Aalto University
School of Electrical
Engineering

TAKE 5 -5G TEST NETWORK Customer Edge Switching & 5G@II

Raimo Kantola
raimo.kantola@aalto.fi

www.re2ee.org

Agenda

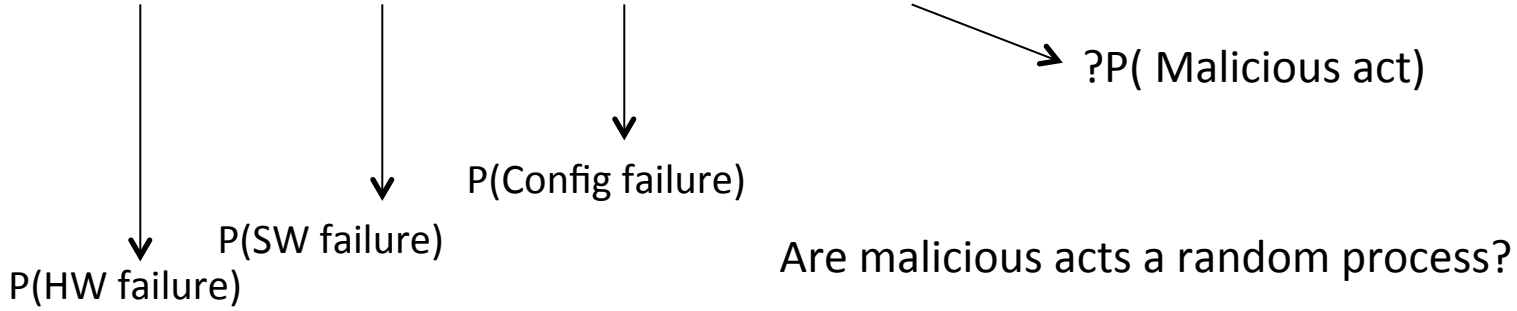
- Customer Edge Switching
  - 5G Security challenges
  - What, how
- 5G meets Industrial Internet (5G@II): 2017-18
  - Motivation
  - Access control using policy
- Business relevance

5G Security Challenges

1. If 5G = Broader band mobile Internet → Can not be ultra-reliable
   - Hackable, DdoSsable with trivial tricks
   - → Better end system security for battery powered devices
2. Virtualized network function security:
   - VNF to VNF interface = socket interface/multivendor
   - Flexibility and ease of deployment of new VNFs → interface in the Internet like any other
   - Security says: no, must be a closed network interface
3. Control/Data plane interface
   - Closed interface? Not on the Internet?

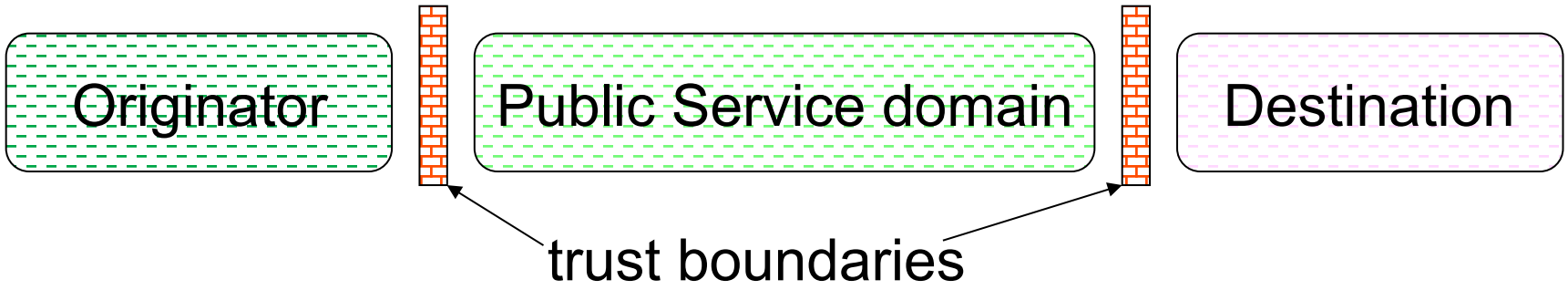
5G – ultra reliable communications

$$R = (1 - F1)(1 - F2)(1 - F3)(1 - F4)$$



- Is it a very secure network over which malicious actors can effectively conduct fraud?
- Or will the MOs do their best to prevent fraud and protect their customers using whatever means are technically feasible?

Communication over Trust Domains

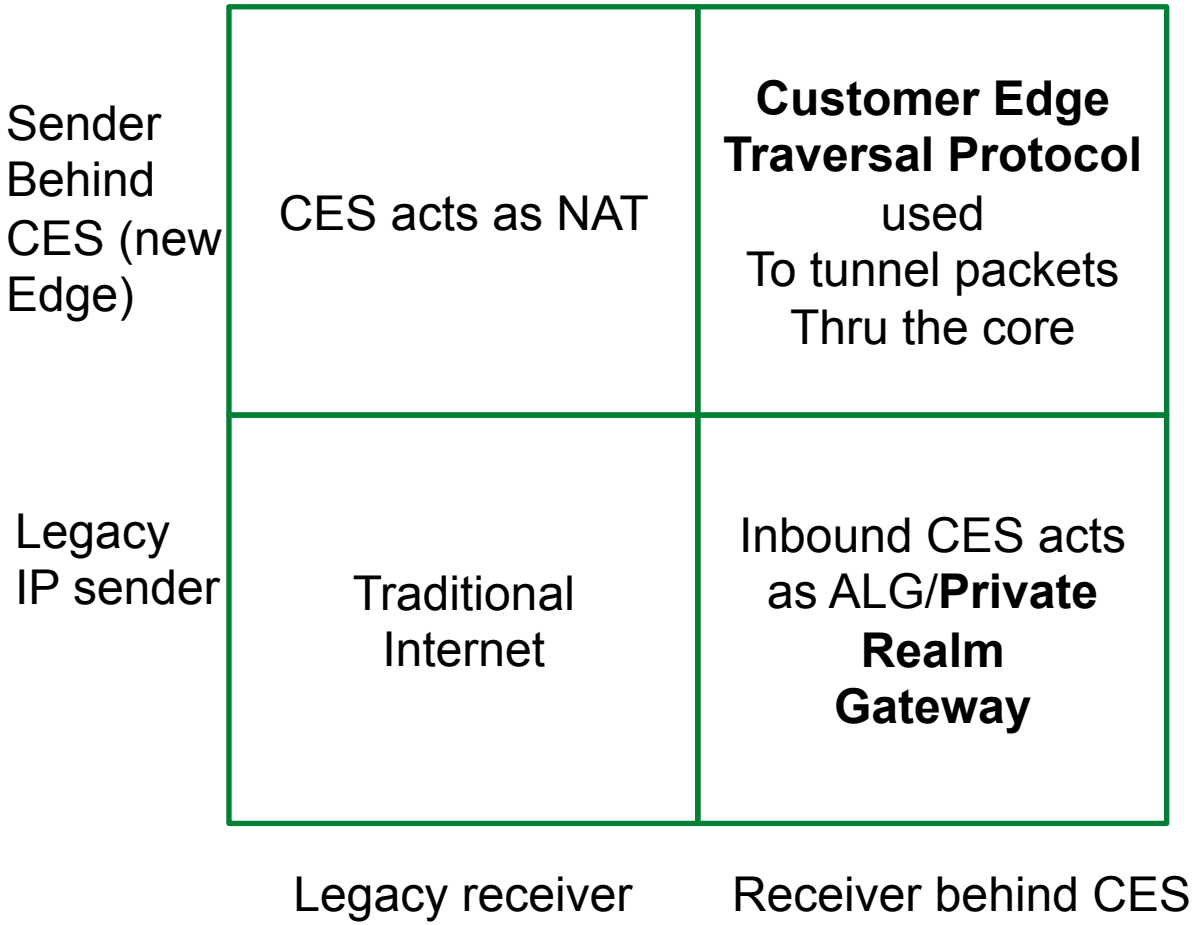


Originator and Destination are customer networks (stub networks in terms of IP routing)
+ each of them may have one or many private address spaces;
+ extreme case: mobile network addressing model: each user device is in its own address space and all communication takes place through the gateway or edge node connecting the user devices to the Internet

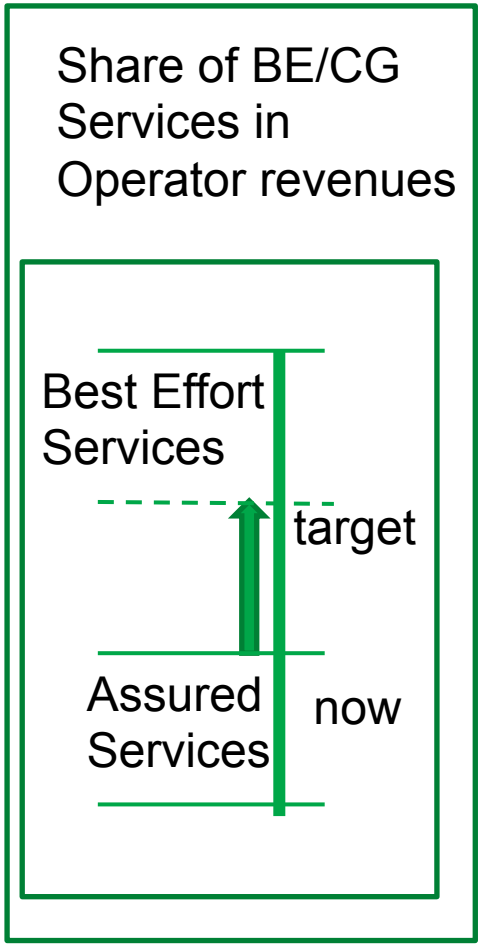
Trust Boundary == Customer Edge Switch == cooperative firewall

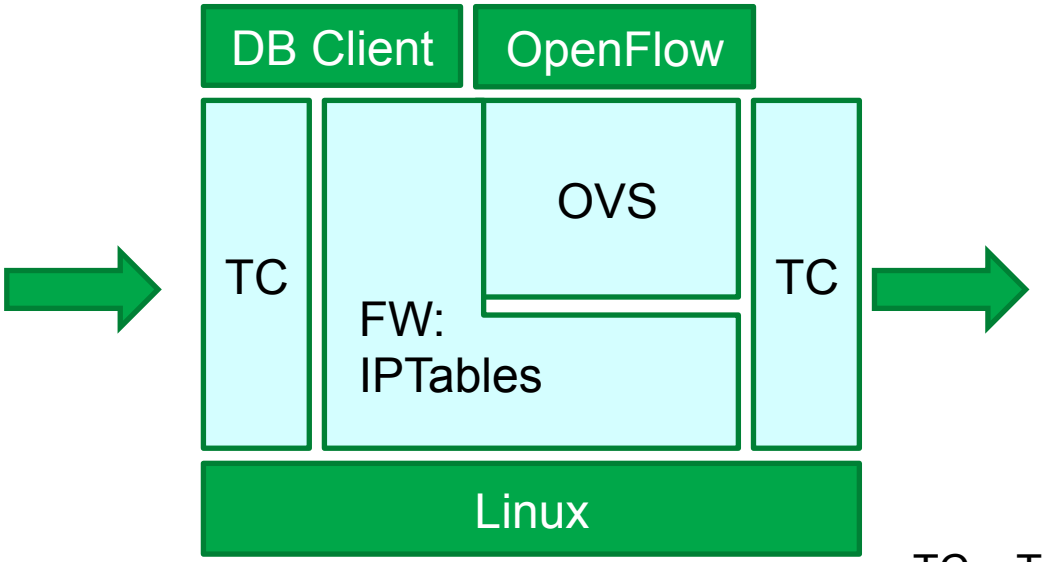
A CES has one or several RLOCs (routing locators) that make it reachable in the public service domain

Signaling Cases



Practical Data Plane of Edge Gateway





TC – Traffic Control

Role of OVS: mangle packets/reformat forwarding formats
Role of IPTables: packet filtering, rate limiting of nrof new flows, rate liming of service flows, spoofing elimination
CP resides in the DC and will have rules DB, Flow level Firewalling logic with edge to edge signaling and Connection control
TC and IPTables use a common flow abstraction

5G meets Industrial Internet (5G@II)

- A raising theme in European Research
- II → machine to machine communication
- 5G delivers to II:
  - Ultra high reliability
  - Low delay (1ms in radio)→ radio can be in a control loop
  - High capacity
  - New RF capacity regimes (free vs. licensed spectrum)

5G@II – how to manage billions of IoT devices

- Site = one or several masters + N service/hw providers + many outsourcing contracts.
- Physical transport/roads: industry wide applications
- Data flows within a provider + between providers either for data collection OR real time control loops
- Must be possible
  - to audit that real data flows correspond to cooperation or outsourcing contracts
  - to change the access rights to data as contracts change

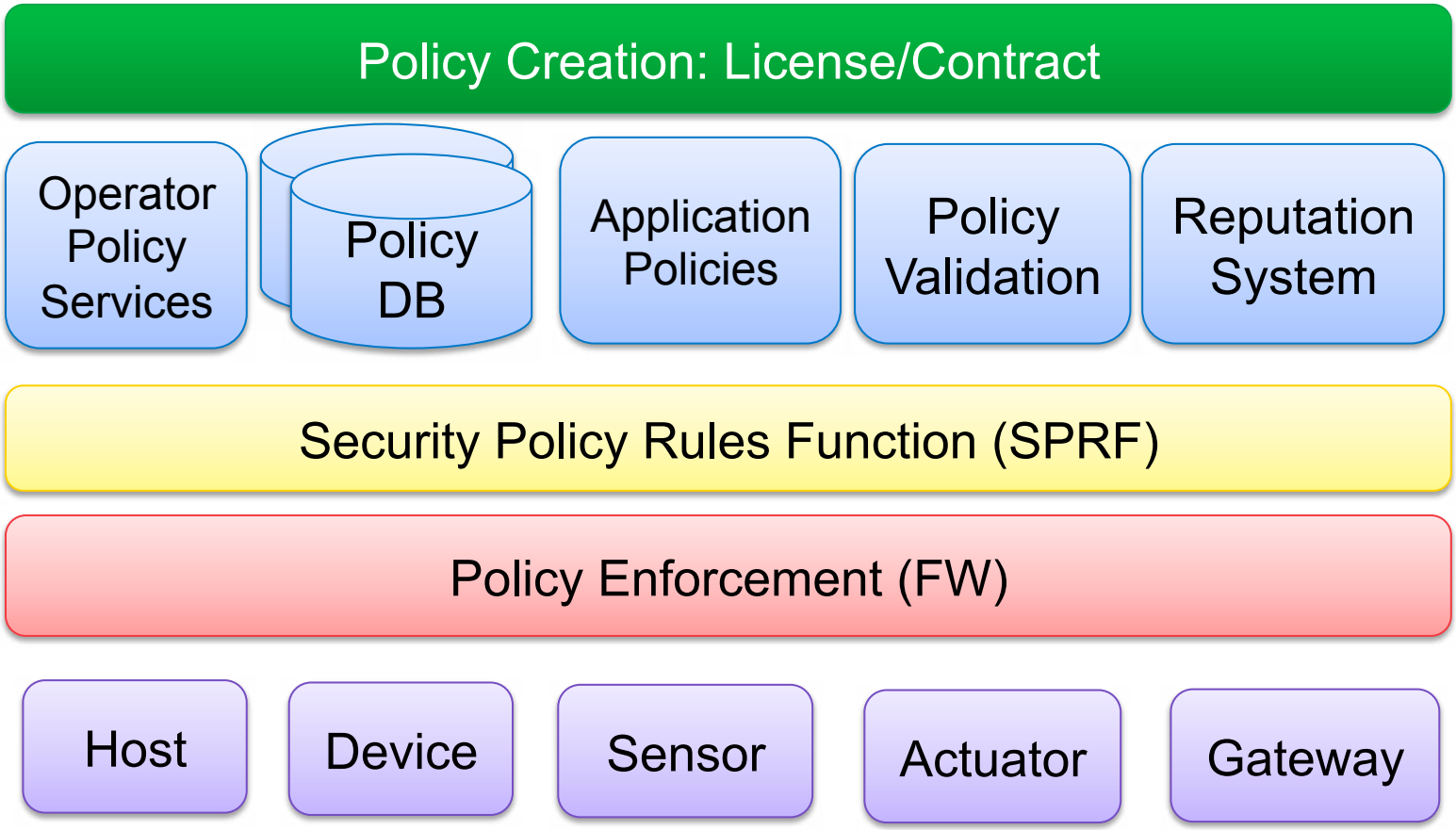
Alternatives for managing II devices

- Virtual Private networks
  - Take existing technology and patch it up
  - Internet core will have scaling challenges if millions of VPNs
  - When business relations change → heavy management burden
  - How to scale to data sharing across multiple players?
- Push all access control to network edge
  - Core has transport allocations
  - Security logic is at the edge
  - All flows are policy controlled
  - Cooperative Firewalling matches this need

What can we achieve for SECURITY by CES and Internet wide trust management?

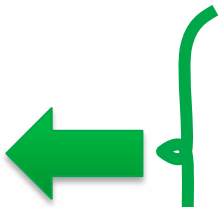
- CES
  - Eliminate Source Address spoofing
  - Tackle DDoS attacks efficiently
  - Dissolve boundary between closed and open networks
  - Push access control to the edge nodes
  - Leverage Mobile network style IDs for data communications
- Trust:
  - Fast location of bots → "useful" lifetime of a bot is reduced → bot renting business becomes less profitable
  - Scope of malicious activity is reduced
- Together: improved robustness of critical infra → national security
- **BUT: most vulnerabilities are on application layer → security should be based on multiple layers of defense + proactive trust mgt**

Policy Architecture manages access at the edge



Policies are dynamic – they change depending on security situation

- **When under attack, network gateway may ask for more secure credentials**
- **Emergency situations (Fire, terrorist attack etc…)**
- **Admission may depend on the reputation of the sender**
  - Blacklisting
  - Greylisting
  - Whitelisting

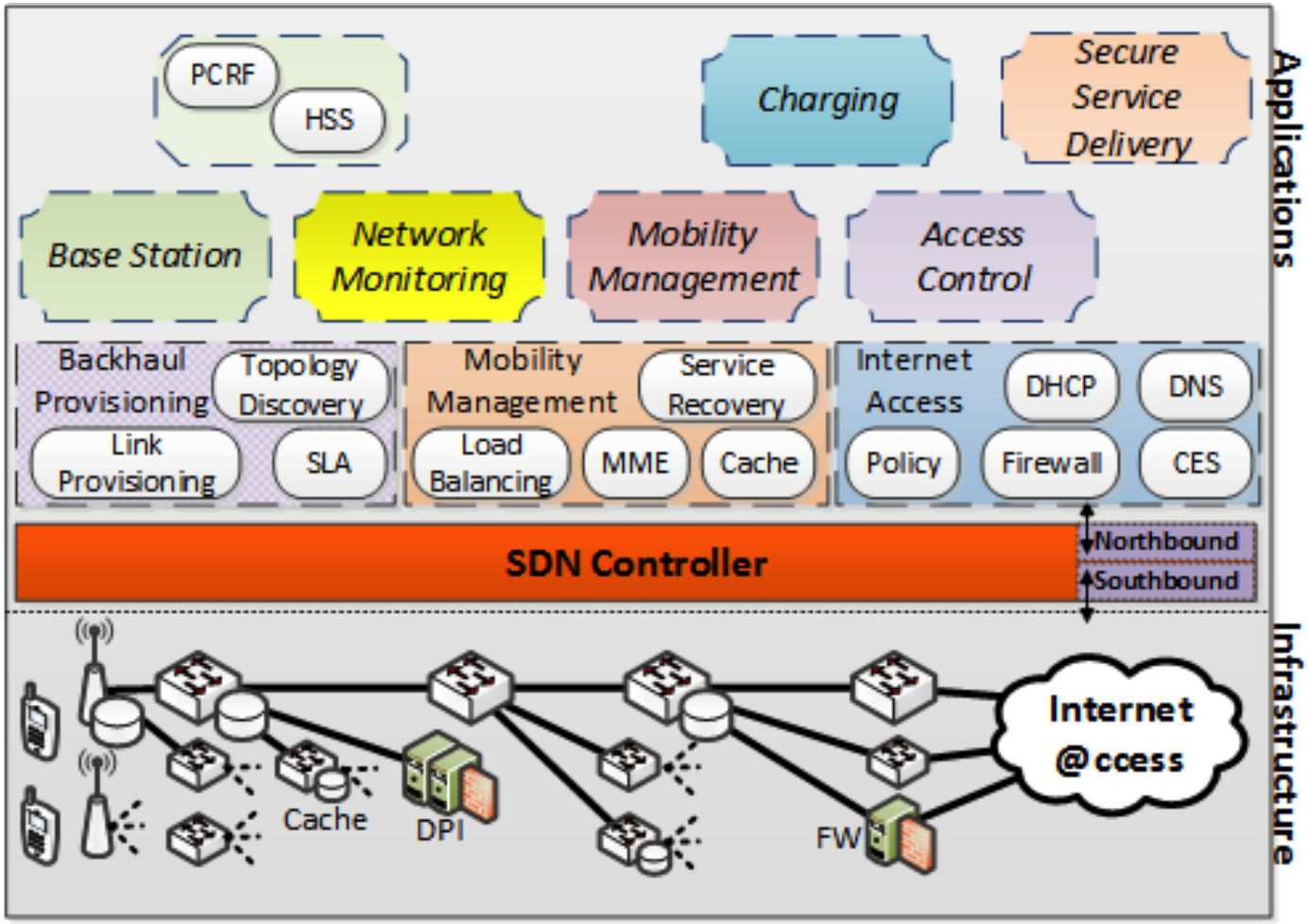


Trust/Reputation management for all entities

Steps in Cooperative Security

	CES Benefits to security
• One operator	• Centralized Policy management Simple black listing in all CES based on CES level detection
• Operator + its corporate customers	• More CES defending and detecting, ISP rating corporate CES credibility Outsourcing of CES/RGW services to operator
• Multiple operators	• If CERT/Regulator authorization, Detection also in hosts → triggering of network monitoring → Full Trust Domain = Cooperative FW + Trust
• MTC	• Can monitor all traffic in network → full deployment possible

5G Control as a Group of SDN Apps



TAKE 5 Architecture