UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

Mapping Security-enabling Virtualized Network Functions

Ramona Kühn

in cooperation with Andreas Fischer, Waseem Mandarawi, Hermann de Meer

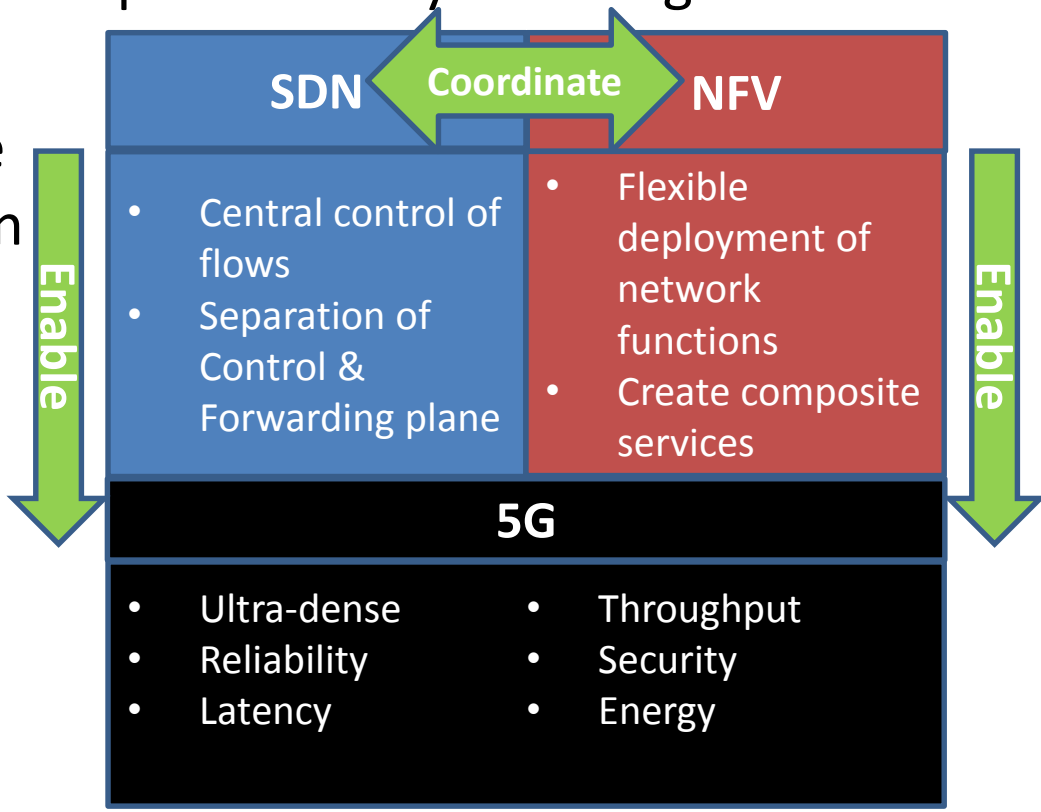
University of Passau

Faculty for Computer Science and Mathematics

Joint Meeting of the VDE/ITG Section:
IP and Mobility & Network Security
Network and Services Security towards 5G
December 5th, 2016, Technical University of Munich

Motivation

- Mobile networks based on SDN/NFV
- Network functions also encompass security-enabling functions
- Functions pose qualitative constraints to construction of a composite service
- Coordinated SDN/NFV is needed in 5G



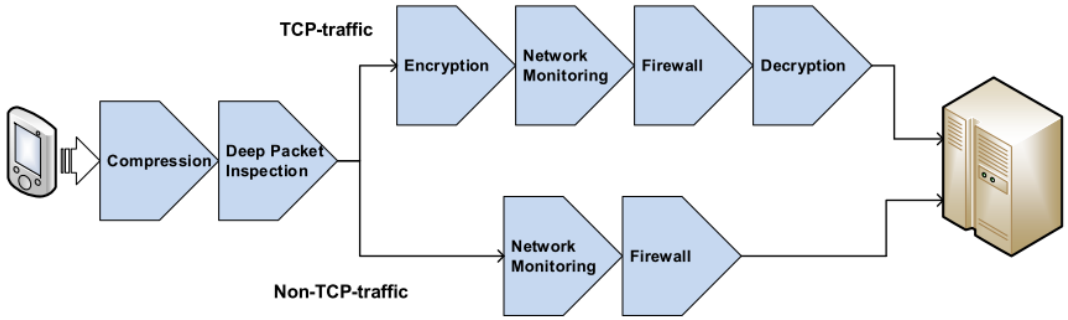
Background: SDN and NFV

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

- High flexibility in planning large environment
  - Virtualizing security functions
  - Integration with cloud computing
    - Utilize flexibility
    - On-demand computational capacity
    - Edge computing: deploy required functions closer to groups of users
  - Using SDN to easily establish paths for these functions
- Combining SDN/NFV:
  - Scalability, throughput, low latency in connection setup
- → Connection to 5G

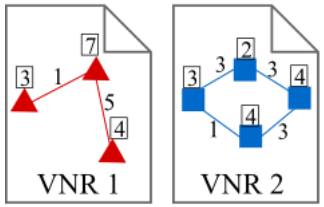
The NFV Mapping Problem

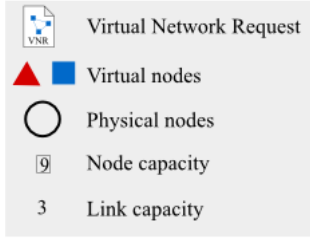
- The combination of network functions imposes a topology
- This topology is not fixed – several variations might be possible
  - E.g., encryption before or after compression?
- This has effects on resource usage – some variations may be easier on resources than others
- Problem is somewhat similar to VNE

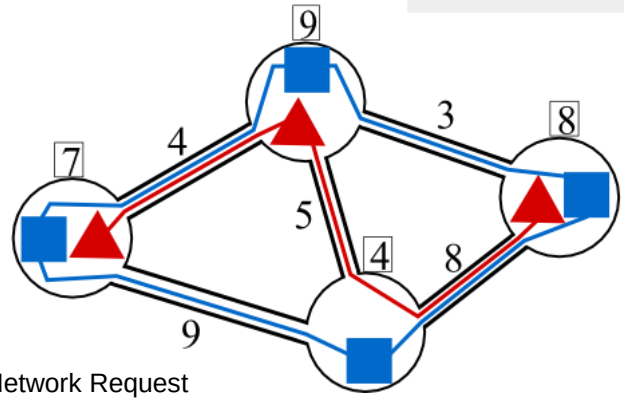


The Virtual Network Embedding Problem

- Virtual Network Embedding
  - Deploy multiple VNs on a single substrate network
  - Networks are represented as a graph
  - Virtual nodes or links pose demands for certain resources
- NP-hard problem
  - Efficiency requires heuristics
- Most VNE algorithms are performance oriented
  - Optimize for cost
  - Maximize accepted # of VNs
- Security not regarded in depth!







VNR: Virtual Network Request

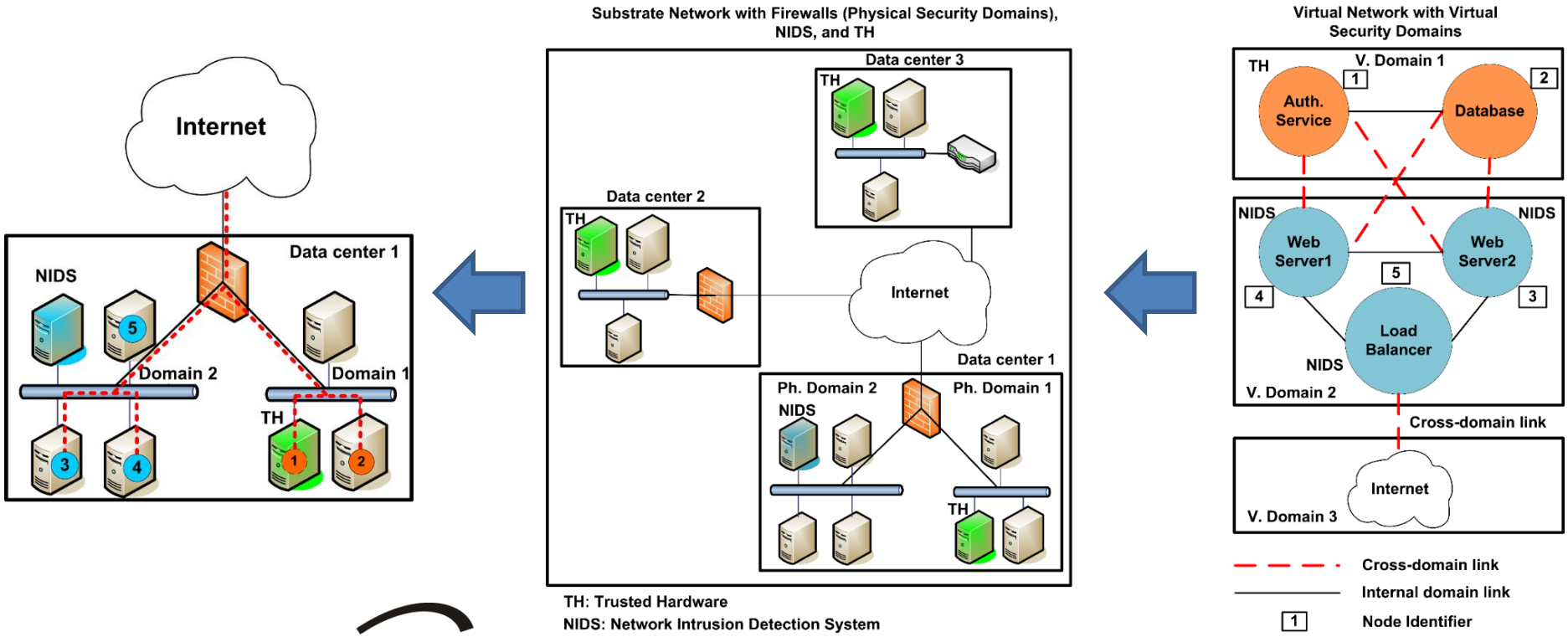
Security-aware VNE model

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

- Classified and defined a basic set of security requirements for VNs
  - Trusted Hardware
  - Network Intrusion Detection
  - Firewall
- Identified topological constraints as a new type of constraint that requires additional support
- Presented a generic methodology for modeling and implementing topological constraints
- Provided a proof-of-concept implementation of a security-aware VNE model in ALEVIN (VNE simulation framework)

Security-aware VNE model

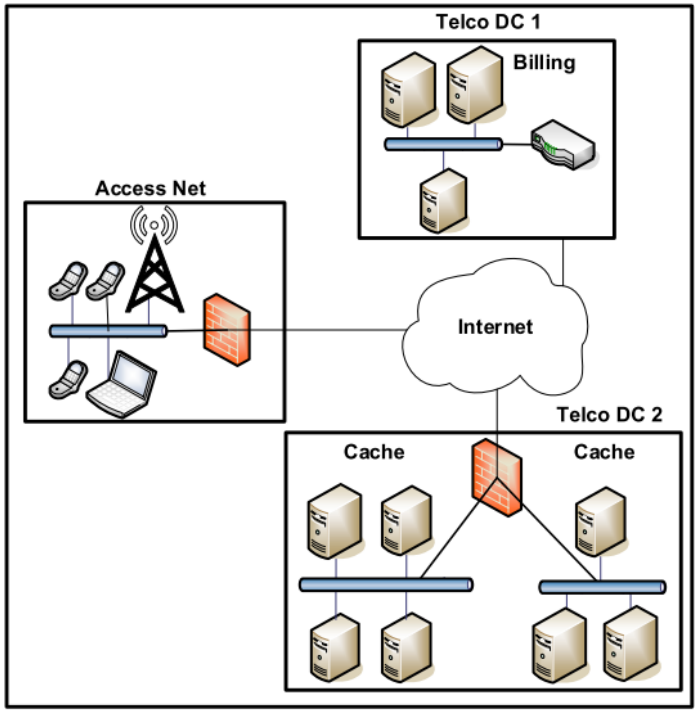
- A use case: web service with three domains
- Virtual nodes have specific qualitative requirements (such as TH)
- Domains as a topological requirement:
  - To realize it, cross domain links are mapped through firewalls



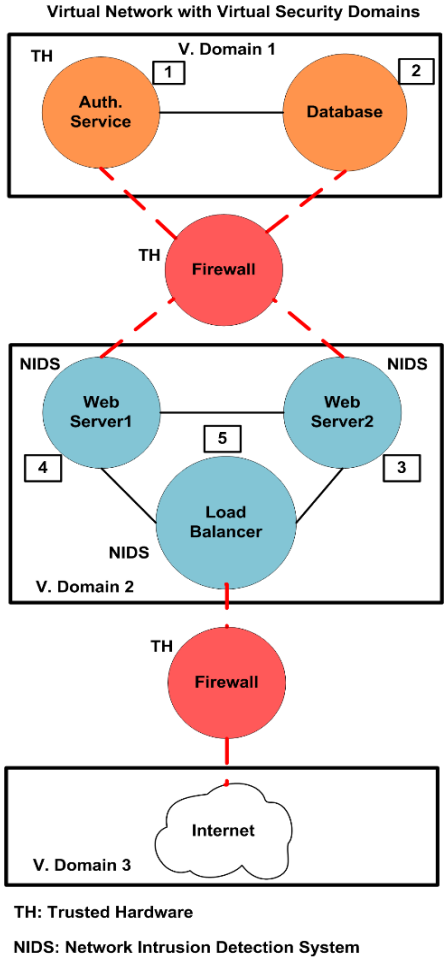
Adaptation to NFV/SDN context

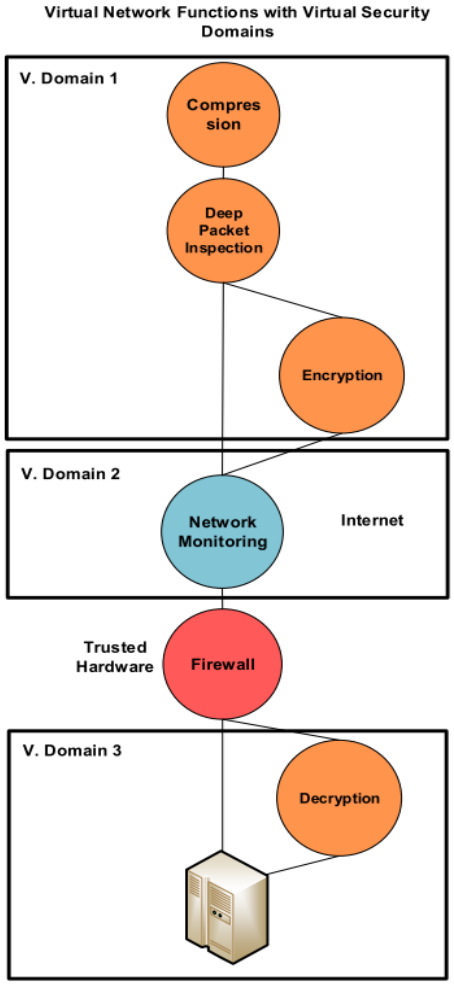
UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

- Similarities to VNE:
  - Consider administrative domains
  - Define trust boundaries
  - Determine cross-domain links
  - Determine and add virtualized firewalls
  - Embed the complex services
- Differences to VNE:
  - Nodes may be co-hosted
  - Order of network functions is relevant (i.e., a directed graph)



Planned Implementation





Conclusion and Future Work

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

- Strong similarities between VNE and realization of SDN/NFV networks
- Security is a major concern in 5G
- VNE concepts can be adapted to realize secure complex services

- Next step: Evaluation of concept
- Future Work: Optimization with regard to performance

Prior Work

- Andreas Fischer, Ramona Kühn, Waseem Mandarawi and Hermann De Meer. Modeling Security Requirements for VNE algorithms Valuetools 2016, 10th EAI International Conference on Performance Evaluation Methodologies and Tools 2016

- M. T. Beck, A. Fischer, F. Kokot, C. Linnho-Popien, and H. De Meer. A simulation framework for virtual network embedding algorithms. In 6th International Telecommunications Network Strategy and Planning Symposium (Networks 2014), pages 1-6. IEEE, Sept. 2014.

- B. Doll, D. Emmerich, R. Herkenhöner, R. Kühn, and H. de Meer. On Location-determined Cloud Management for Legally Compliant Outsourcing, pages 61-73. Springer Fachmedien Wiesbaden, Wiesbaden, 2015.

- Michael Niedermeier and Hermann De Meer. Constructing Dependable Smart Grid Networks using Network Functions Virtualization. Journal of Network and Systems Management, 2016