- **B** Network state assessment and decision making
- **C** MTD management/orchestration
- **D** MTD enforcement

MERLINS Components

- MOTDEC implements IPv6 and port shuffling, VNF reinstantiation, and stateless VNF live migration as MTD actions
  - Integrated with the NFV, Scalable for MEC, near real-time sync

[IEEE Comm. Std. 2021]
[IEEE NFV/SDN 2023]
[IEEE CSR 2024]

- ContMTD provides stateful live migration (LiMi) for CNFs
  - Optimized for parallel LiMi and heterogeneous service loads

[IEEE ICC 2025]
[ACM Computing Surveys]
(Sigcomm 2025 submission)

- TopoFuzzer introduces a seamless session handover in traffic redirection for MTD requirements
  - Enabled TCP and QUIC session handover for moving servers

[IEEE NOMS 2023]

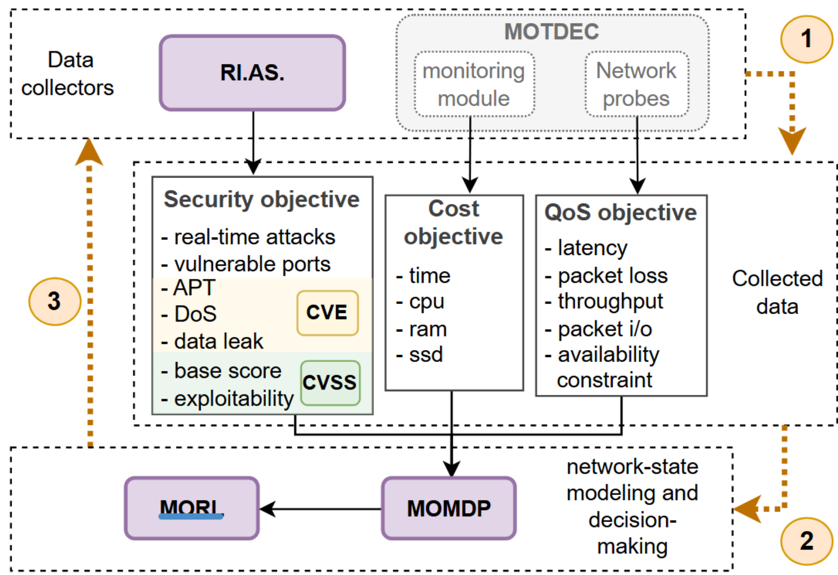
- OptSFC optimizes MTD strategies for Security, QoS, and Costs
  - Modelling the network state into a multi-objective Markov Decision Process (MOMDP), enabling deep-RL and MORL training

[IEEE NFV/SDN 2023]
[IEEE Network 2024]

Optimizing the MTD: OptSFC

- ❑ Multi-Objective Markov Decision Process (MOMDP):
  - Near real-time modeling of the 5G network state
  - Deep-RL model training and decision-making

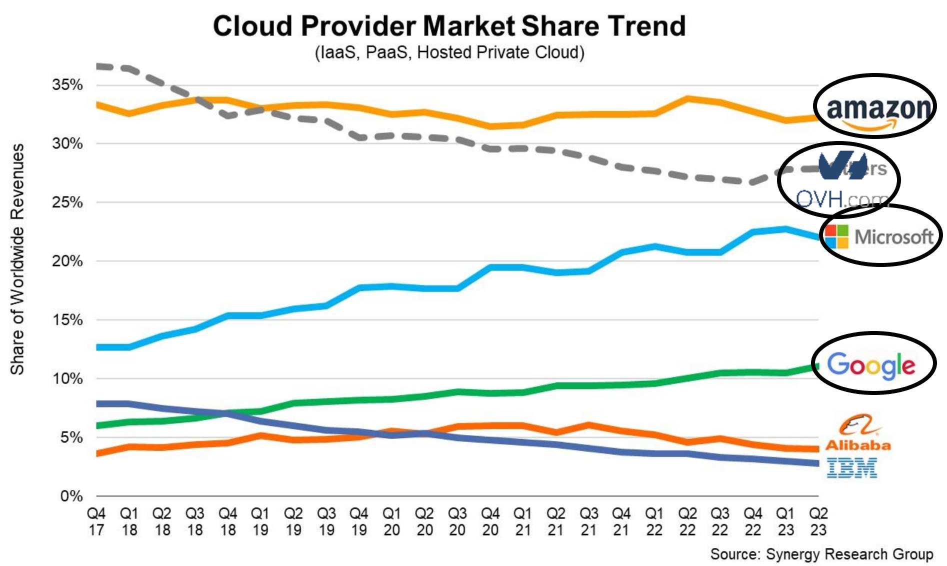
- ❑ Definition of the Deep-RL reward system based on:
  - MTD operational cost (resource consumption metrics)
  - MTD network overhead (QoS metrics)
  - MTD security (attack success probability)



OptSFC – Cost Assessment Module

- ❑ Resources cost function
- ❑ Empirical study of today's cloud resource costs

$$resource_{cost} = \beta + \alpha_1 \times cpu + \alpha_2 \times ram_{gb} + \alpha_3 \times storage_{gb}$$



- ❑ Over 70 VM offers collected from 4 major cloud providers
- ❑ 66% of cloud market share in Q2 2023

	Dependent variable:
	Price ($/hour)
α_1 (CPU_core)	0.031*** (0.001)
α_2 (RAM_GB)	0.004*** (0.0002)
β (constant)	−0.082*** (0.018)
Observations	72
R^2	0.994
Adjusted R^2	0.994
Residual Std. Error	0.127 (df = 69)
F Statistic	5,706.468*** (df = 2; 69)
Note:	*p<0.1; **p<0.05; ***p<0.01

zh aw

OptSFC – Cost Assessment Module (2)

- Resources cost function
- Empirical study of today's cloud resource costs

$$resource_{cost} = \beta + \alpha_1 \times cpu + \alpha_2 \times ram_{gb} + \alpha_3 \times storage_{gb}$$

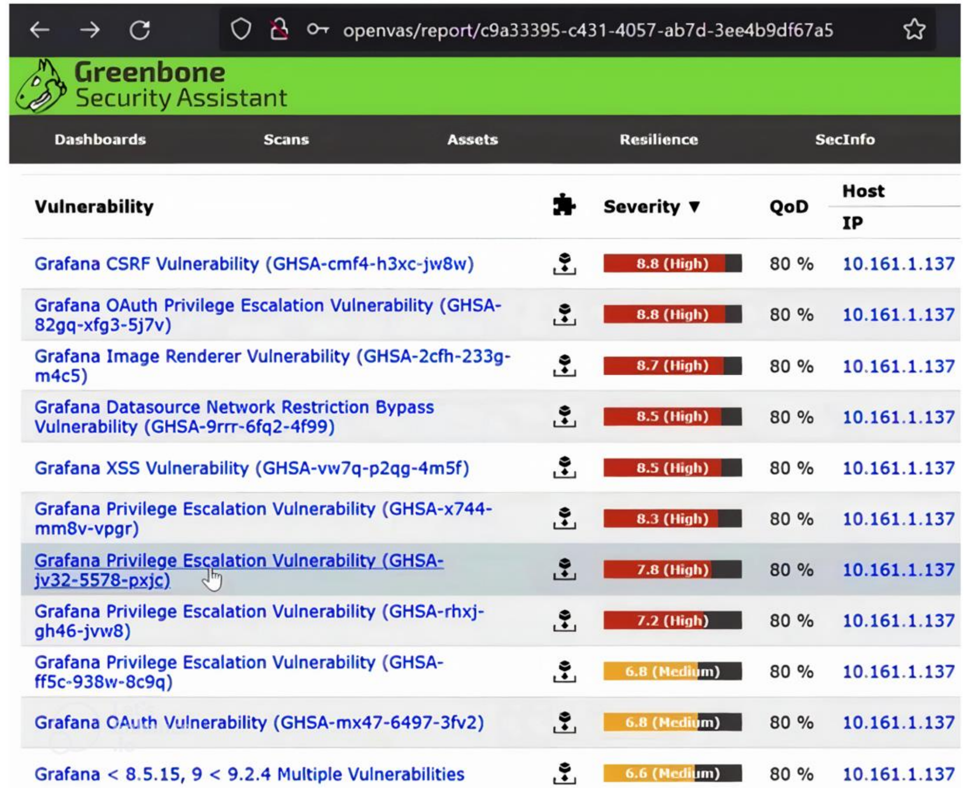
	Dependent variable:
	Price ($/hour)
α_1 (CPU_core)	0.031*** (0.001)
α_2 (RAM_GB)	0.004*** (0.0002)
β (constant)	−0.082*** (0.018)
Observations	72
R^2	0.994
Adjusted R^2	0.994
Residual Std. Error	0.127 (df = 69)
F Statistic	5,706.468*** (df = 2; 69)
Note:	*p<0.1; **p<0.05; ***p<0.01

- Storage prices are defined separately
- Average over the 4 cloud providers:

0.000066 *$/h* per GB

OptSFC – Risk Assessment Module

- Vulnerability scans
  - For all VNFs
  - Every 24h (immediate for new VNFs)
- Risk assessment calculation per VNF based on:
  - Number of CVEs detected
  - CVSS exploitability scores and base scores of CVEs
- External threat landscape not integrated yet

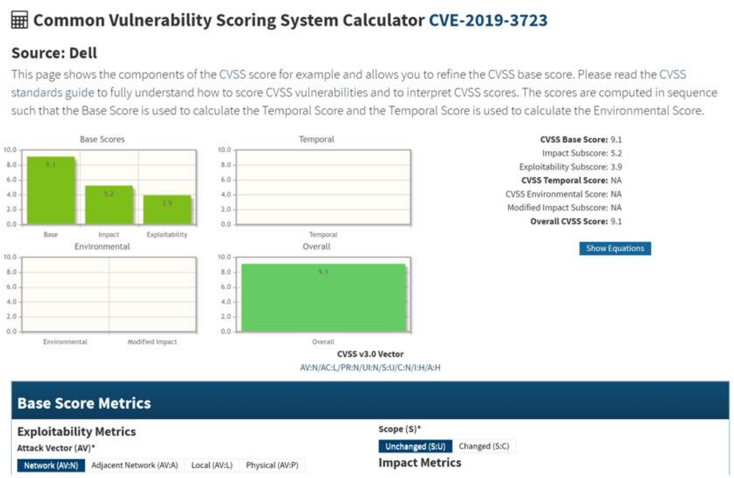


OptSFC – Risk Assessment Module (2)

Risk and threat assessment:

1. Vulnerability scan → 2. Threat evaluation (with CVSS) → 3. LSE estimate per threat

OpenVAS
Open Vulnerability Assessment Scanner



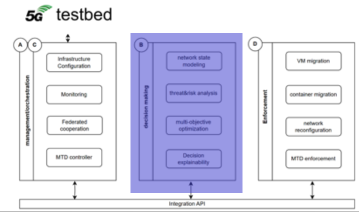
Tampering category vulnerabilities:	CVE-2019-3723	CVE-2021-1106	CVE-2021-1090	AVG
$CVSS_{base}$	9,01	7,8	7,1	7,9
LSE -> (CVSS exploitability)	3,90	1,8	1,8	2,5

OptSFC – Risk Assessment Module (3)

- Vulnerabilities grouped into three types of threat
  - Advanced persistent threat (APTs) → remote code exec and injection flaw
  - Data leak threat → SQL injection, XSS injection, directory traversals, local file inclusion
  - Denial of Service (DoS) threat → buffer overflow and network-based DoS (from active scans)
- Aggregation of the different metrics for the MOMDP security objective

$$sec\_risk = \max_{threat\ t} (ASP_t \times cvss\_score_t) \times vnf\_impact$$

OptSFC – MOMDP



MOMDP represents the networks state as a tuple $(S, A, P, \overline{R}, \gamma)$

- S is the set of all possible states of the network
- A is the set of actions
- P is the transition probability matrix
- $\overline{R}$ is the vector of rewad functions R
- γ is the discount factor

Soft MTD actions:
- IPv6 shuffling
- Port shuffling

Hard MTD actions:
- Stateless LiMi
- Stateful LiMi
- Reinstantiate stateless NF

R_1 Security function

$$sec\_risk = \max_{threat\ t} (ASP_t \times cvss\_score_t) \times vnf\_impact$$

R_2 Operational cost function

$$resource_{cost} = \beta + \alpha_1 \times cpu + \alpha_2 \times ram_{gb} + \alpha_3 \times storage_{gb}$$

R_3 QoS function

$$mtd\_QoS\_overhead = (1 + p\_loss\_rate\_increase) \times latency\_increase$$

For each VNF:
- status (run, idle, soft stop, accidental stop)
- resource consumption
- network traffic
- anomaly detection alerts

MERLINS Components

MERLINS

- **MOTDEC** implements IPv6 and port shuffling, VNF reinstantiation, and stateless VNF live migration as MTD actions
  - Integrated with the NFV, Scalable for MEC, near real-time sync

[IEEE Comm. Std. 2021]
[IEEE NFV/SDN 2023]
[IEEE CSR 2024]

- **ContMTD** provides stateful live migration (LiMi) for CNFs
  - Optimized for parallel LiMi and heterogeneous service loads

[IEEE ICC 2025]
[ACM Computing Surveys]
(Sigcomm 2025 submission)

- **TopoFuzzer** introduces a seamless session handover in traffic redirection for MTD requirements
  - Enabled TCP and QUIC session handover for moving servers

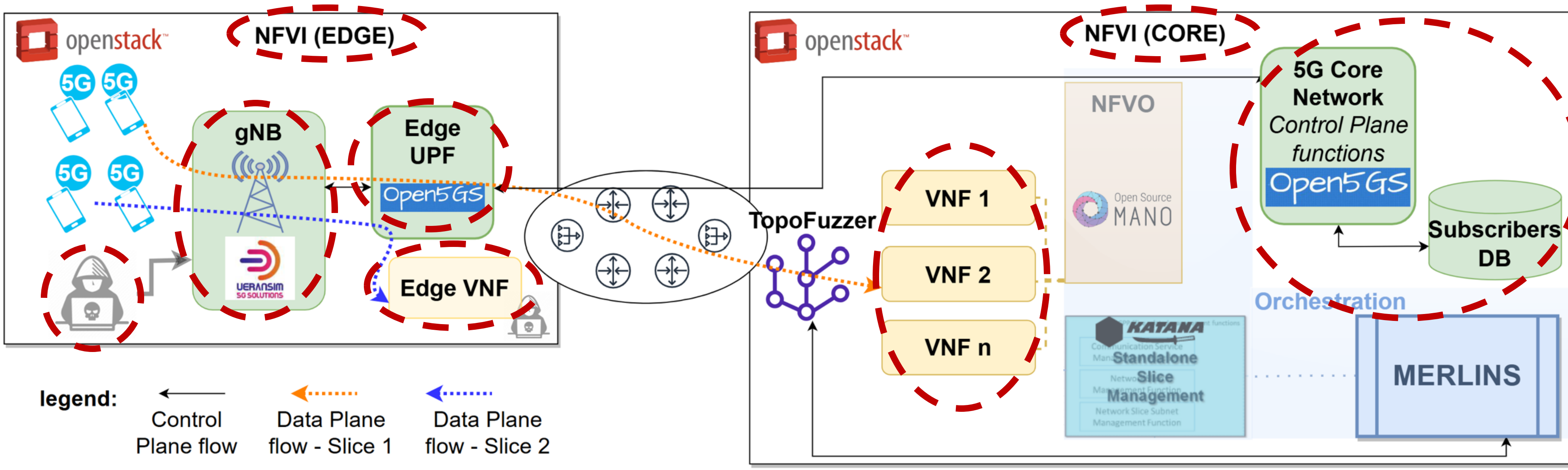
[IEEE NOMS 2023]

- **OptSFC** optimizes MTD strategies for Security, QoS, and Costs
  - Modelling the network state into a multi-objective Markov Decision Process (MOMDP), enabling deep-RL and MORL training

[IEEE NFV/SDN 2023]
[IEEE Network 2024]

- **MTDFed** uses privacy-aware FL for multi-tenant OptSFC (in progress)
  - Deep-RL model confidentiality using Secure Multi-party Computation (SMC)

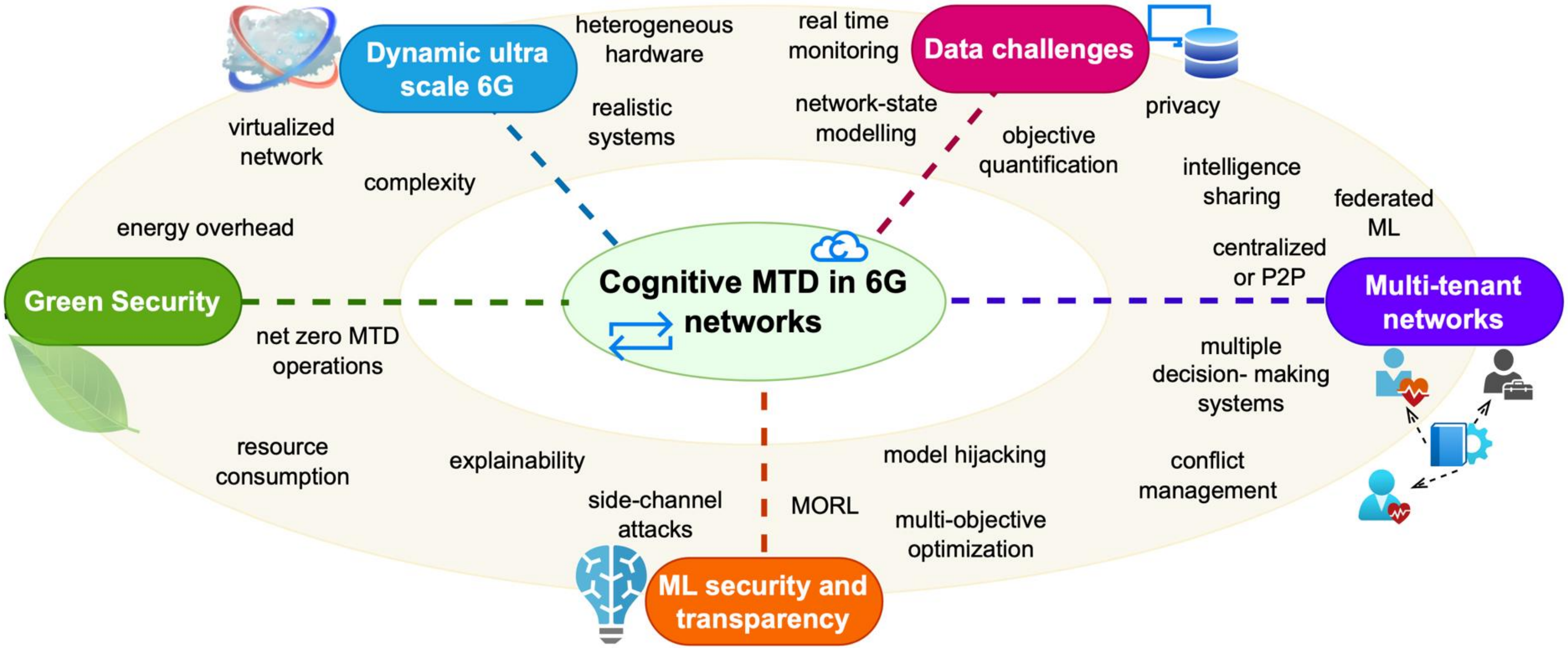
5G Testbed – MERLINS Integration



Emulated attacks:

- Active network reconnaissance attack
- Node intrusion and tampering attack
- Data exfiltration attack

Challenges and Research Directions



[IEEE Network 2024]

Challenges and Research Directions (2)

Dynamic Ultra-Large-Scale Networks

- Future 6G networks are massive and heterogeneous.
- Example: Remote surgery vs. smart agriculture needs.
- Challenge: Account for diverse latency, bandwidth, and processing demands.

Data Challenges

- Requires real-time and diverse metrics.
- Must align reward design with MTD goals.
- Monitoring public networks may risk user data privacy.
- Consider privacy-preserving analytics.

MTD in Multi-Tenant Networks

- Federated MTD Designs:
  Centralized: Simpler, needs high trust among parties.
  P2P: Independent, complex coordination.
- Hybrid systems need conflict resolution.

[IEEE Network 2024]

Challenges and Research Directions (3)

Green Security

- Aim to minimize energy consumption of MTD.
- Tactics: Use green energy nodes for VNF placement.
  Include energy cost in MTD optimization.
- Also relevant for net-zero and SDG goals.

Security and Transparency of AI control

- Risks: Model hijacking, poisoning, evasion, DoS.
- Needs: Explainable RL, secure input data.

[IEEE Network 2024]

Conclusion and Future Directions

- MTD is a key defensive mechanism in future networks, e.g., cloud-native systems, MEC, and multi-tenant networks.

- AI/ML is instrumental in adapting and optimizing MTD decision and orchestration.
  - MERLINS adds a cognitive security layer in Telco Cloud networks.

- Research directions include:
  - Scalability in bigger networks (thousands of VNFs/CNFs)
  - Novel MTD actions based on security scenarios
  - Secure and green MTD strategies
  - Make ML decisions in MERLINS humanly explainable
  - Scalable and federated MTD architectures
  - Adaptation to dynamic, heterogeneous future networks

Publications

1. [Full Paper] W. Soussi, G. Cantali, **G. Gür**, B. Stiller: ContMTD: Live Migra-tion Optimization for Containers in Moving Target Defense; ACM SIGCOMM, submittedon January 2025. (Under Review)
2. [Full Paper] Y. Abdullah, M.B Alshawki, P. Ligeti, W. Soussi, B. Stiller: Byzantine-Resilient Federated Learning: Evaluating MPC Approaches; IEEE ICDCS Workshop 2025,FL4WEB Workshop at the 45th IEEE International Conference on Distributed Computing Systems, Glasgow, Scotland, UK, 20-23 July 2025.
3. [Full Paper] A. Mamaril, R. Kolodziejczyk, W. Soussi, **G. Gür**: Containers on the Move: An Experimental Analysis of Container Migration in Kubernetes; ICC 2025 - IEEE International Conference on Communications, Montreal, Canada, 8-12 June 2025.
4. [Journal] W. Soussi, **G. Gür**, B. Stiller: Democratizing Container Live Migration for Enhanced Future Networks - A Survey; ACM Computing Surveys 57, 4, Article 97 (April 2025), 37 pages.
5. [Journal] W. Soussi, **G. Gür**, B. Stiller: Moving Target Defense (MTD) for 6G Edge-to-Cloud Continuum: A Cognitive Perspective; IEEE Network, vol. 39, no. 1, pp. 149-156,Jan. 2025.
6. [Full Paper] N. Mayone, P. Kunz, B. Yigit, W. Soussi, B. Stiller, **G. Gür**: IPv6 ConnectionShuffling for Moving Target Defense (MTD) in SDN; 2024 IEEE International Conferenceon Cyber Security and Resilience (CSR), London, United Kingdom, 2024, pp. 373-378.
7. [Full Paper] S. Birtane, W. Soussi, **G. Gür**, B. Stiller, et al.: Footprint-Optimized Orchestration and Management of Secure Complex Services over 6G Continuum; 2024 IEEE Conference on Standards for Communications and Networking (CSCN), Belgrade, Serbia,2024, pp. 383-388.
8. [Recent Results Paper] A. Mamaril, R. Kolodziejczyk, W. Soussi, **G. Gür**: Exploring Live Pay-load Migrations for MTD in Microservices Architecture; 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring), Singapore, Singapore, 2024, pp. 1-5.
9. [Full Paper] W. Soussi, M. Christopoulou, **G. Gür**, B. Stiller: MERLINS–Moving Target Defense Enhanced with Deep-RL for NFV In-Depth Security; IEEE Conference on Net-work Function Virtualization and Software Defined Networks (NFV-SDN), Dresden, Ger-many, 2023, pp. 65-71.
10. [PhD School] W. Soussi, **G. Gür**, B. Stiller: ML-Driven Moving Target Defense for Network Slice Protection; 11th TMA PhD School at the Network Traffic Measurement and Analysis Conference (TMA), Naples, Italy, 26-29 June 2023.
11. [Short Paper] W. Soussi, M. Christopoulou, T. Anagnostopoulos, **G. Gür**, B. Stiller: TopoFuzzer - A Network Topology Fuzzer for Moving Target Defense in the TelcoCloud; NOMS2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA,2023, pp. 1-5.
12. [Demo Paper] W. Soussi, M. Christopoulou, G. Xilouris, E.M.d Oca, V. Lefebvre, **G. Gür**, B.Stiller: Demo: Closed-Loop Security Orchestration in the TelcoCloud for Moving Tar-get Defense; NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, 2023, pp. 1-3.
13. [Full Paper] G. Chollon, R.A. Garriga, A.M. Zarca, A. Skarmeta, M. Christopoulou, W. Soussi, **G. Gür**, U. Herzog: ETSI ZSM Driven Security Management in Future Networks; 2022IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 334-339.
14. [Full Paper] W. Soussi, M. Christopoulou, **G. Gür**, B. Stiller: Moving Target Defense as a Proactive Defense Element for Beyond 5G; IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 72-79, September 2021.
15. [Poster Paper] M. Christopoulou, W. Soussi, G. Xilouris, **G. Gür**, E.M.d Oca, H. Koumaras: AI-Enabled Slice Protection Exploiting Moving Target Defense in 6G Networks; EuCNC6G Summit Virtual Conference, 6G Vision Poster Session B, (Porto, Portugal) 8-11 June 2021.

Mulţumesc!

Thank You!