12.-13. November in Karlsruhe

energieinformatik2015

RSE Ricerca Sistema Energetico

13 November 2015

Cyber Security Analysis of Smart Grid Communications with a Network Simulator

Roberta Terruggia and Giovanna Dondossola

RSE Ricerca sul Sistema Energetico

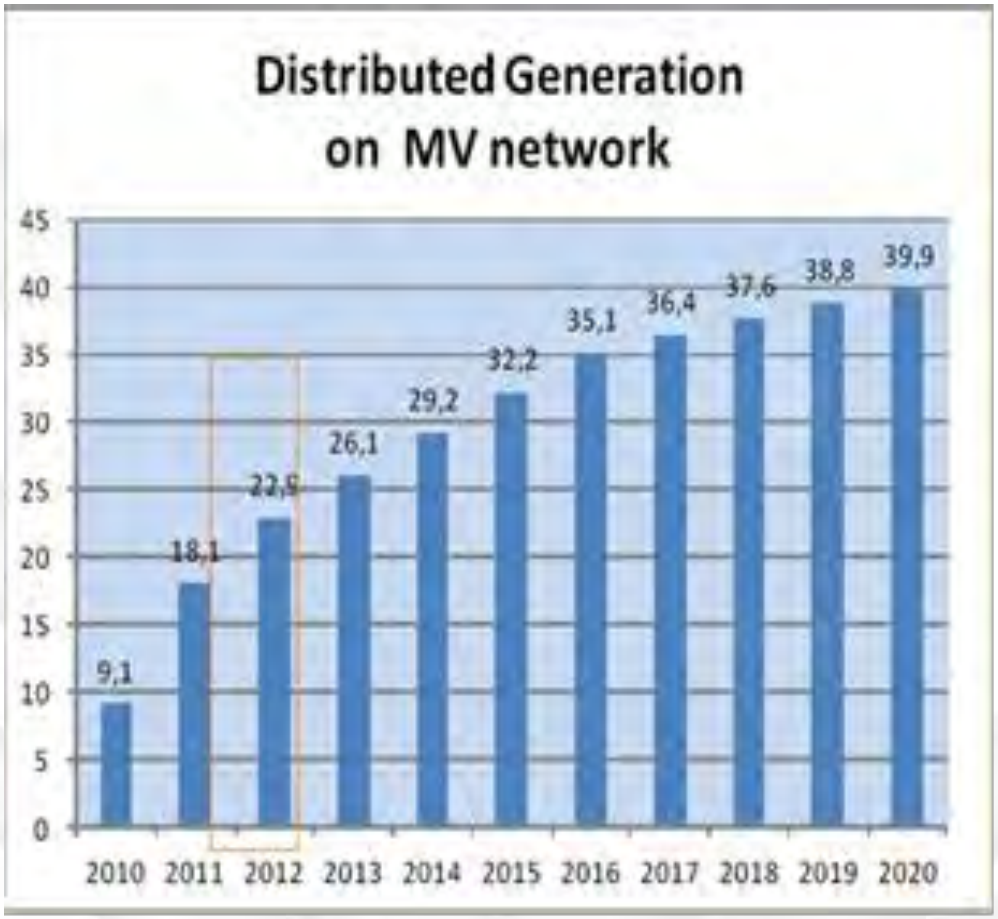
Milano ITALY

SMART C²NET

Agenda

- The Medium Voltage Control use case & Medium Voltage testbed
- Simulation model
  - Communication
  - DoS attack
  - LTE mobile technology
- Results
  - Attack setup parameters
  - Scaling up the model
  - LTE model
- Conclusion

DER (Distributed Energy Resource) forecast in MV grids: a realistic grid 2020 scenario



Source: ENEL, CIRED 2012

About 40 GW from installed renewables (PV/wind) connected to MV grids within 2020 in Italy

Connection rules (Norm CEI 0-16)

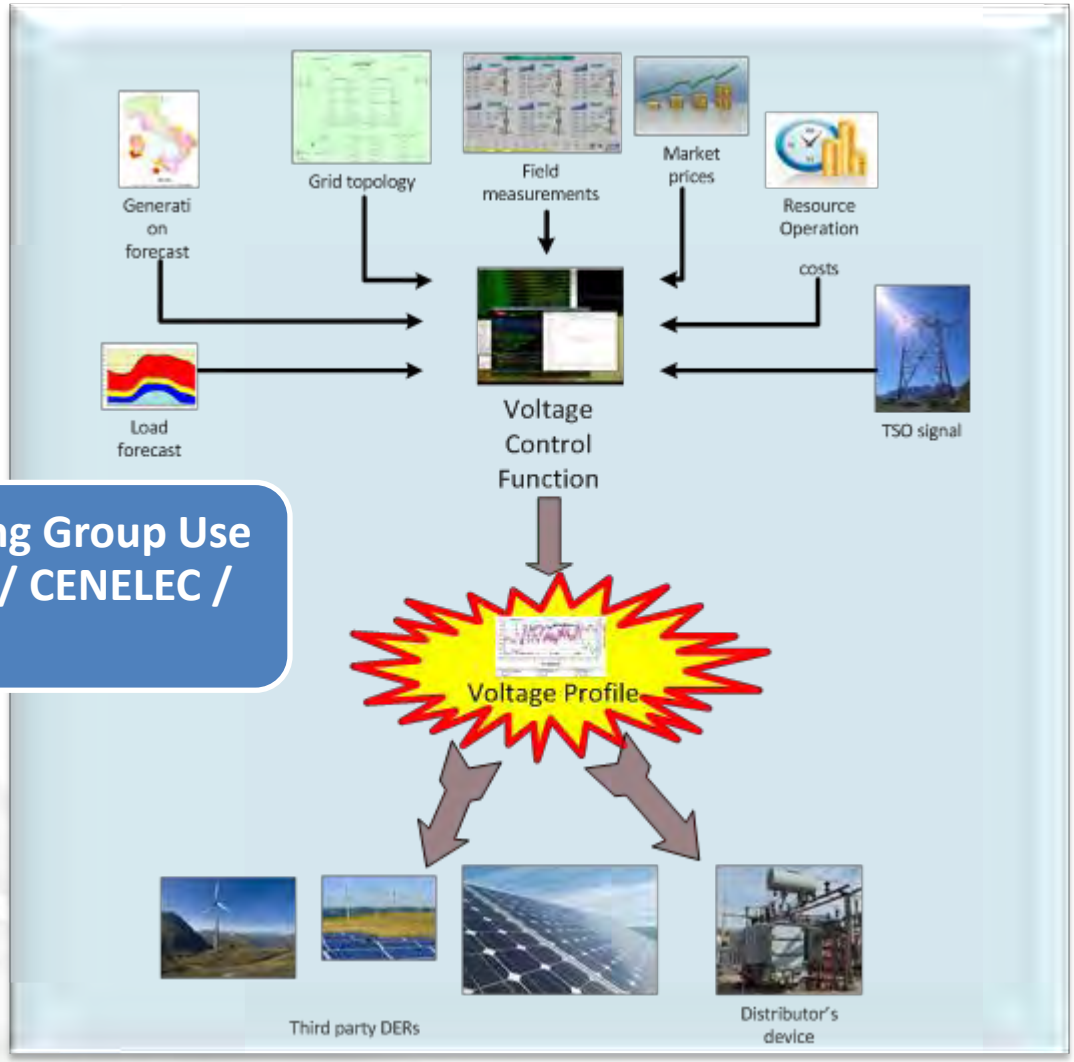
MV DER power

- 200 kW < Pn < 6 MW (mandatory)

Extended grid topology

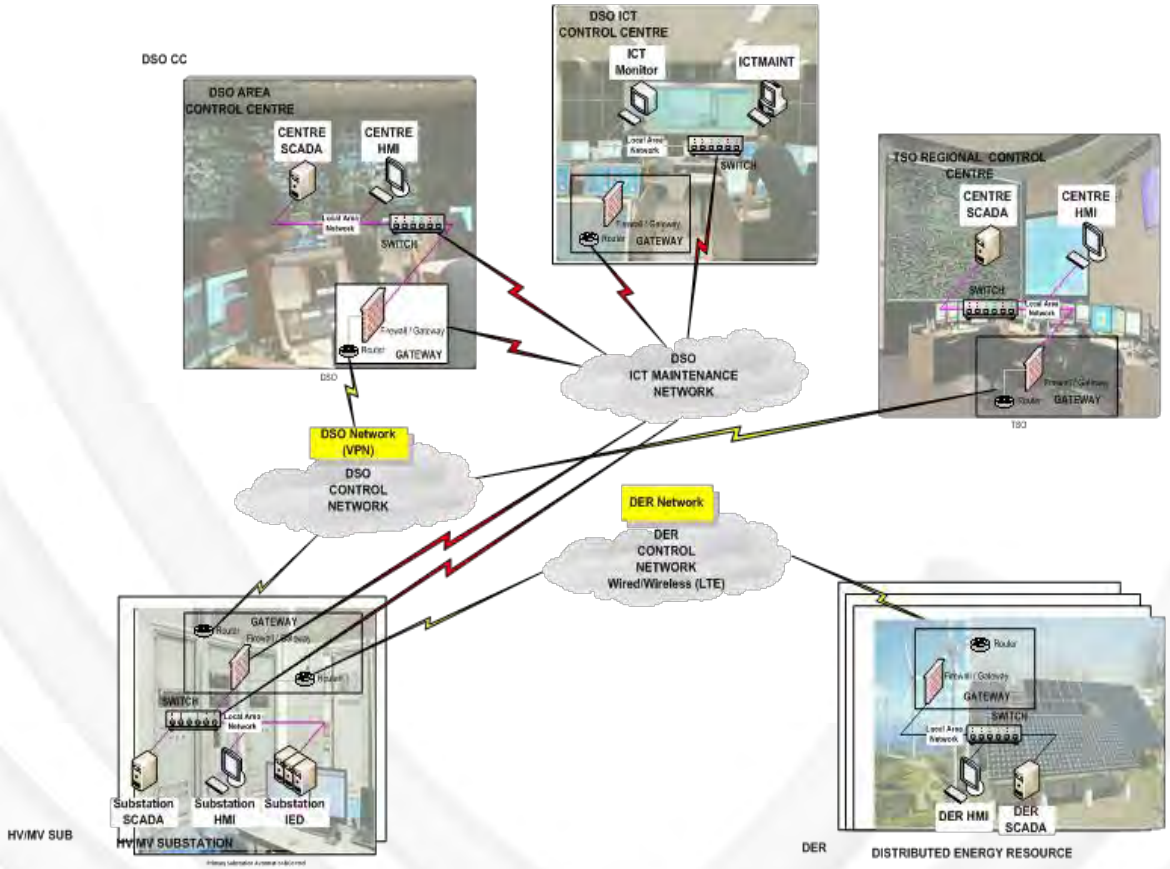
- about 10% of new HV/MV substations

Medium Voltage Control



Based on SGSP Working Group Use Case WGSP-0200 CEN / CENELEC / ETSI

RSE PCS-ResTest Lab Layout



Focus: security of communications

Objective: run cyber security experiments over realistic VC scenarios

Technologies

- Data models
  - IEC 61850 Part 7
    - DER data models: IEC 61850 - 7 - 420
- Communication **protocols**
  - IEC 61850 Part 8-1 ed. 2 ->Manufacturing Message Specification (MMS)
- **Security** measures
  - End-to-end security -> IEC 62351-3 (TLS) ed.2
  - Monitoring -> IEC 62351-7
- Network **technologies**
  - Wired/wireless (Ethernet, LTE)

MV Control Test Bed

Grid and ICT Control Centres

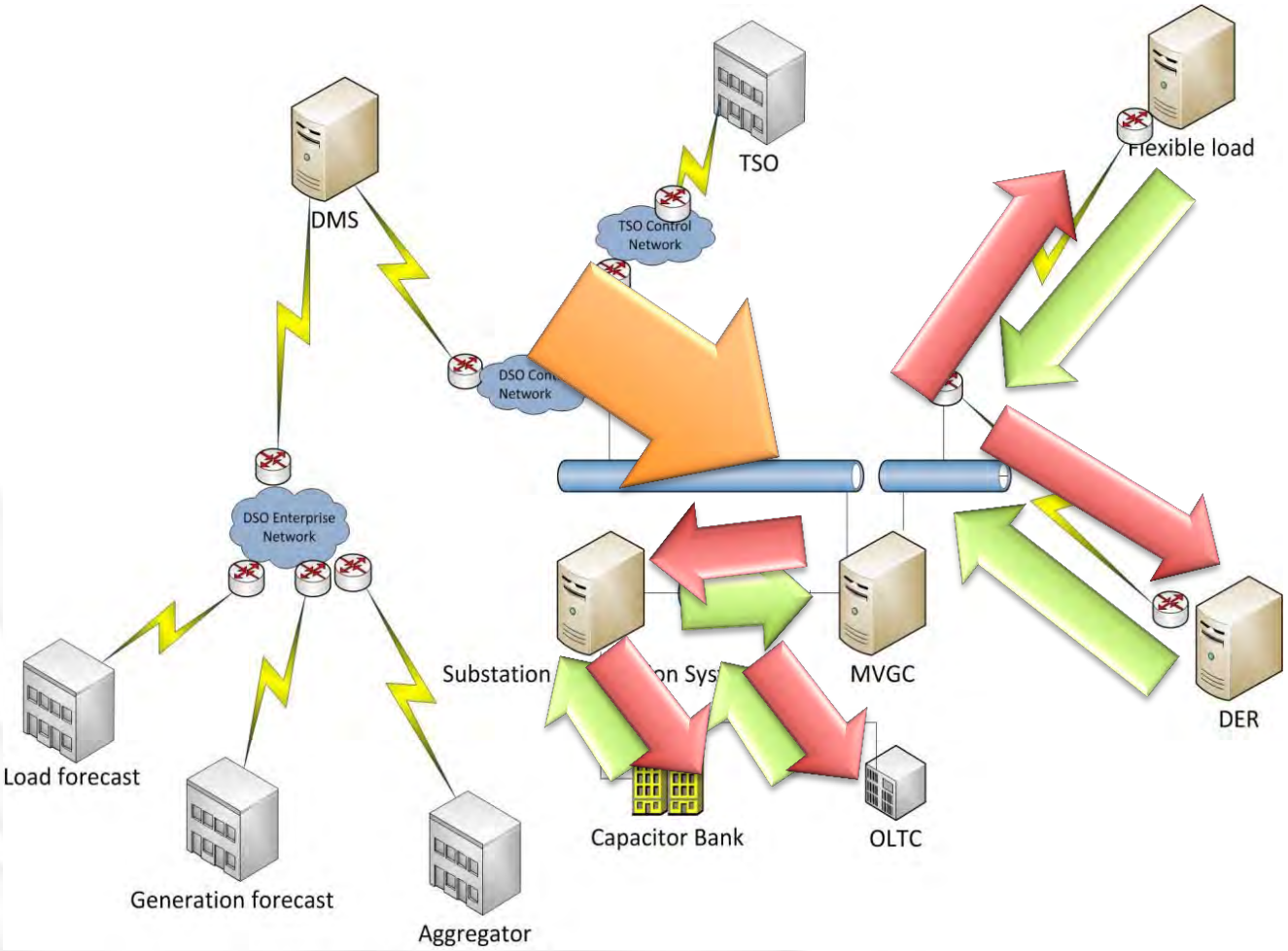
SNMP, NTP, PTP
IEC 60870-5-104
ACL, VPN, IPSEC

Substation Control

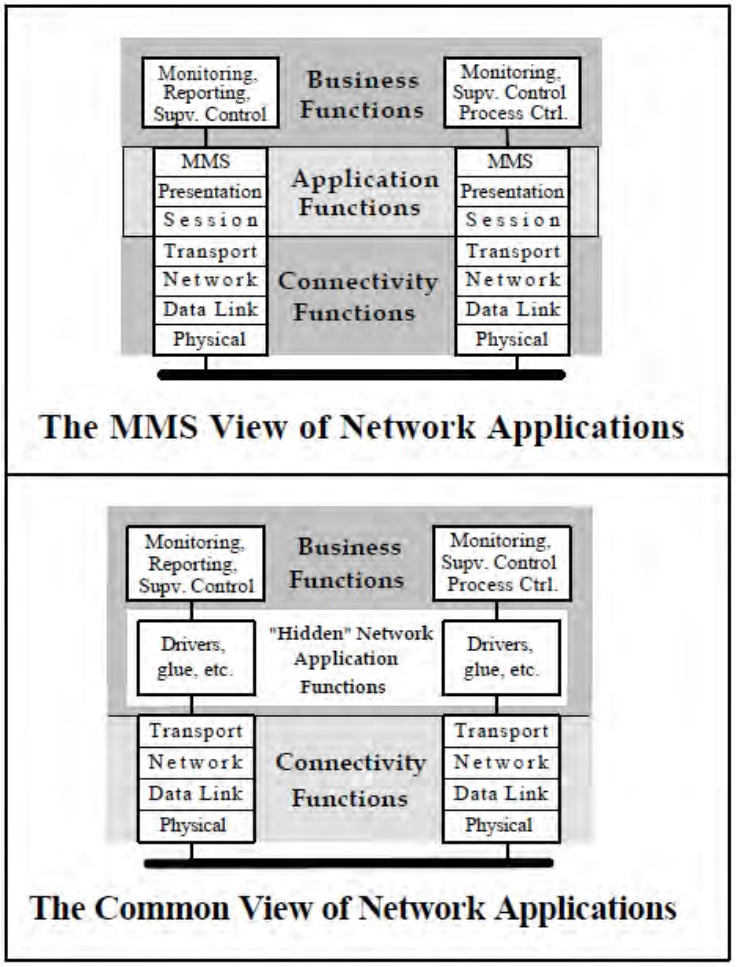
IEC 61850-7(-420)
IEC 61850-8-1
ACL, IEC 62351-3, TLS

DER Control

Information Flows – RES measurements



IEC 61850 – MMS



IEC 61850-8: Specific communication service mapping (SCSM) -> IEC 61850-8-1: Mappings to MMS

Manufacturing Message Specification ISO 9506

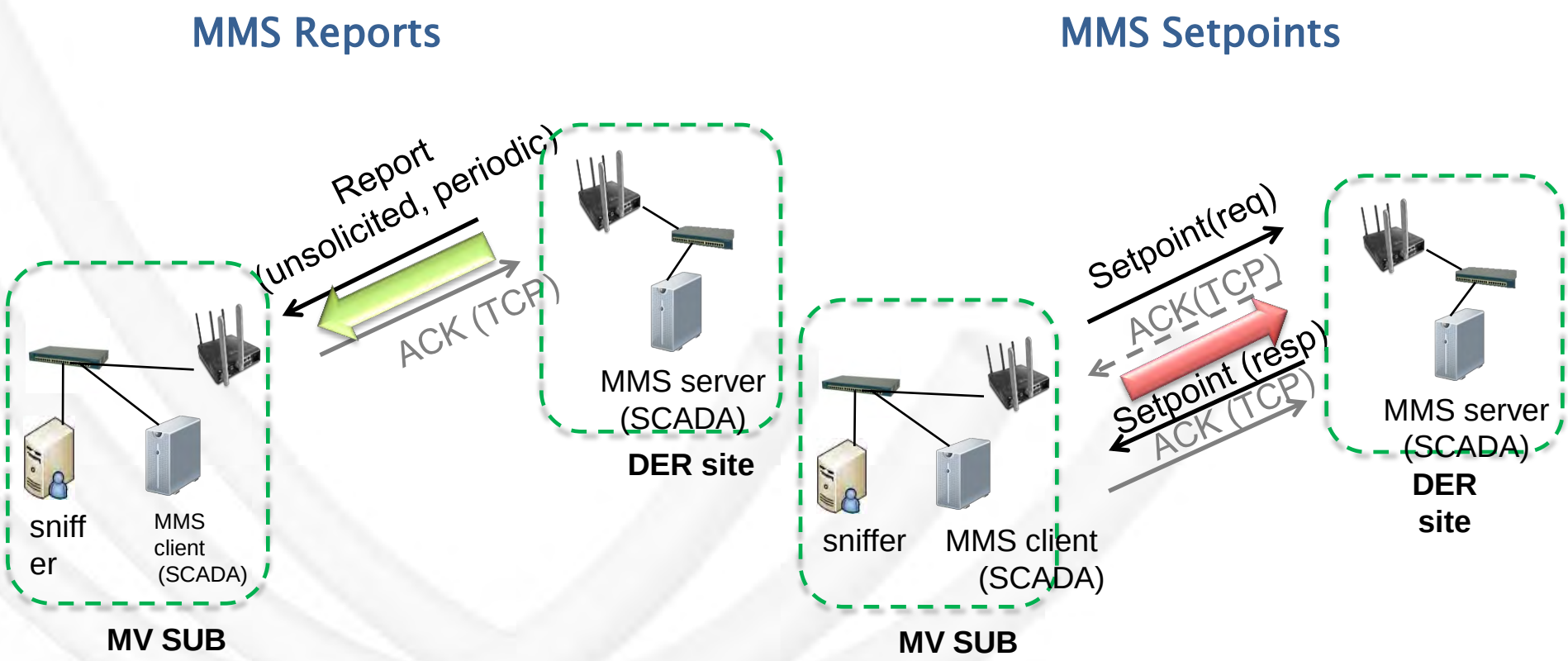
Application Level Protocol

Internationally standardized messaging system for the exchange of real-time data and supervisory control info

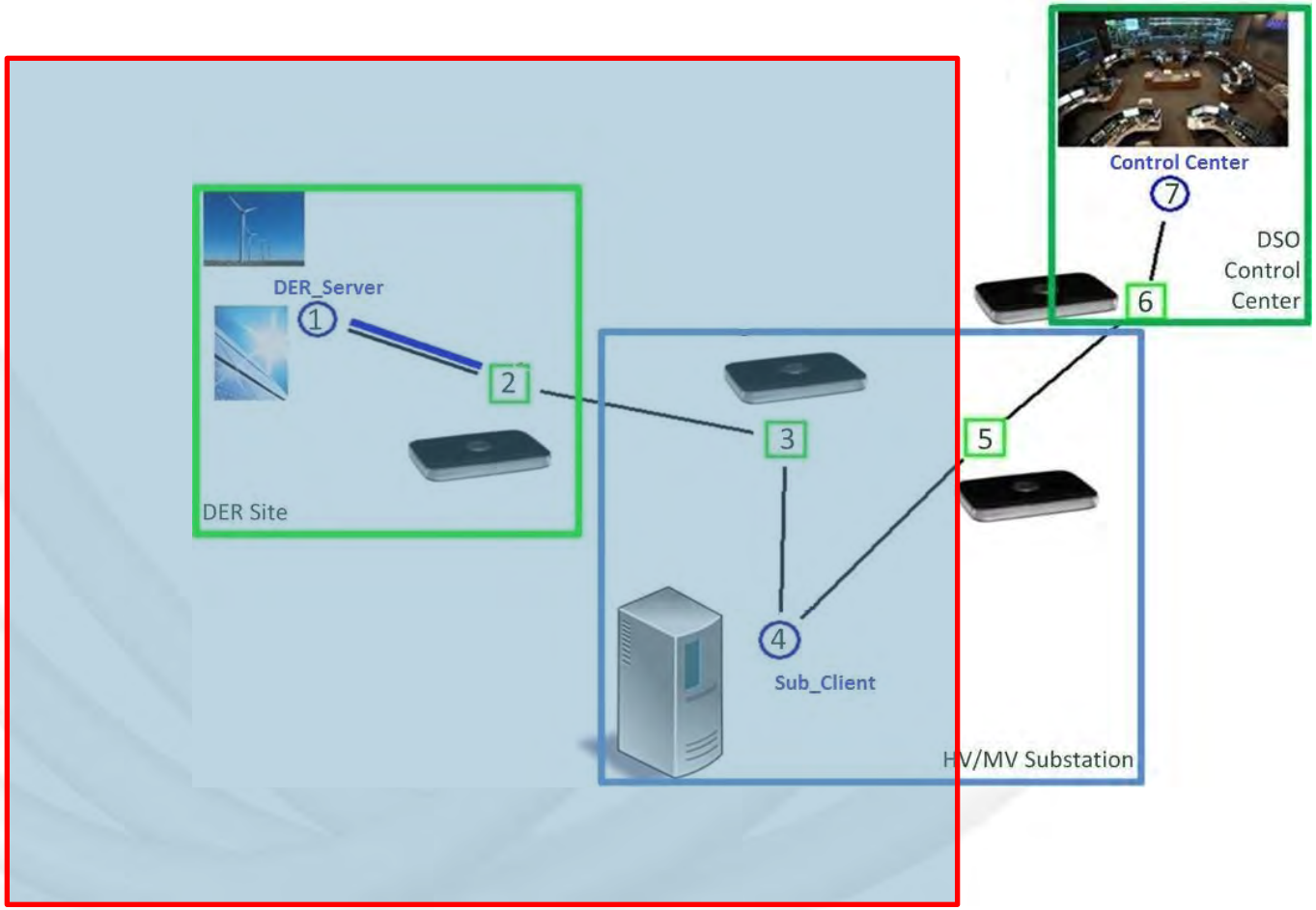
Independent of:

- the application function being performed
- the device vendor

Substation/DER communications

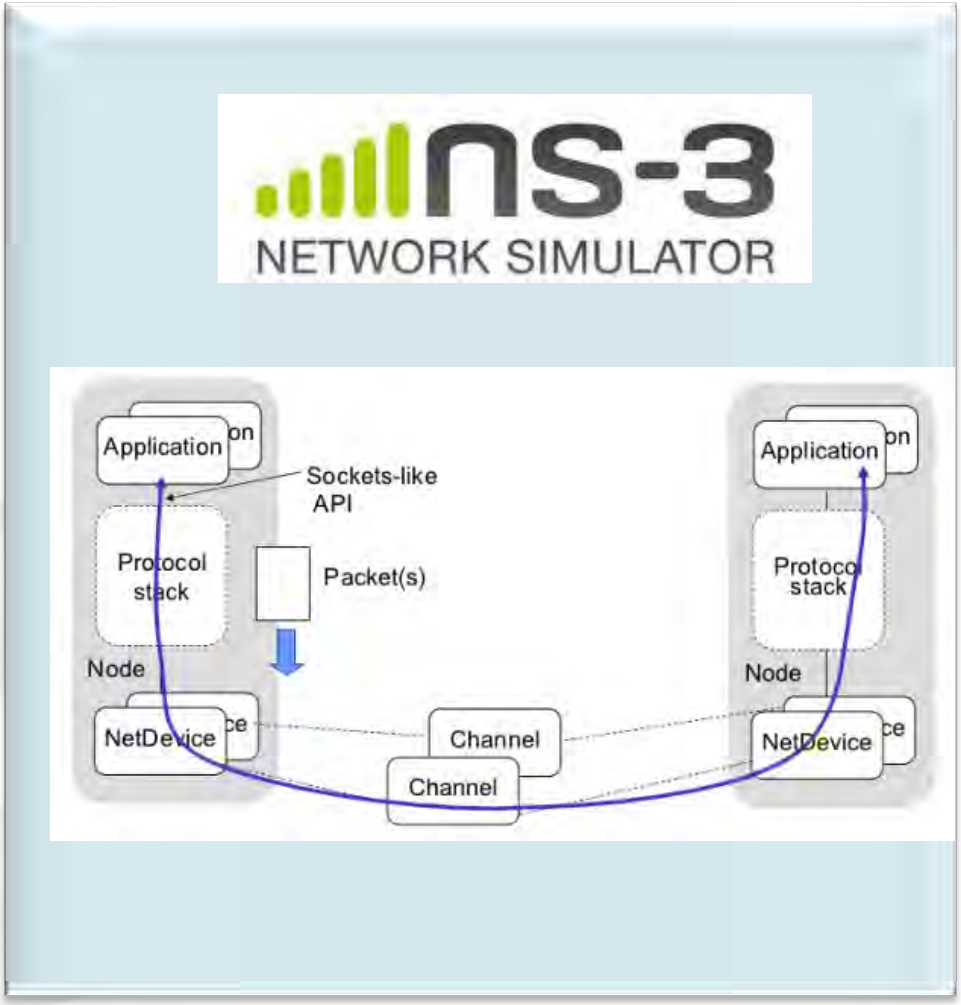


Focus of the simulation model



Network simulator: Why ns-3?

- C++ (no Otlc)
- IP address
- Sockets
- More interfaces per node
- Packets contain real string of bytes
- Integration of real source code - application layer protocols
- Pcap traces



ns-3: DCE framework

Direct Code Execution:

- Direct Code Execution (DCE) is a framework for ns-3 that provides facilities to **execute**, within ns-3, **existing implementations** of userspace and kernelspace network protocols or applications without source code changes.
  - Include MMS client / server testbed implementation
  - Include attack tools

ns-3 model

7 nodes

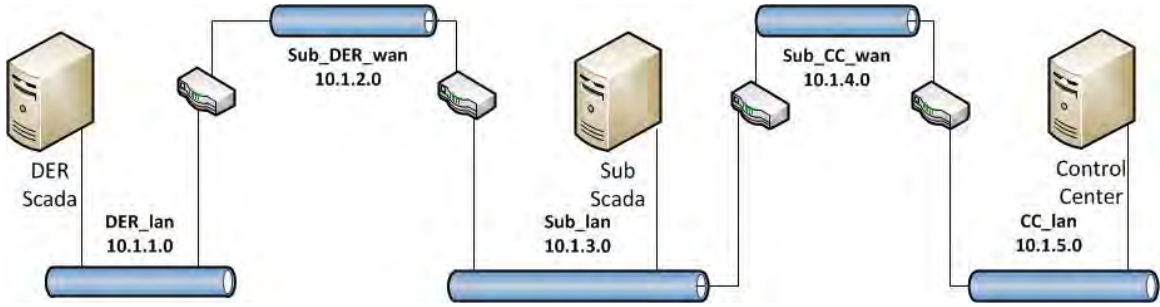
- Router nodes -> 2 NetDevices
- Server nodes -> 1 NetDevice

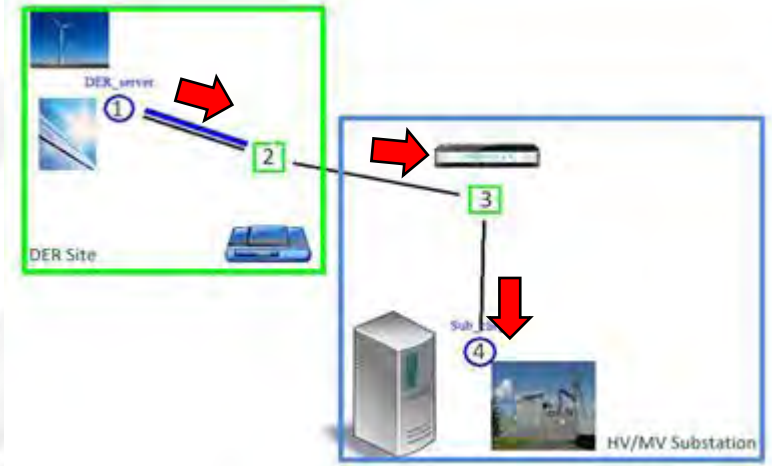
5 networks

- IP address

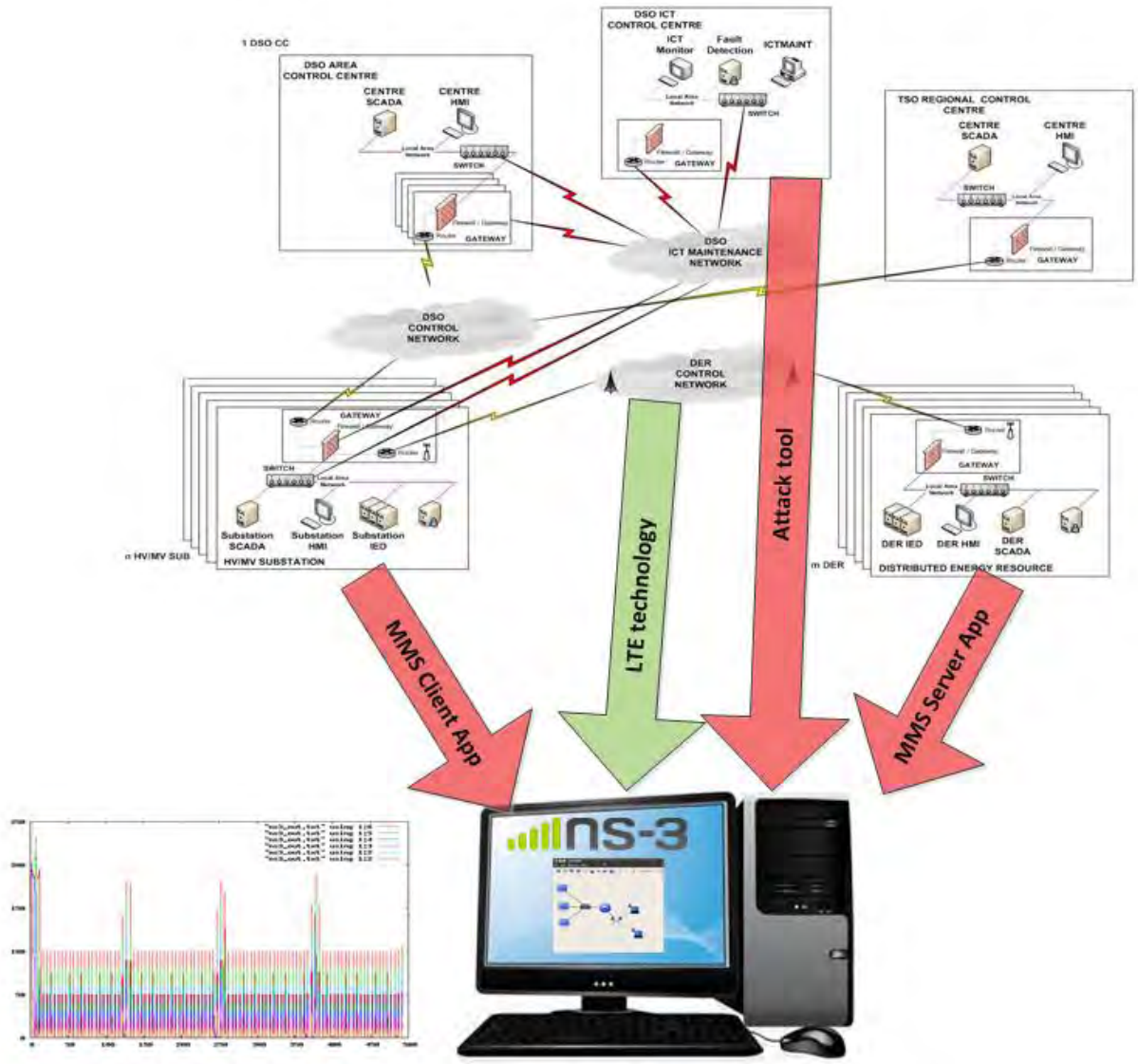
Measurements

- From DER Scada to MVGC
- TCP stack (TcpSocketFactory)
  - sink port 102
- Data rate 500 Kbps





Tools from the testbed



Testbed – Simulation alignment
Information flow

48	14.964851	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
49	16.978357	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
50	16.978454	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
51	18.990947	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
52	18.991044	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
53	21.004561	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
54	21.004657	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
56	23.007143	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
57	23.007238	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
58	25.022732	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
59	25.022828	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
60	27.036353	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
61	27.036449	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
62	29.038935	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
63	29.039028	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]
64	31.052553	192.168.1.43	158.47.121.32	MMS	179	unconfirmed-PDU
65	31.052653	158.47.121.32	192.168.1.43	TCP	66	35314 > iso-tsap [ACK]

62	17.002374	10.1.1.1	10.1.3.1	MMS	unconfirmed-PDU
63	17.204617	10.1.3.1	10.1.1.1	TCP	49153→102 [ACK]
64	19.002374	10.1.1.1	10.1.3.1	MMS	unconfirmed-PDU
65	19.204617	10.1.3.1	10.1.1.1	TCP	49153→102 [ACK]
66	21.002374	10.1.1.1	10.1.3.1	MMS	unconfirmed-PDU
67	21.204617	10.1.3.1	10.1.1.1	TCP	49153→102 [ACK]
68	23.002374	10.1.1.1	10.1.3.1	MMS	unconfirmed-PDU
69	23.204617	10.1.3.1	10.1.1.1	TCP	49153→102 [ACK]
70	25.002374	10.1.1.1	10.1.3.1	MMS	unconfirmed-PDU
71	25.204617	10.1.3.1	10.1.1.1	TCP	49153→102 [ACK]
72	27.002374	10.1.1.1	10.1.3.1	MMS	unconfirmed-PDU
73	27.204617	10.1.3.1	10.1.1.1	TCP	49153→102 [ACK]
74	29.002374	10.1.1.1	10.1.3.1	MMS	unconfirmed-PDU
75	29.204617	10.1.3.1	10.1.1.1	TCP	49153→102 [ACK]

Testbed trace

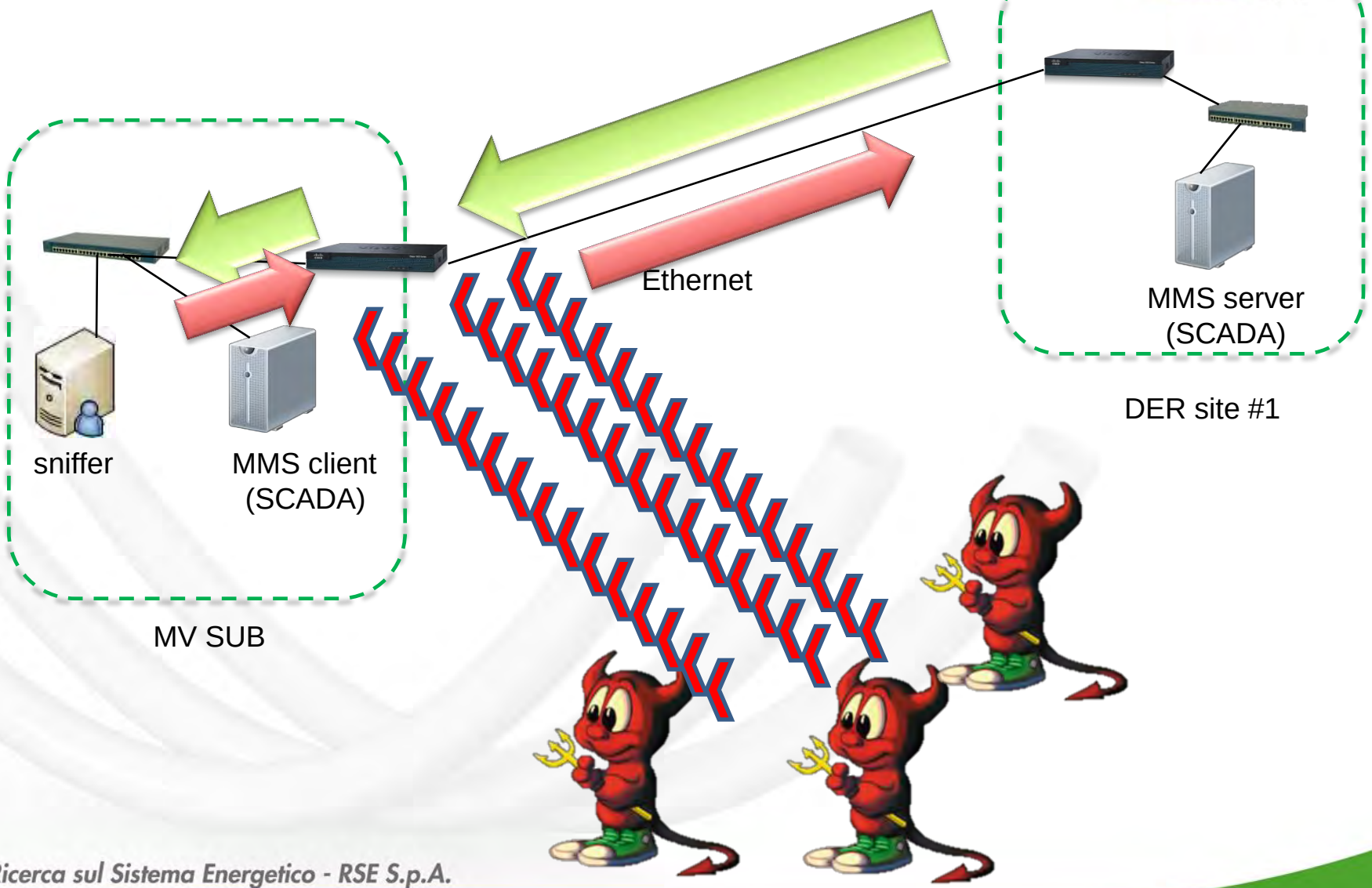
Simulation trace

Testbed – Simulation alignment
Packet content

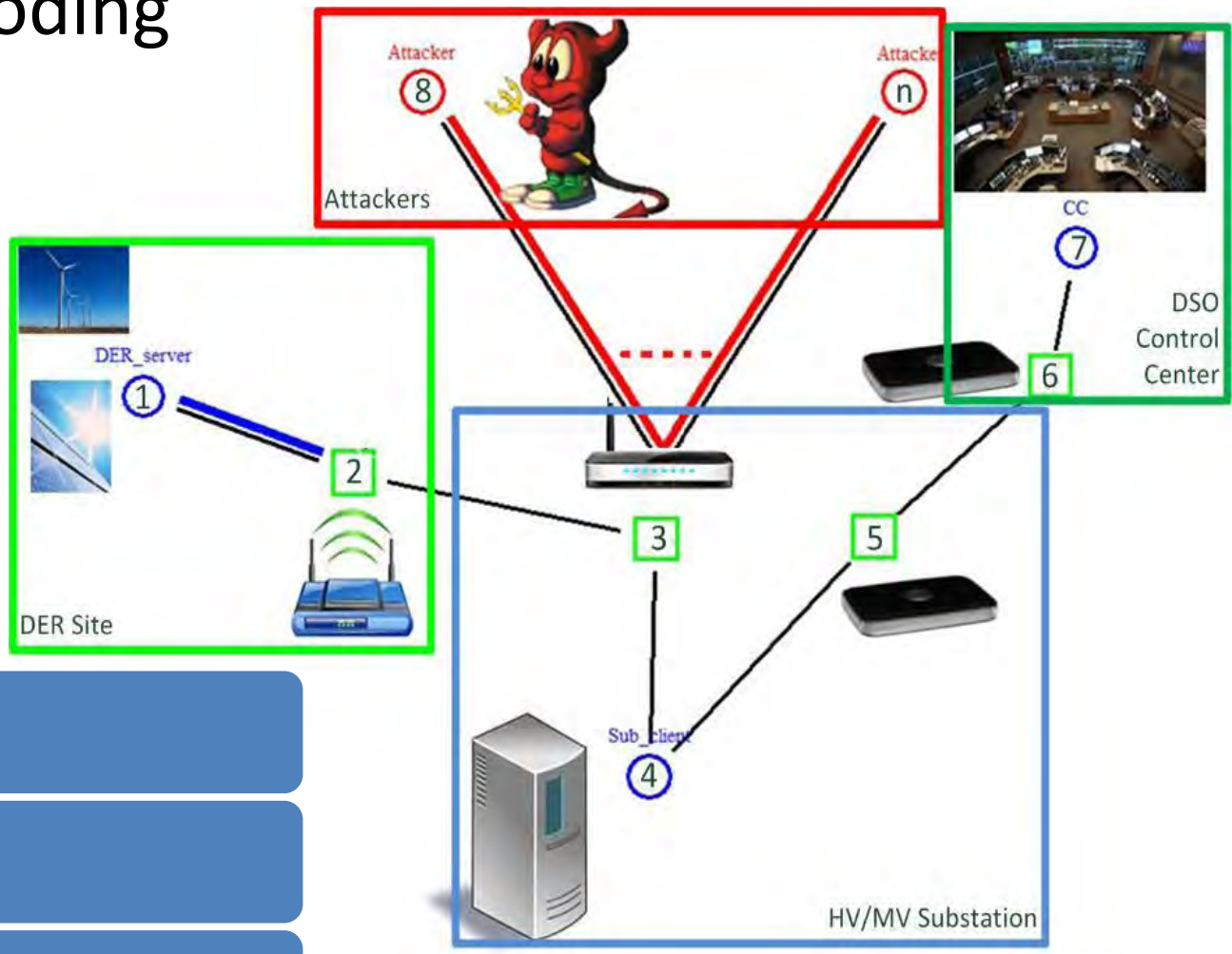
Testbed trace

Simulation trace

Flooding Attack



Attack model: Flooding



UDP traffic generator

Source one or more attackers (node 8 to node n)

Target the substation router (node 3).

ns-3 DCE: attack trace

Node 8..n -> RSE testbed flooding attack tool

- UDP packet size: parameter of the scenario
- Target-> router@substation

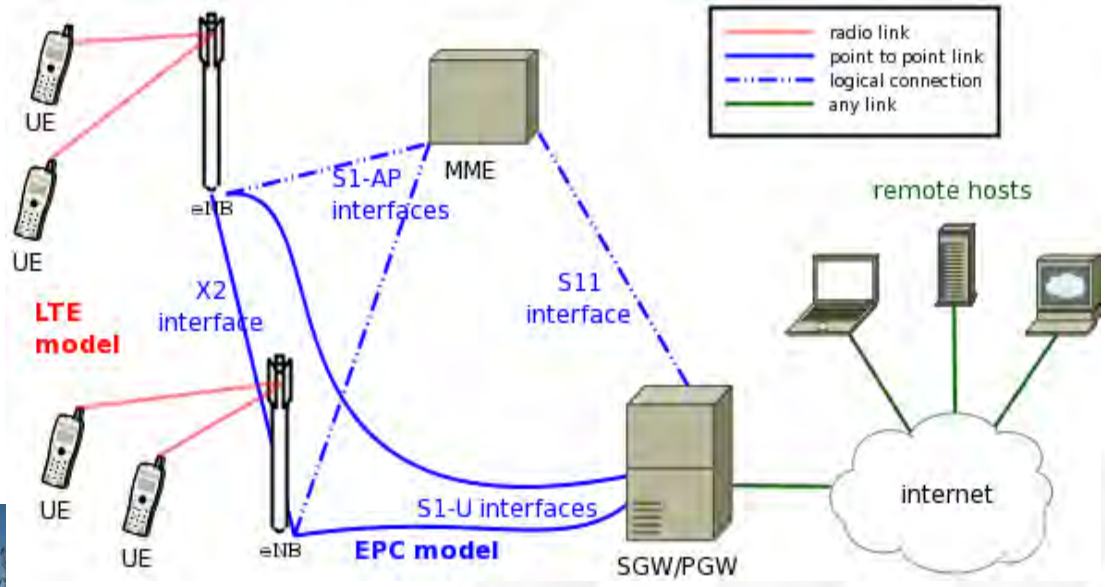
No.	Time	Source	Destination	Protocol	Length	Info
66	9.490018	10.1.1.1	10.1.3.1	MMS	222	unconfirmed-PDU
67	9.690041	10.1.3.1	10.1.1.1	TCP	64	49153 > iso-tsap [ACK] Seq=805 Ack=5497 Win=65535 Len=0
68	11.490018	10.1.1.1	10.1.3.1	MMS	222	unconfirmed-PDU
69	11.690041	10.1.3.1	10.1.1.1	TCP	64	49153 > iso-tsap [ACK] Seq=805 Ack=5661 Win=65535 Len=0
70	13.490018	10.1.1.1	10.1.3.1	MMS	222	unconfirmed-PDU
71	13.690041	10.1.3.1	10.1.1.1	TCP	64	49153 > iso-tsap [ACK] Seq=805 Ack=5825 Win=65535 Len=0
72	15.490018	10.1.1.1	10.1.3.1	MMS	222	unconfirmed-PDU
73	15.690041	10.1.3.1	10.1.1.1	TCP	64	49153 > iso-tsap [ACK] Seq=805 Ack=5989 Win=65535 Len=0
74	16.495988	00:00:00_00:00	Broadcast	ARP	64	Who has 10.1.2.1? Tell 10.1.2.3
75	16.495988	00:00:00_00:00	00:00:00_00:00:0	ARP	64	10.1.2.1 is at 00:00:00:00:00:05
76	16.496006	10.1.2.3	10.1.2.1	UDP	146	Source port: ddi-udp-1 Destination port: interwise
77	16.496019	10.1.2.3	10.1.2.1	UDP	146	Source port: ddi-udp-1 Destination port: interwise
78	16.496032	10.1.2.3	10.1.2.1	UDP	146	Source port: ddi-udp-1 Destination port: interwise
79	16.496077	10.1.2.3	10.1.2.1	Syslog	558	Attack UDP message from: NODE_4 to 10.1.2.1 : 514\0008\000\
80	16.496123	10.1.2.3	10.1.2.1	Syslog	558	Attack UDP message from: NODE_4 to 10.1.2.1 : 514\0008\000\
81	16.496168	10.1.2.3	10.1.2.1	Syslog	558	Attack UDP message from: NODE_4 to 10.1.2.1 : 514\0008\000\
82	16.496214	10.1.2.3	10.1.2.1	Syslog	558	Attack UDP message from: NODE_4 to 10.1.2.1 : 514\0008\000\
83	16.496260	10.1.2.3	10.1.2.1	Syslog	558	Attack UDP message from: NODE_4 to 10.1.2.1 : 514\0008\000\
84	16.496305	10.1.2.3	10.1.2.1	Syslog	558	Attack UDP message from: NODE_4 to 10.1.2.1 : 514\0008\000\

ns-3: trace analysis

Simulation trace analysis

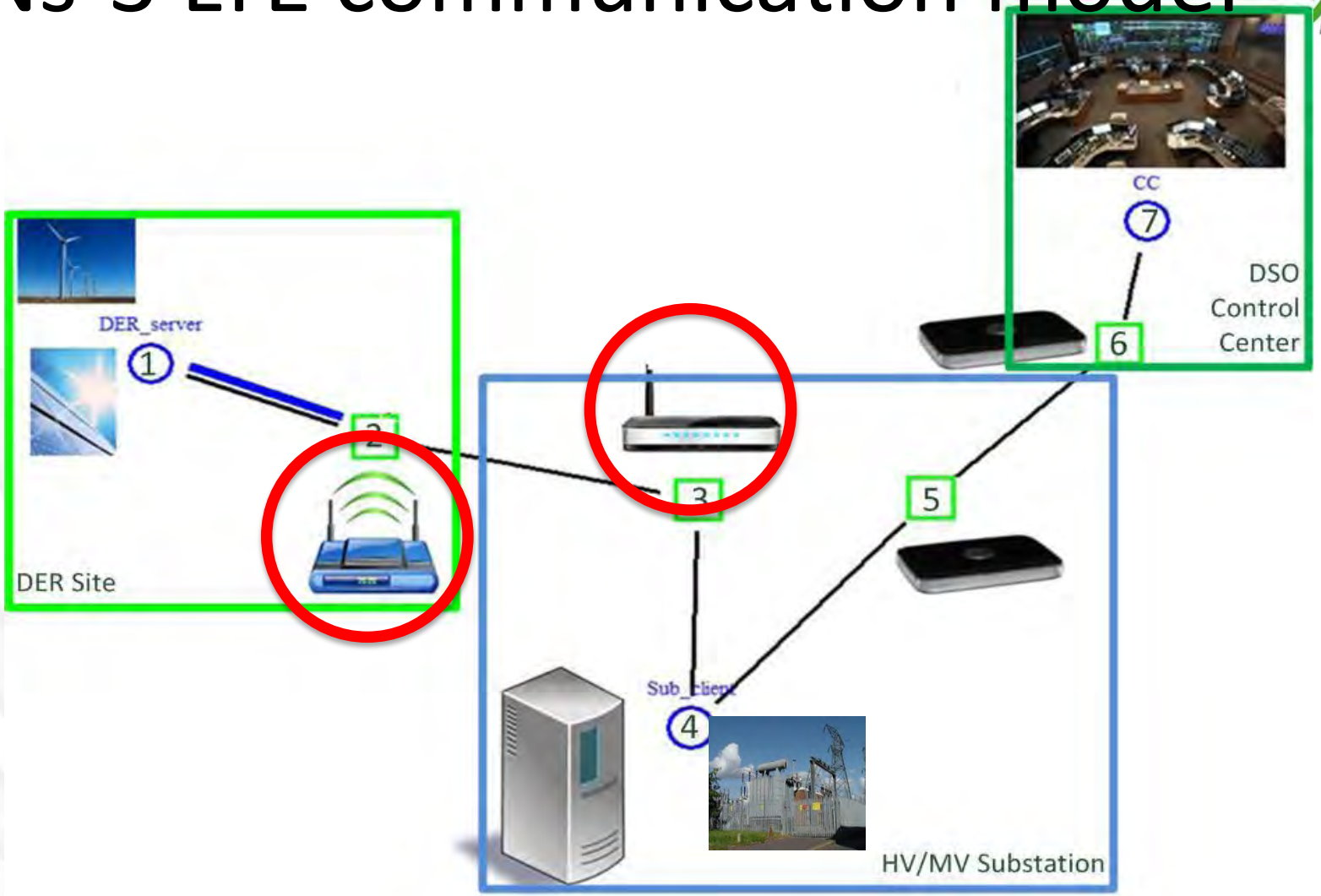
- Varying parameters
  - Number of attackers
  - Packet size
  - Packet rate
- Same indicators as testbed
  - Report RTT, retransmissions, losses …

LTE mobile technology

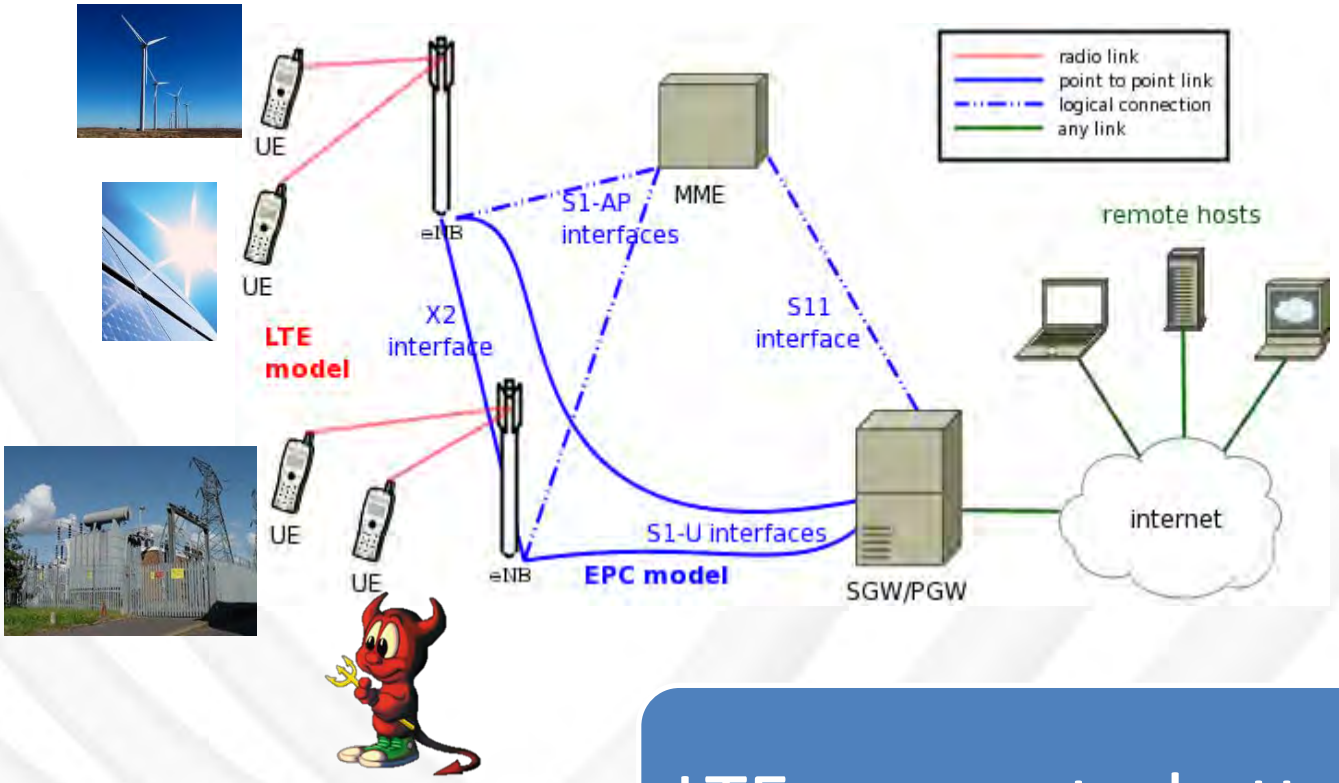


HV/MV substation - DERs communication by means of LTE technology

Ns-3 LTE communication model

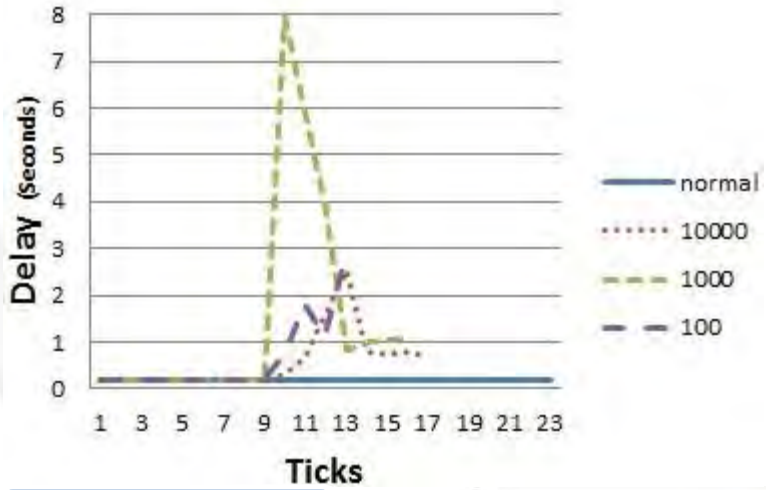


Ns-3 LTE communication model

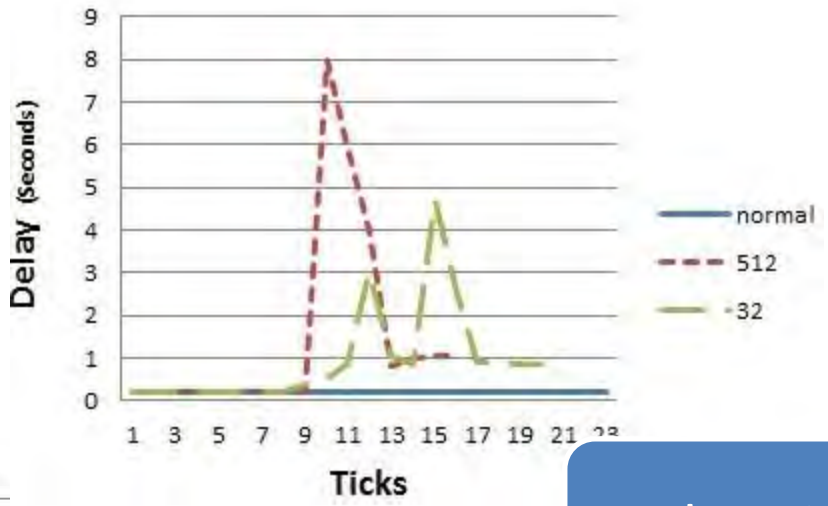


LTE connected attackers

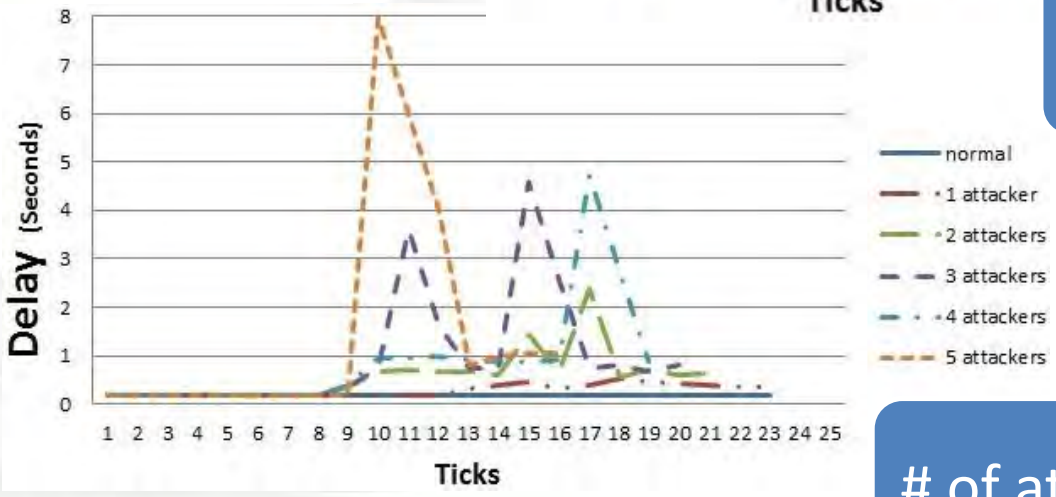
Sensitivity analysis



Packet rate

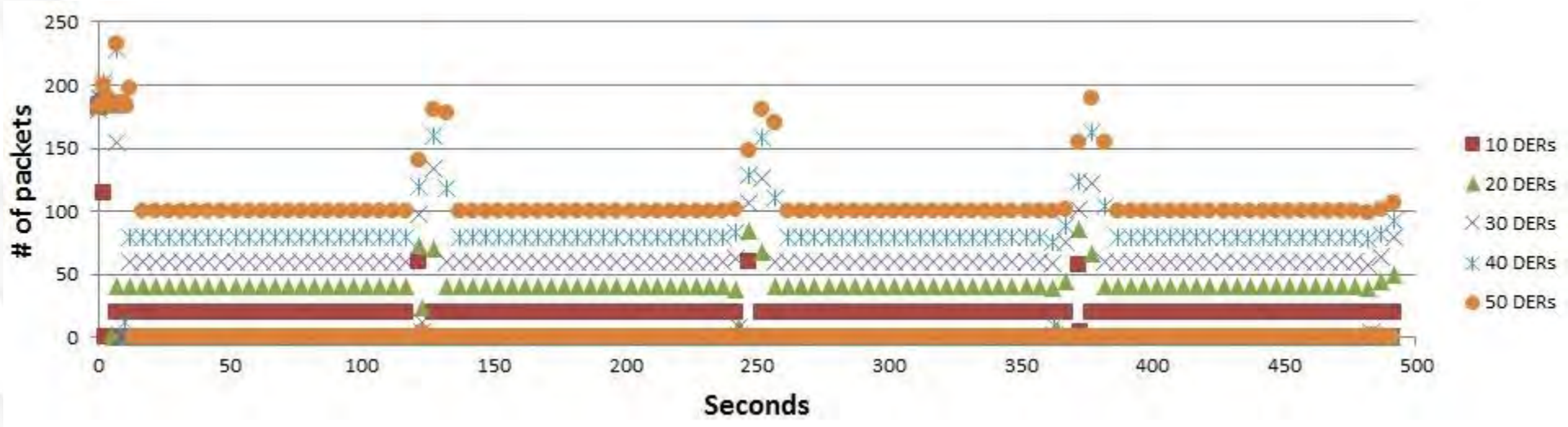


Packet size

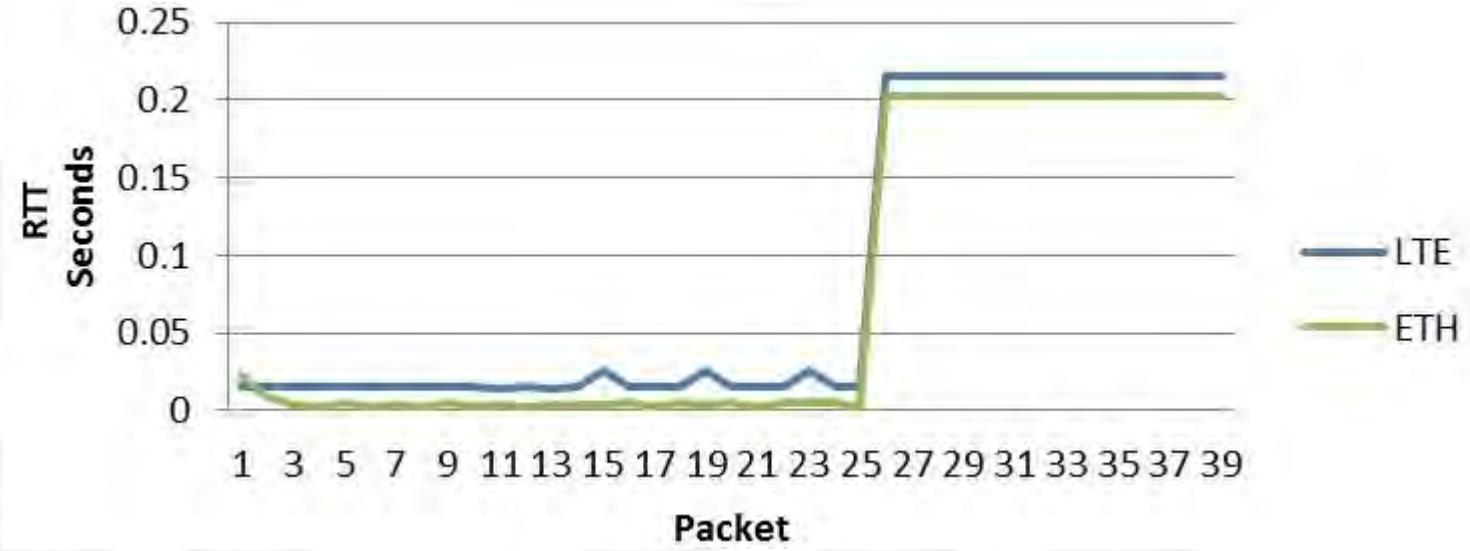


# of attackers

Scaling up the model



LTE model


0.25
0.2
0.15
0.1
0.05
0
RTT Seconds
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39
Packet
LTE
ETH

Conclusion

Simulation **model** of the **communications** and attacks for Voltage Control function in Smart Grid

Model aligned with the **testbed**

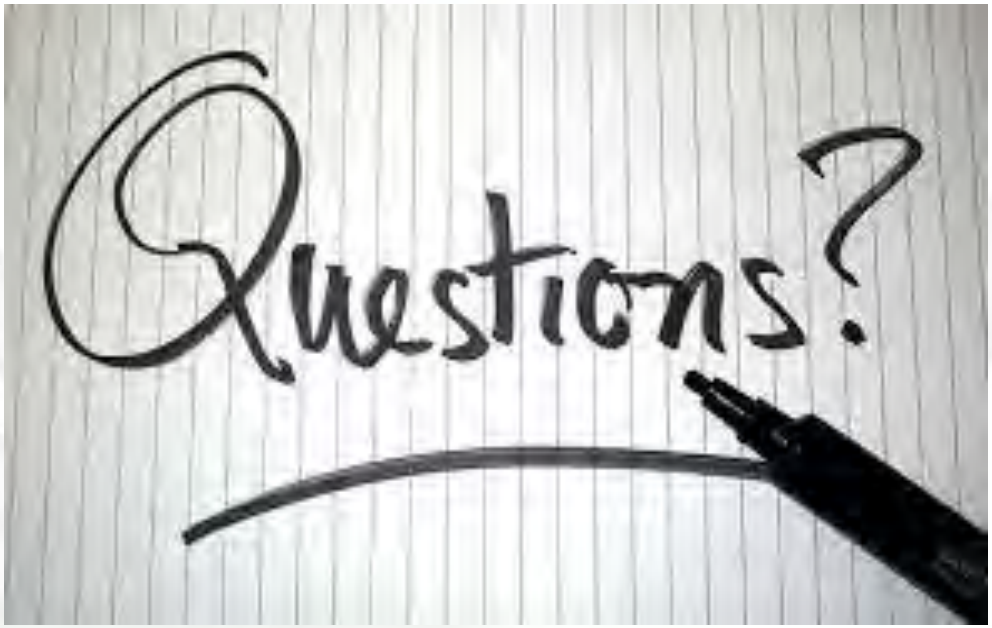
The attack scenarios modeling activity helps to **select more significant attack scenarios** to be demonstrate

- Varying the attack parameters for flooding attack:
  - Number of attackers
  - Packet size
  - Packet rate

Analysis of several scenarios **scaling up** the model size in order to demonstrate scenarios not feasible in the testbed

- Including the ns-3 LTE module
- Varying
  - the number of DERs
  - the number of attackers
  - LTE parameters


THANK
YOU!


Questions?