UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

# Secure embedding of virtual networks

**VDE/ITG Workshop**
**„Mobile Network (Function) Virtualization and Software Defined Networking**
**TUM, München / Garching, 2013**

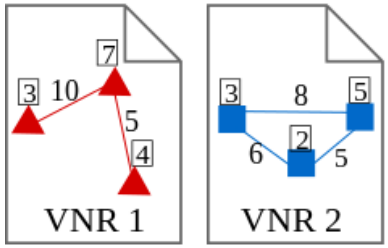
Andreas Fischer and Hermann de Meer

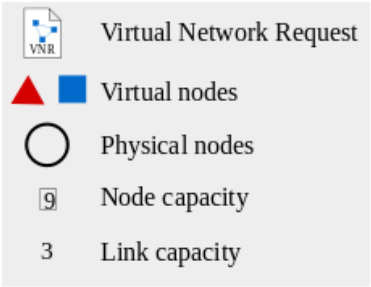
Computer Networks
& Communications
Prof. Hermann de Meer

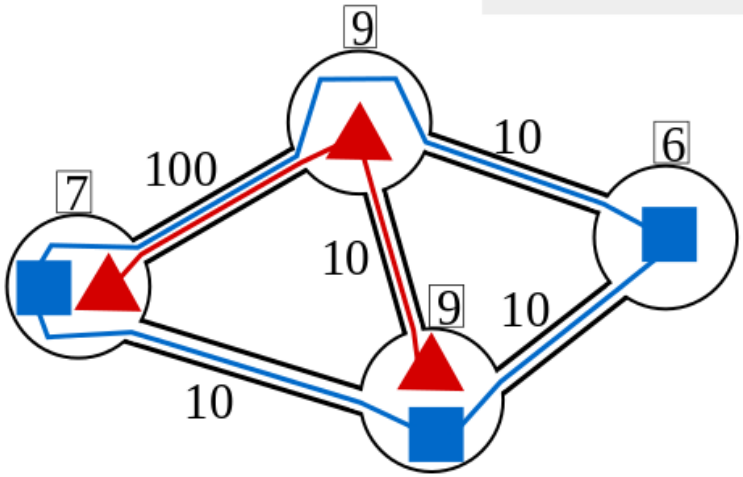
# Virtual Network Embedding



- Virtual Network Embedding (VNE): Map virtual resources to physical resources
  - Physical network provides resources
  - Virtual networks consume resources
- Resources are node and link properties
  - Node: E.g. CPU power
  - Link: E.g. bandwidth



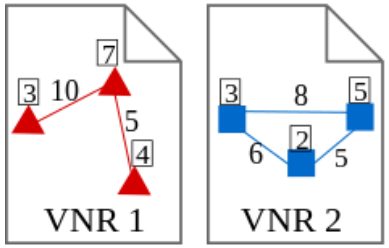



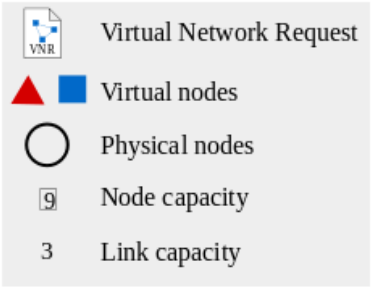



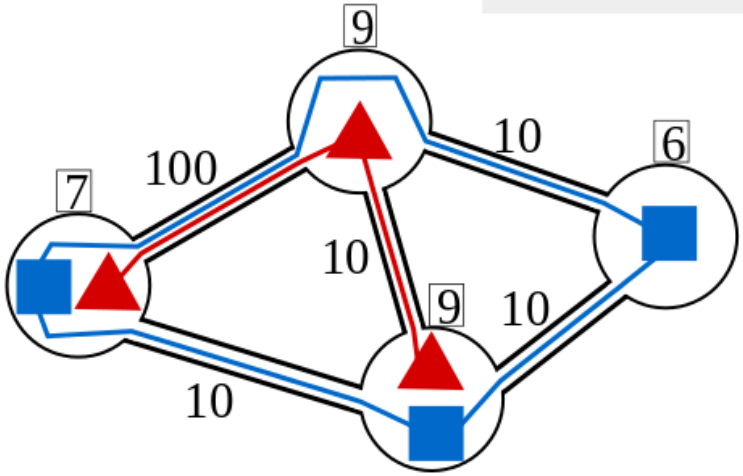
# VNE: Problem complexity



- Embedding is NP-hard
  - Bin-packing problem (nodes)
  - Unsplittable flow problem (links)
- Possible approaches
  - Exact (slow)
  - Heuristic
  - Meta-heuristic
- Different optimization criteria
  - High acceptance ratio
  - Low resource spending



# Virtual network security issues



- Virtual node to virtual node
  - Resource starvation: Excessive CPU usage
    - Can be used as Denial of Service attack
  - Sidechannel attacks

- Virtual machine to virtual link
  - Eavesdrop on communication
  - Resource starvation: Excessive network traffic

- Virtual machine to physical machine
  - Exploit vulnerabilities in virtualization solution
  - Threatens other virtual machines as well

# Security-aware VNE

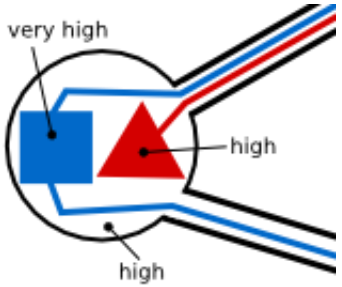
UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

- Apply VNE concepts to achieve security goals
  - Ensure performance by giving resource guarantees
  - Restrict critical virtual resources to special hardware
    - Real-time capable hardware for availability
    - Encryption capable hardware for confidentiality
  - Avoid co-hosting of potentially dangerous virtual nodes with other, critical virtual nodes
- New properties to consider for virtual resources
  - Real-time capabilities
  - Encryption capabilities
  - Reliability / trustworthiness

# Modeling reliability / trustworthiness (1)

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

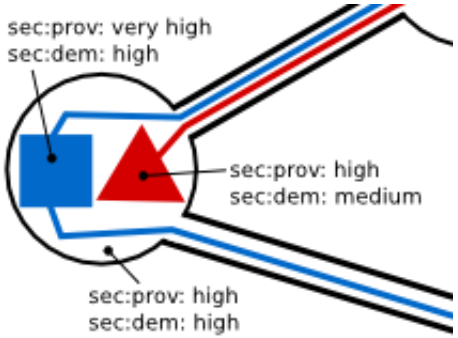
- First approach
  - Binary distinction: Secure / Insecure
  - Drawbacks
    - Too inflexible
    - Acceptance ratio can become very bad
- Second approach
  - Assign security levels to physical and virtual resources
    - Very low / low / medium / high / very high security
    - Try to minimize difference between security levels on same machine
  - Drawback: Semantic overload: Required vs. provided security



# Modeling reliability / trustworthiness (2)



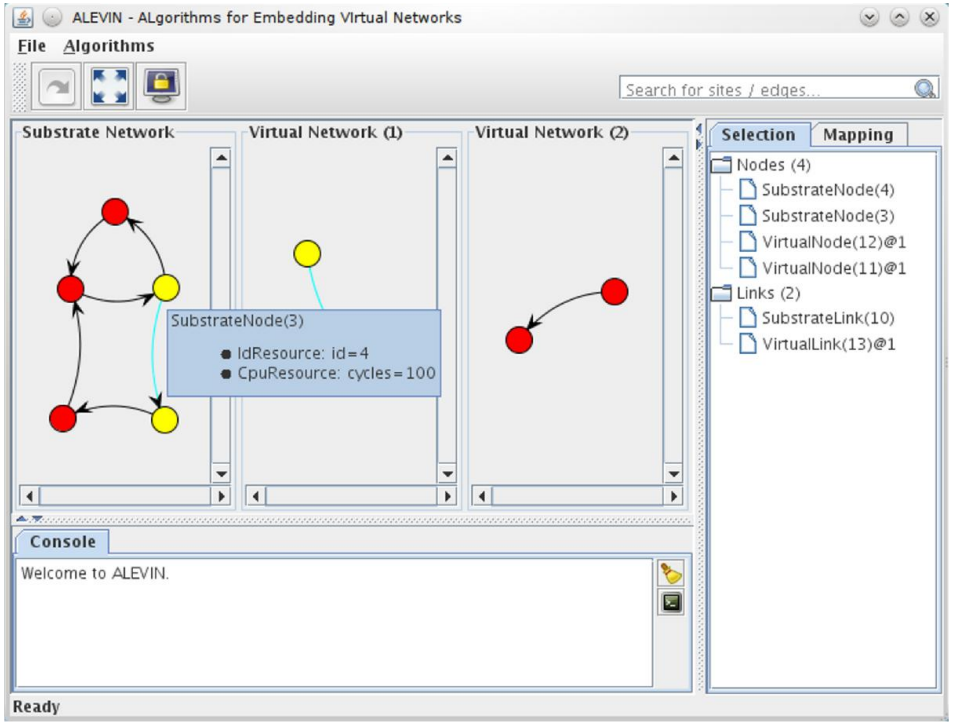
- Third approach
  - Assign security levels for security required and security provided (both physical and virtual resources)
    - Assign tuple (sec:required, sec:provided) to each resource
    - Try to cross-match:
      Ressource A (sec:required) <-> Ressource B (sec:provided)
  - Drawbacks
    - Acceptance ratio still not good
    - Still only focused on individual resources



# Evaluation with “ALEVIN”: Simulation of VNE algorithms

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

- Create networks
  - Physical and virtual
  - Arbitrary topologies
- Support various resources
  - Link and node
  - Beyond just CPU and bandwidth
- Run VNE algorithms
  - Evaluate with common metrics
  - Compare results




Visualization

# Next steps



- Extend existing simulation software
  - Support security requirements definition
  - Support evaluation of security metrics
- Implement security-aware VNE algorithm
  - Adhere to security requirements
  - Minimize performance impact
- Evaluate with realistic topologies
  - Predefined topologies (e.g., SNDlib)
  - Structured, randomly generated topologies

# Conclusion

- Virtual networks enable flexible network management
  - Rapid creation of virtual network topologies
  - Dynamic modification possible
- Optimizing resource assignment is hard, but solvable
  - Comparison of algorithms is necessary
  - Common simulation environment required
- Secure instantiation of virtual networks remains to be solved
  - Going beyond performance requirements
  - Requires new VNE approaches