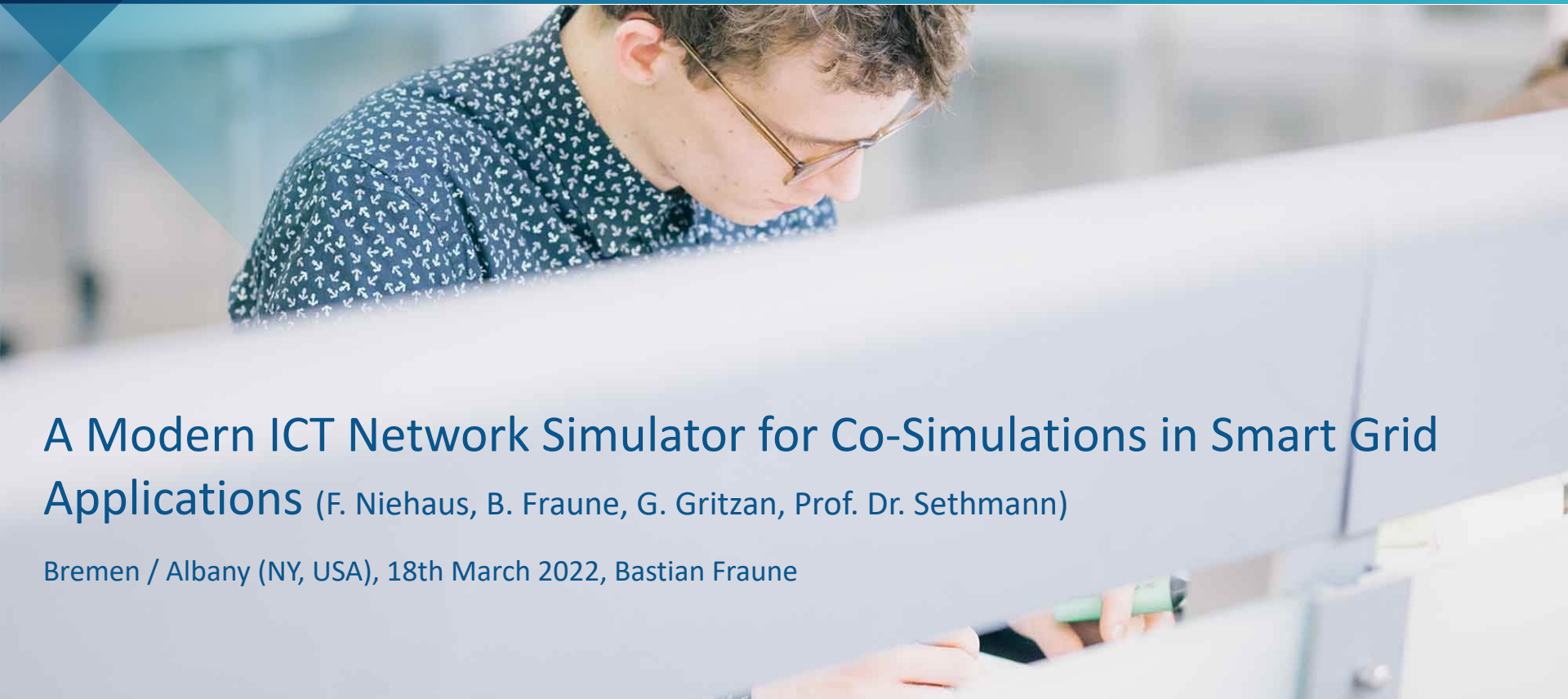
Hochschule Bremen
City University of Applied Sciences

HSB



A Modern ICT Network Simulator for Co-Simulations in Smart Grid Applications (F. Niehaus, B. Fraune, G. Gritzan, Prof. Dr. Sethmann)

Bremen / Albany (NY, USA), 18th March 2022, Bastian Fraune

Agenda

1 Introduction Smart Grid Security Research
2 Structure and Usage of rettij
3 Practical Application Scenario
4 Conclusion

Agenda

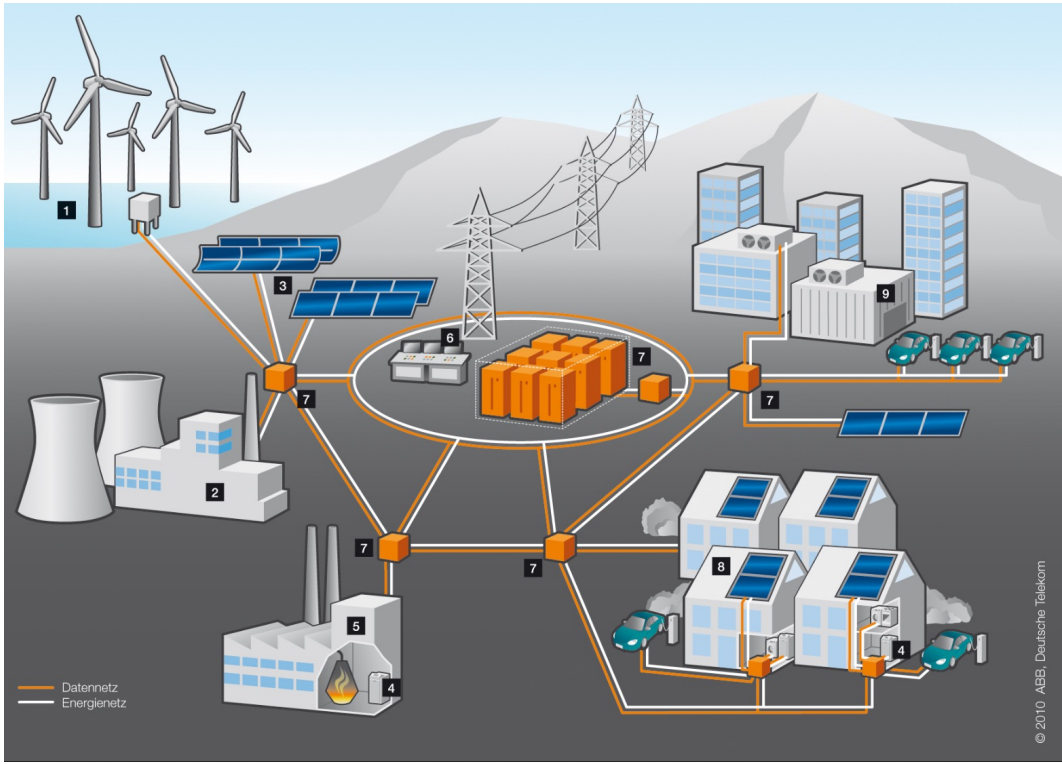
1 Introduction Smart Grid Security Research
2 Structure and Usage of rettij
3 Practical Application Scenario
4 Conclusion

Research Area: ICT Attack Simulation in Smart Grids

Energy transition

- Decentralized generation
- „Prosumers“: generate and consume energy
- Requires much more (intelligent) digital coordination

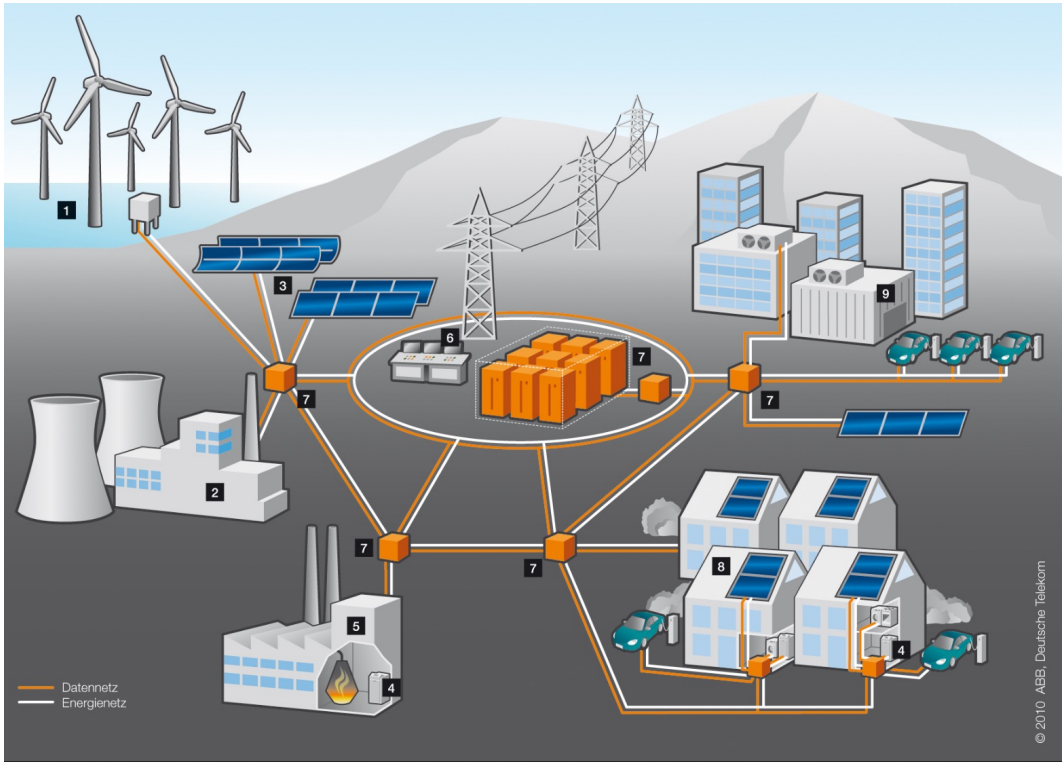
- Requires more security research and testing
- BUT: real power grid system is complex and sensitive



Research Area: ICT Attack Simulation in Smart Grids

Simulating smart grid

- Simulate attacks- and defense scenarios
  - Impacts?
- Holistic view necessary
- Co-simulation of domains
  - Power grid
  - ICT
  - Energy market



Application Scenarios: Project PYRATE

AI attacker goals

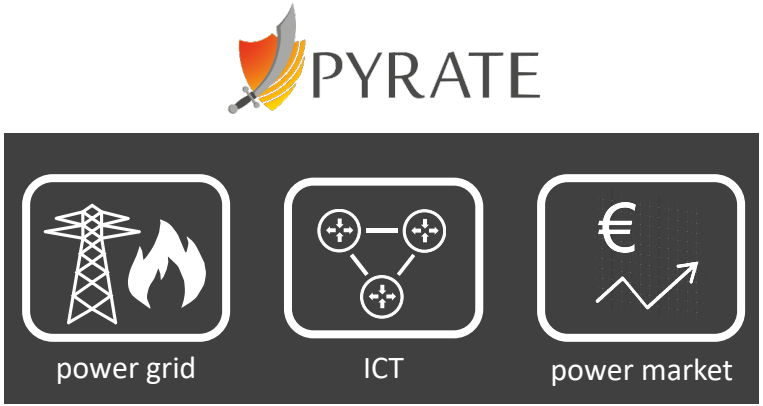
- Optimize benefits on market

AI attacker has access to:

- Power grid control
- ICT control (restart, DoS, traffic manipulations)
- Power market

Requires the simulation of

- Power grid
- ICT network / components
- Local energy market



Research Area: ICT Attack Simulation in Smart Grids

Requirements for network simulation in co-simulation

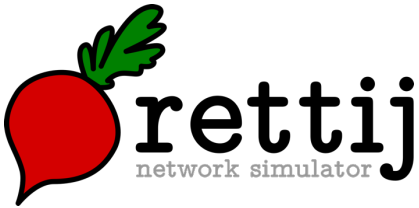
- Seamlessly and **natively** work with co-simulations
- Easily **integrate custom** and well-known ICT components (webservers and stuff)
- Display **realistic network** traffic
  - No noise from simulation management ☺
- **Linux network** stack!
- Easy configuration
- **Simple** definition of **network configuration**
- Decentralized execution
- **Scalability**
- Integration of **docker file format**

Agenda

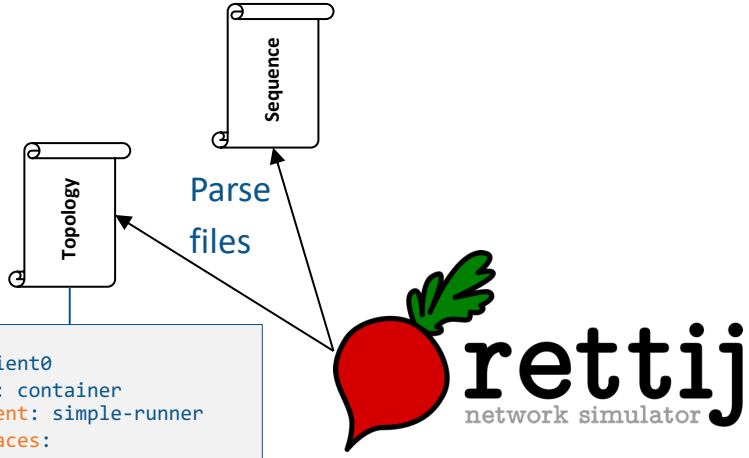
1 Introduction Smart Grid Security Research
2 Structure and Usage of rettij
3 Practical Application Scenario
4 Conclusion

Important Terms

- Topology -> defines a computer network
  - Node -> network component (switch, router, container/PC/server)
  - Interface -> network interface of a node
  - Channel -> logical connection between two interfaces (like „ethernet cable“)
- Command -> Command within a node (unix bash cmd)
- Sequence -> defines the execution of defined commands
- Scheduled sequence -> Command, executed at a certain time / step
  - Script sequence -> Commands, executed sequently



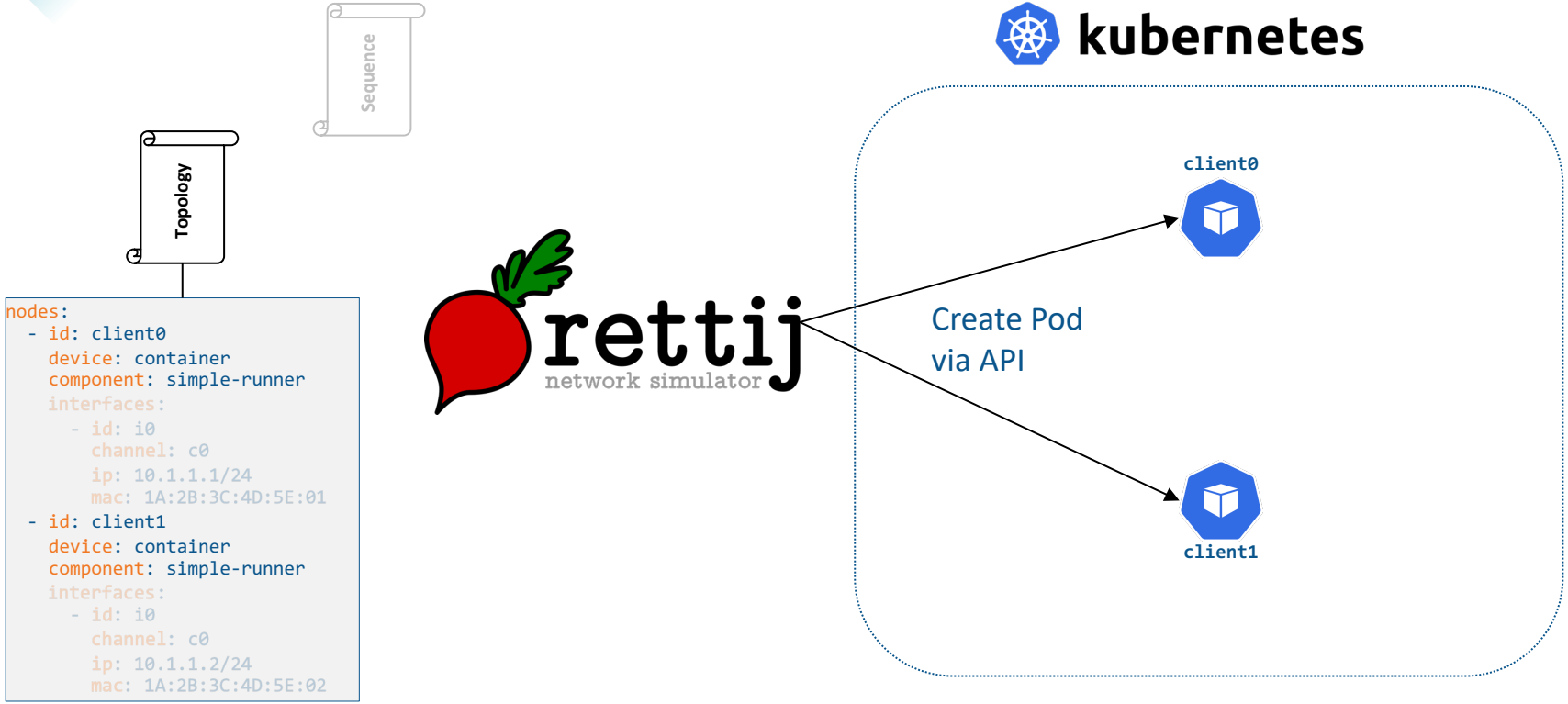
rettij Start Sequence – Parsing



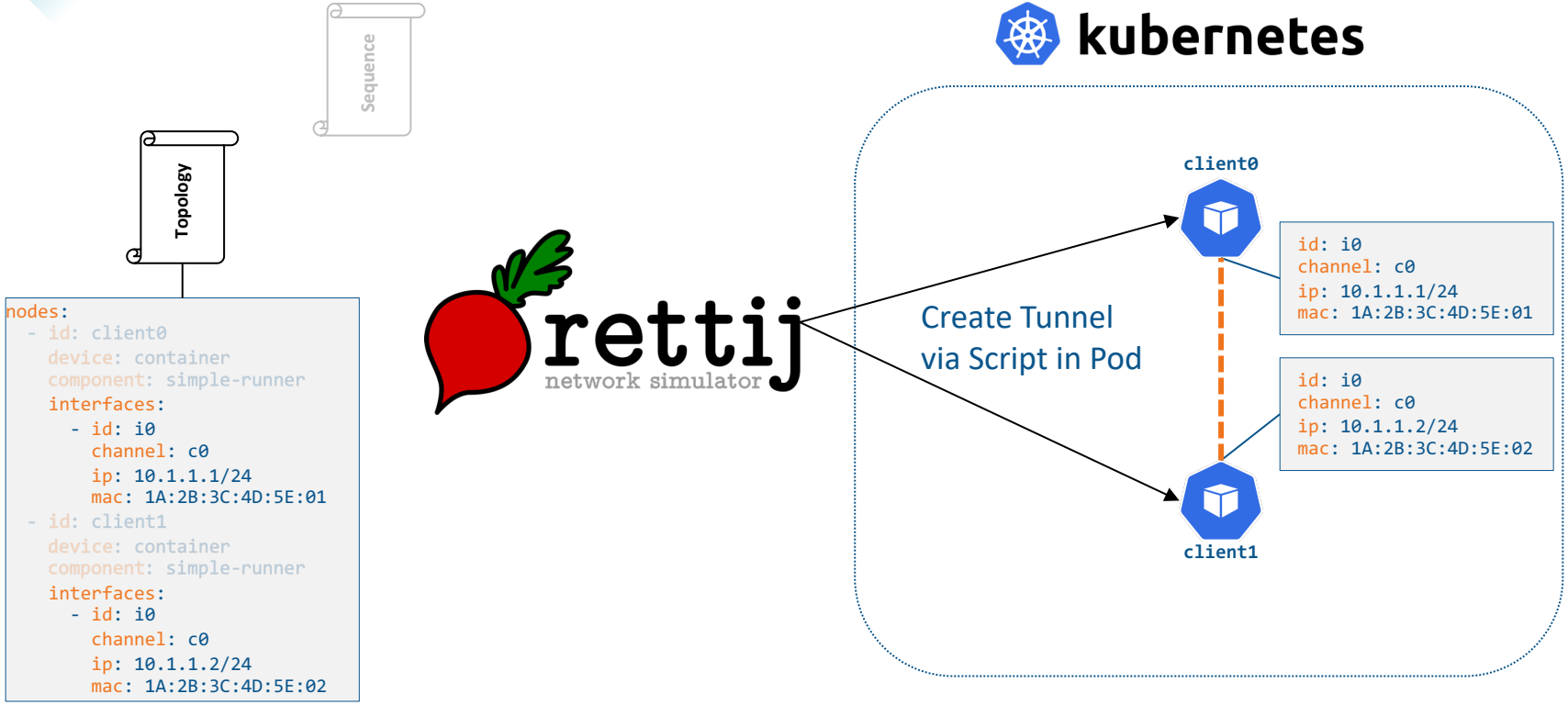

```yaml
nodes:
  - id: client0
    device: container
    component: simple-runner
    interfaces:
      - id: i0
        channel: c0
        ip: 10.1.1.1/24
        mac: 1A:2B:3C:4D:5E:01
  - id: client1
    device: container
    component: simple-runner
    interfaces:
      - id: i0
        channel: c0
        ip: 10.1.1.2/24
        mac: 1A:2B:3C:4D:5E:02
```

kubernetes

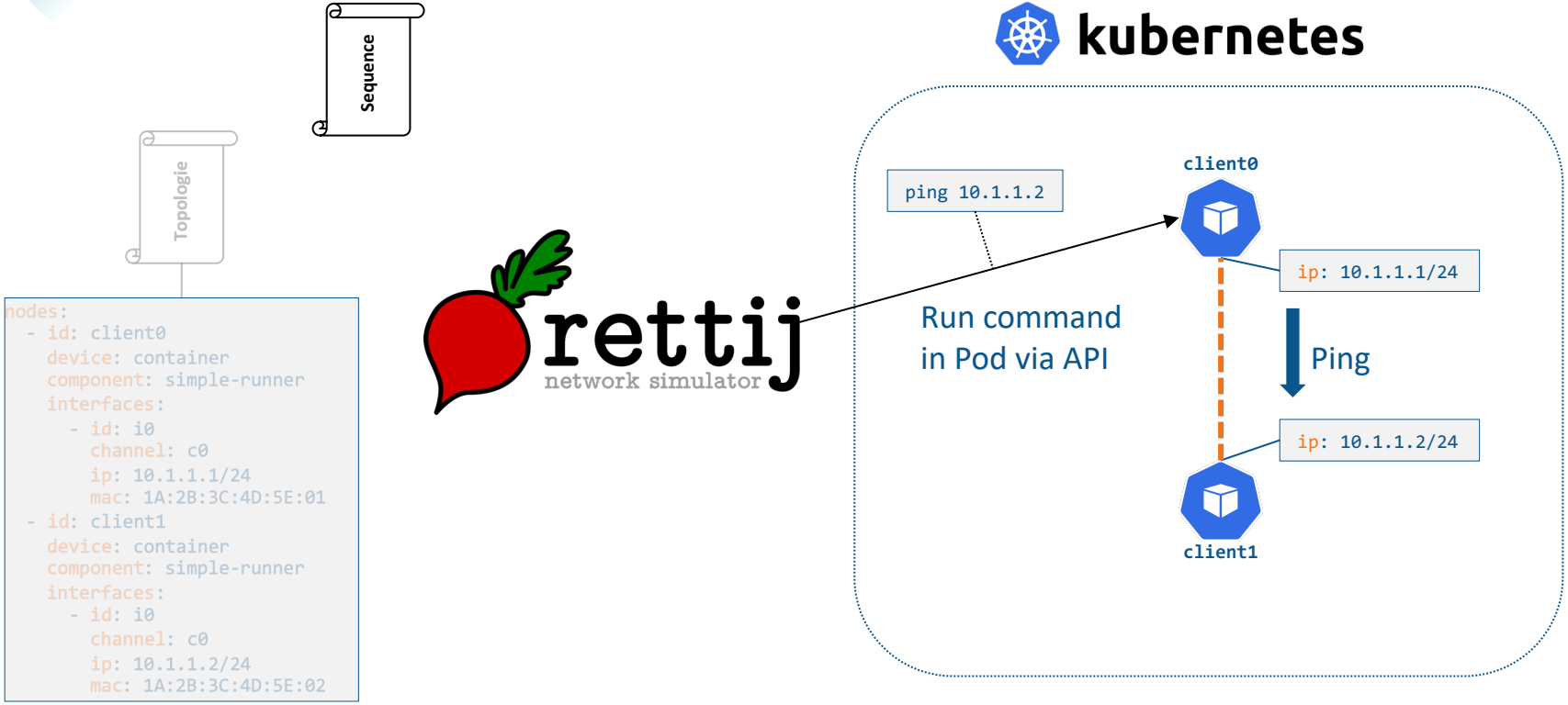
rettij Start Sequence – Pod Deployment



rettij Start Sequence – Tunnel Setup



rettij Start Sequence – Command Execution

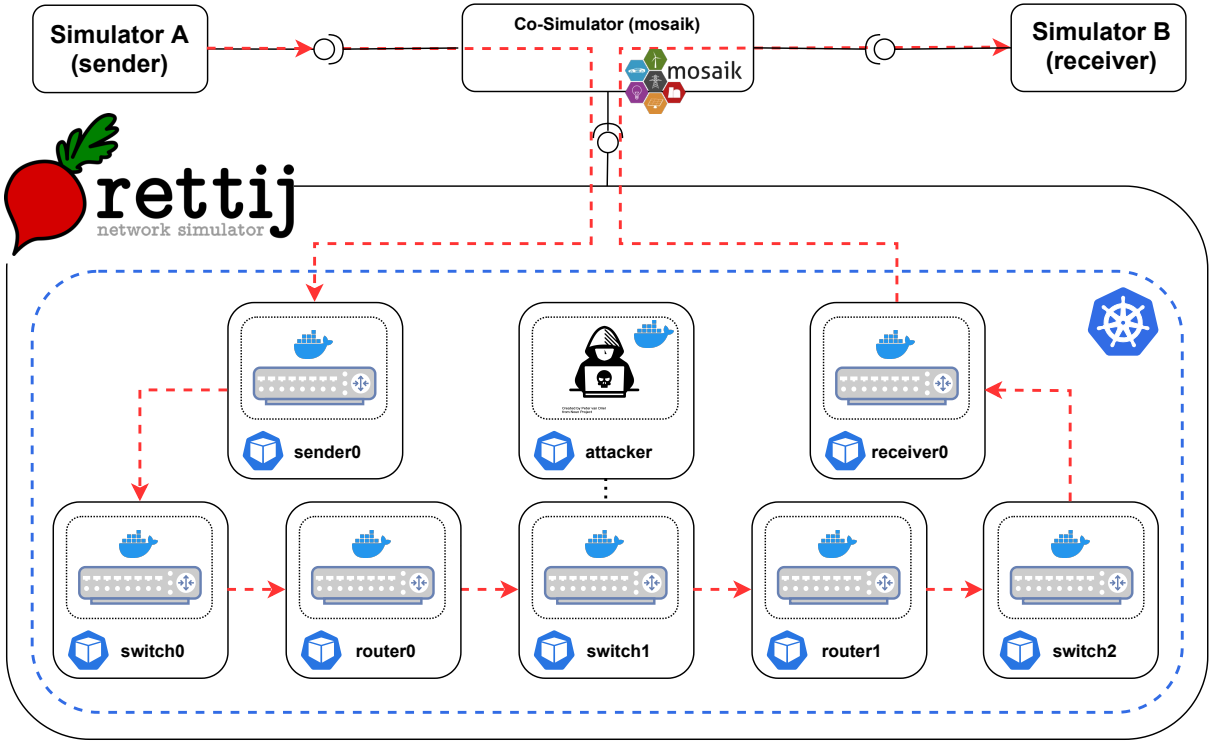


Agenda

1 Introduction Smart Grid Security Research
2 Structure and Usage of rettij
3 Practical Application Scenario
4 Conclusion

Practical Example: Data Flow

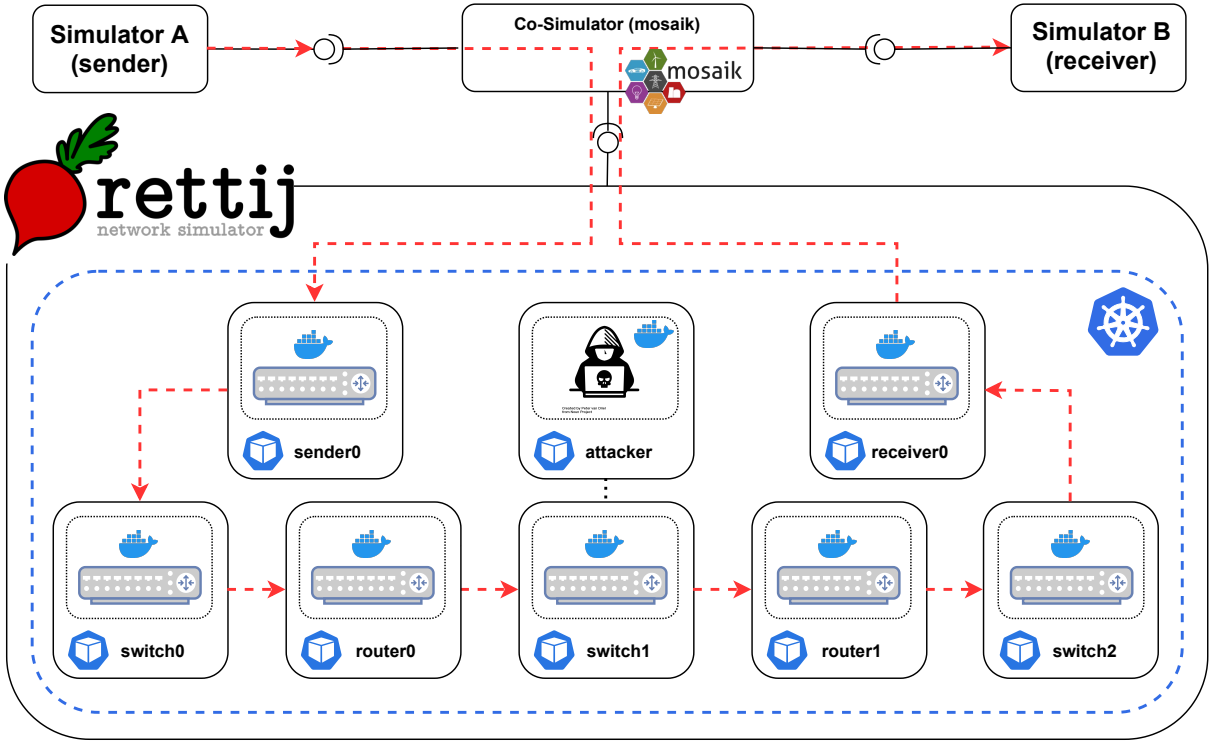
- Simulator A → Simulator B
- Co-Simulator connected to rettij
- Data is routed via rettij's network
- Attacker in the network:
  - MITM
  - Data Manipulation



Practical Example: Data Flow

Simulator A

- Sends incrementing numbers
- Sender0 sends receiver0
  - TCP data
- Execution via CLI



Practical Example: Data Manipulations

Simulator A

- Sends incrementing numbers
- Sender0 sends receiver0
  - TCP data

- Attacker inverting numbers

Simulator B receives manipulated data

```
Entity Model_sender_0 sent '4' for attribute 'value' at time 0.
Entity Model_receiver_0 received '4' for attribute 'value' at time 0.
Entity Model_sender_0 sent '6' for attribute 'value' at time 1.
Entity Model_receiver_0 received '6' for attribute 'value' at time 1.
Entity Model_sender_0 sent '16' for attribute 'value' at time 2.
Entity Model_receiver_0 received '16' for attribute 'value' at time 2.
Entity Model_sender_0 sent '22' for attribute 'value' at time 3.
Entity Model_receiver_0 received '-22' for attribute 'value' at time 3.
Entity Model_sender_0 sent '28' for attribute 'value' at time 4.
Entity Model_receiver_0 received '-28' for attribute 'value' at time 4.
Entity Model_sender_0 sent '37' for attribute 'value' at time 5.
Entity Model_receiver_0 received '-37' for attribute 'value' at time 5.
```

Practical Example: Data Manipulations

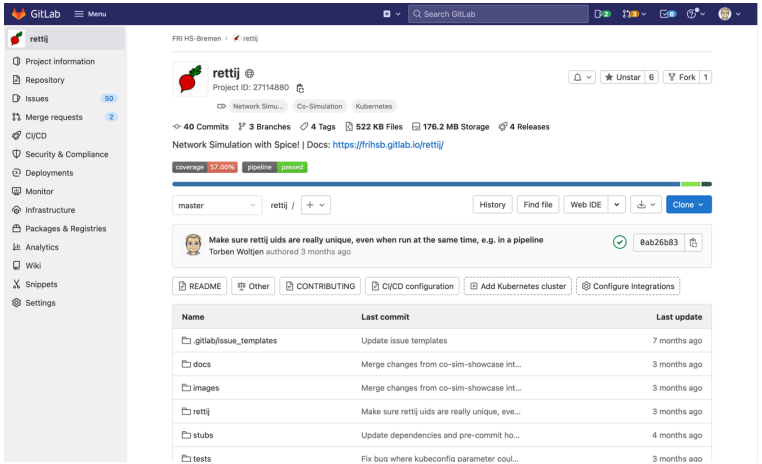
Network traffic is real

- Export dumps from each node
  - After / during simulation
- Analise with Wireshark
- Add IDS/SIEM

```
10:07:28.541382 02:00:00:00:ff:01 > 02:00:00:00:ff:02, ethertype IPv4 (0x0800),
    length 80: 192.168.0.10.44984 > 192.168.1.10.9999: Flags [P.], seq
    785500028:785500042, ack 695056372, win 510, options [nop,nop,TS val
    3366767962 ecr 1158610599], length 14
        0x0000:  4500 0042 63a7 4000 3f06 55aa c0a8 000a  E..Bc.@.?.U.....
        0x0010:  c0a8 010a afb8 270f 2ed1 c77c 296d b7f4  ......'....|)m..
        0x0020:  8018 01fe 8299 0000 0101 080a c8ac cd5a  ...............Z
        0x0030:  450e fea7 7b22 7661 6c75 6522 3a20 3136  E...{"value":.16
        0x0040:  7d0a                                     }.
10:07:36.946983 02:00:00:00:ff:01 > 02:00:00:00:ff:05, ethertype IPv4 (0x0800),
    length 80: 192.168.0.10.45090 > 192.168.1.10.9999: Flags [P.], seq
    1836877175:1836877189, ack 1944996579, win 510, options [nop,nop,TS val
    3366776367 ecr 1158619003], length 14
        0x0000:  4500 0042 e4a8 4000 3f06 d4a8 c0a8 000a  E..B..@.?.......
        0x0010:  c0a8 010a b022 270f 6d7c 8577 73ee 4ae3  ....."'.m|.ws.J.
        0x0020:  8018 01fe 8299 0000 0101 080a c8ac ee2f  .............../
        0x0030:  450f 1f7b 7b22 7661 6c75 6522 3a20 3232  E..{{"value":.22
        0x0040:  7d0a                                     }.
10:07:36.949176 02:00:00:00:ff:05 > 02:00:00:00:ff:02, ethertype IPv4 (0x0800),
    length 80: 192.168.0.10.45090 > 192.168.1.10.9999: Flags [P.], seq 0:14, ack
     1, win 510, options [nop,nop,TS val 3366776367 ecr 1158619003], length 14
        0x0000:  4500 0042 e4a8 4000 3e06 d5a8 c0a8 000a  E..B..@.>.......
        0x0010:  c0a8 010a b022 270f 6d7c 8577 73ee 4ae3  ....."'.m|.ws.J.
        0x0020:  8018 01fe f0fa 0000 0101 080a c8ac ee2f  .............../
        0x0030:  450f 1f7b 7b22 7661 6c75 6522 3a20 2d32  E..{{"value":.-2
        0x0040:  327d                                     2}
```

Presenting rettijj network simulator

- Available at https://gitlab.com/frihsb/rettij
- MIT licence ☺
- Default components
  - simple-router
    - FRRouting (BGP, OSPFv3, RIPv2, etc..)
  - simple-switch
  - simple-runner (debian)



rettij
network simulator

kubernetes

docker

python powered

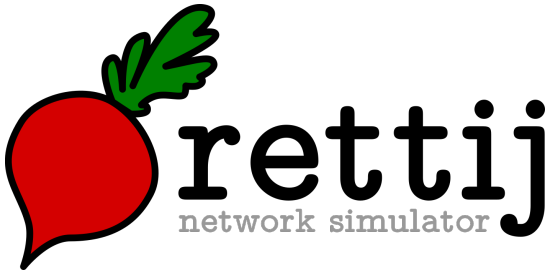
Agenda

1 Introduction Smart Grid Security Research
2 Structure and Usage of rettij
3 Practical Application Scenario
4 Conclusion

Conclusion

Energy transition

- Requires ICT in smart grid co-simulations
- ICT security cannot be tested on real power systems
- Smart grid simulation requires co-simulators



rettij network simulator

- Provides integration for co-simulation
- Integrate more real ICT components into smart grid simulations
- Supports to design new security tools
- Uses modern distributed container orchestration software

Hochschule Bremen
City University of Applied Sciences

HSB

Thanks!
Q / A

Research Group for Information Security and Computer Networks
Bremen, Germany
Bastian.Fraune@hs-bremen.de
www.fri.hs-bremen.de