# Cyber Security Analysis of Smart Grid Communications with a Network Simulator

Roberta Terruggia[✉] and Giovanna Dondossola

Transmission & Distribution Technologies Department Ricerca
Sul Sistema Energetico, Milan, Italy
{Roberta.Terruggia,Giovanna.Dondossola}@rse-web.it

**Abstract.** This paper proposes a methodology for analyzing communication security in smart grid domains. As an application case, in this paper, we focus on information exchanges between Distributed Energy Resources (DER) and primary substations employed in the medium voltage control of active grids. The ICT (Information and Communication Technology) architecture of the application is modeled through a network simulator integrating the standard communication modules and the attack processes experimentally evaluated in a voltage control cyber security testbed. The paper presents the cross validation of the simulation model with the experimental traces, the sensitivity analysis with the validated model of the flooding attack effects on the communication performance and the scaling-up capability of the simulation model for the analysis of more realistic grid size.

**Keywords:** Cyber security · Smart grid · DER · Communication · MMS

## 1 Introduction

The evolution of the energy infrastructures connecting Distributed Energy Resources (DER) at different levels of the power grids leads to rethink the functionalities of the Supervisory Control And Data Acquisition (SCADA) systems. The role of the ICT (Information and Communication Technology) infrastructure is becoming more and more fundamental and the communications among power control entities become crucial assets of the grid operation. Such ICT architectures of future smart grids may be, especially in the case of DER, based on heterogeneous and third party telecommunication services and so prone to cyber attacks. This advanced scenario pushes the cyber security issues and the need of managing ICT risks at a top position in the smart grid agenda. The innovative idea driving the research activity presented in the paper is to use an ICT network simulator for developing a sufficiently accurate communication model providing reliable evaluations of the cyber attack effects on the legal communications. The accuracy of the simulation models is granted by the usage of implementation and data from a laboratory testbed. In this paper, we describe the integration of

S. Gottwalt et al. (Eds.): EI 2015, LNCS 9424, pp. 153–164, 2015.
DOI: 10.1007/978-3-319-25876-8_13

a real traffic protocol and an application layer taken from a voltage control testbed into a simulation model in order to obtain an aligned behaviour. The model can be validated by comparing the outcome from the simulation runs with those from the real setup reinforcing the degree of confidence in the selected approach. Once the model is validated through the testbed comparison, we are allowed to scale up the model and include in the simulation more complex scenarios in order to perform larger scale analysis not addressable within the testbed size limits. The paper is structured as follows: Sect. 2 introduces an overview on network simulators used in smart grid domains. Section 3 describes the Medium Voltage Control function, its communications and protocols from the testbed. The model of communication addressed in this paper is presented in Sect. 4, where the simulation models integrating malicious traffic from the testbed are described. In Sect. 5 some preliminary results from the attack analysis are discussed. Section 6 concludes the paper and presents the future work.

## 2 Related Work and Tools

Different simulation tools exist that can be used to model the ICT architecture of a power grid. In the following we provide an overview of the mostly used. OPNET [1] is a commercial tool and the main applications of this tool are planning, optimization and evaluation of large (corporate) networks that need to design, analyze or rearrange communication network systems. OPNET in smart grid domain is used in particular for hybrid simulation of power systems and ICT for real-time applications [2] and for co-simulation [3]. Another commercial network simulator is QualNet [4]. In the context of smart grid applications several approaches using QualNet are discussed in the literature [5]. The simulation focus is the analysis of protocols on a large scale (nodes in the tens of thousands) in heterogeneous (unicast, multicast, satellite, internet) networks. A drawback of QualNet emanates from the fact that it is focused on the analysis of protocols and their interaction with each other and the network structure, which makes it difficult to quantify the impact of ones own application on the network. Another network simulation tool is OMNeT++ [6]. It is a modular, extensible and component-based open source simulation library and framework, primarily employed for building network simulators. This framework has been used for modeling communication networks and distributed systems for smart grid applications in [7]. Other well-known open-source network simulators are the Network Simulator 2 (NS-2) [8], and its successor, Network Simulator 3 (ns-3) [9]. ns-2 and ns-3 are object-oriented, discrete event-controlled communication network simulators which are used for research and development. The development of the NS-2 has been abandoned in 2006 in favour of a new product development, i.e. ns-3. ns-3 is a free, open-source software, licensed under GNU GPLv2, written in C++ and offering Python bindings. It is possible to describe the architecture of the network and to schedule simulation events that will be executed at defined time. Different protocols (TCP, UDP, RIP, OSPF, etc.), data traffic sources (FTP, Telnet, Web, CBR, VBR, etc.), mechanics for router queue management as well as of routing algorithms can be included in the simulation model. There are also implementations for the MAC-layer and multicast-protocols for wired and wireless communication networks. The simulation results can be saved to a trace-file and can be analyzed with self-written scripts or with specific thirty party tools. An important utility introduced in ns-3 is the Direct Code Execution (DCE) functionality. This provides the possibility to include and execute existing implementations of protocols and applications without the need of rewriting the source code. This has been the reason why we have selected it as a good candidate tool for our research purposes. NS-2/3 are used in order to evaluate ICT infrastructures for the smart grids, e.g. for the improvement of existing infrastructures based on 802.11s Mesh Networks for Smart Metering [10], or in order to evaluate the interaction between ICT and energy networks in co-simulation as discussed in [11]. Thanks to the DCE functionality of ns-3, in this paper we propose a simulation analysis approach that addresses the cyber security evaluation of the smart grid communications considering the real applications exchanging traffic conform to the communication standards used in the power grids.

## 3 Medium Voltage Control Testbed

The connection of a consistent amount of DERs to medium voltage grids can influence the status of the whole power grid. In particular it is possible to see effects on the capacity of the DSO (Distribution System Operator) to comply with the contracted terms with the Transmission System Operator and so on the quality of service of their neighbour grids. This difficulty not only could be transferred into charges to the DSO, but it may also impact on the TSO operation because the scheduled voltages at grid nodes could not be observed and voltage stability problems cannot be managed properly. In order to maintain stable voltages in the distribution grids a Voltage Control function has been specified in [12] whose main functionality is to monitor the grid status from field measurements and to compute optimized set points for DERs, flexible loads and power equipment deployed in HV(High Voltage)/MV(Medium Voltage) substations. The Voltage Control is a function of the SCADA node of a HV/MV substation control network [12]. In order to compute an optimized voltage profile the algorithm involves communications through components inside the DSO area, but also exchange of information with systems outside the DSO domain. In particular DERs communicate with the substation SCADA via a DER Control Network, possibly deploying heterogeneous communication technologies available in different geographical areas. DERs periodically provide measurements to the substation SCADA and receive set points in order to keep optimized voltage profiles. The RSE PCS-ResTest Lab (Power Control Systems Resilience Testing Laboratory) [17] hosts a test platform for running cyber security experiments over realistic control scenarios, implementing the message exchange involved in the Medium Voltage Control using the IEC 61850 standard with MMS (Manufacturing Message Specification) profile [14]. More info on the testbed architecture can be found in [15].

# 4 Simulation Model

In this section the ns-3 tool introduced in the previous section is used for building the communication architecture. In the following subsection the different developed models are described.

## 4.1 Communication Model

Figure 1 presents a sketch of the model architecture for the legal communications. The network is composed by 7 main nodes: at DER site, the DER server (1) and the router (2); at HV/MV substation site, the router (3) for DER communication, the SCADA server (4) and the router (5) for center communication; at center level, the router (6) and the SCADA server (7). As in the testbed, the router nodes have multiple network interfaces, one for each network link.

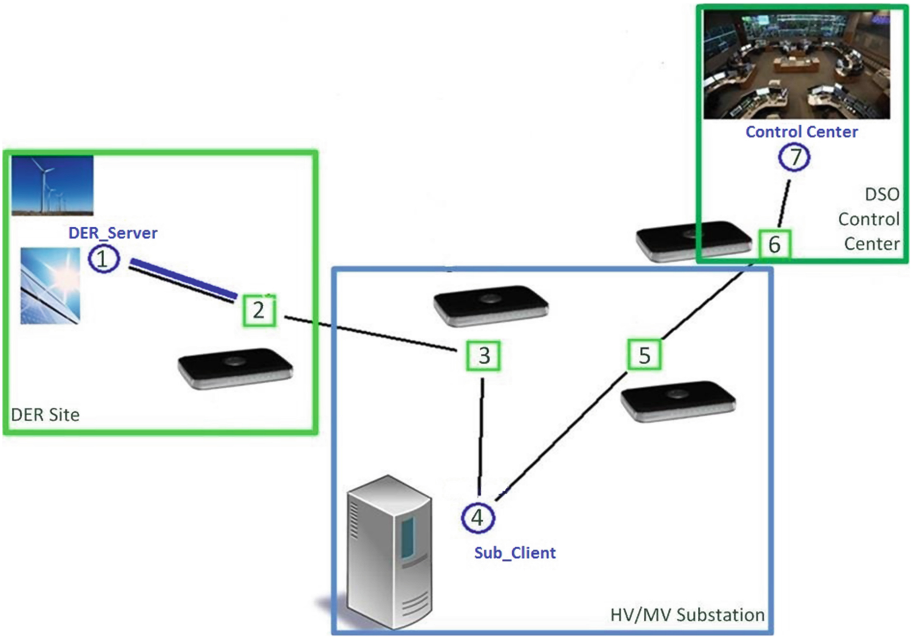


**Fig. 1.** Logical architecture of the simulation model

In particular we focus on DER primary substation communication and considering the Voltage Control function we have two types of information flows: periodic data representing the measurements from the DER site to the primary substation and possible asynchronous set-point sent by the primary substation in order to control the DER behavior. Both the information flows use the MMS protocol over an always on TCP/IP connection. The correspondent ns-3 model is again composed by 7 nodes belonging to 5 different networks: DER LAN NW, DER-SUB WAN NW, SUB LAN NW, SUB-CENTER WAN NW and CENTER LAN NW. Each node has an IP address depending on the network where it is placed. A sketch of the network addressed is presented in Fig. 2.

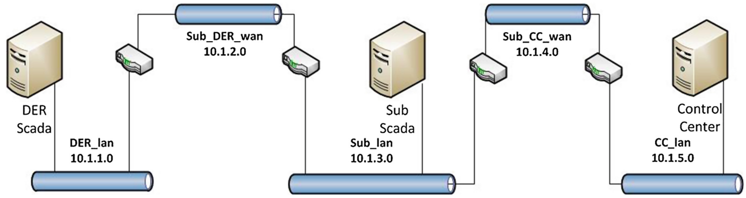
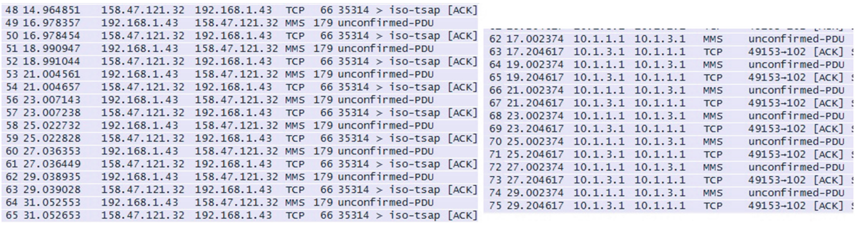


**Fig. 2.** Model architecture

At DER server (node 1) a MMS server application is installed: using the DCE feature of ns-3, we install in the model the testbed application based on the libiec61850 library [16]. At SCADA server (node 4) the corresponding MMS client application is running. We choose to use the testbed implementations instead of ns-3 built-in applications in order to obtain more realistic traffic: the reports containing DER measurements are sent every 2 seconds and if we sniff the traffic of the simulation we expect to obtain the same trace of the real application with the same traffic profile (packet size and content of IP, TCP and higher layer protocols in the MMS stack). In Fig. 3 the comparison between the trace of the information flow from the RSE testbed and the simulation model is shown. It is possible to see the exchange of measurements (the MMS reports) from the DER SCADA to the primary substation SCADA. The traffic pattern is the same; this means that the information flow emitted by the simulator is fully comparable with the real application information flow. Figure 4 allows comparing the structure of a MMS report packet containing the DER measurements. It is possible to note the full stack having the MMS protocol at the highest level.

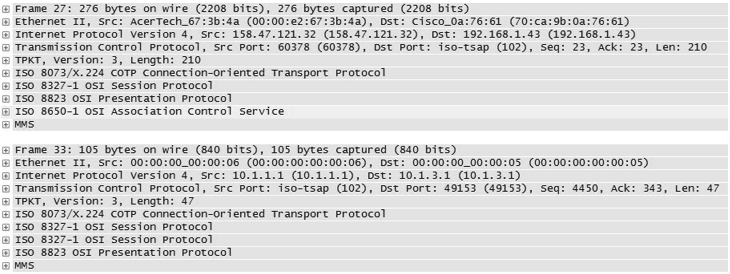


```
48 14.964851   158.47.121.32  192.168.1.43   TCP   66 35314 > iso-tsap [ACK]
49 16.978357   192.168.1.43   158.47.121.32  MMS  179 unconfirmed-PDU
50 16.978454   158.47.121.32  192.168.1.43   TCP   66 35314 > iso-tsap [ACK]
51 18.990947   192.168.1.43   158.47.121.32  MMS  179 unconfirmed-PDU
52 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]
```

**Fig. 3.** Traffic trace from the testbed (left) and the model (right)

Comparing the content of a MMS report frame obtained from the real application with a report frame from the ns-3 simulation with DCE, we see the same

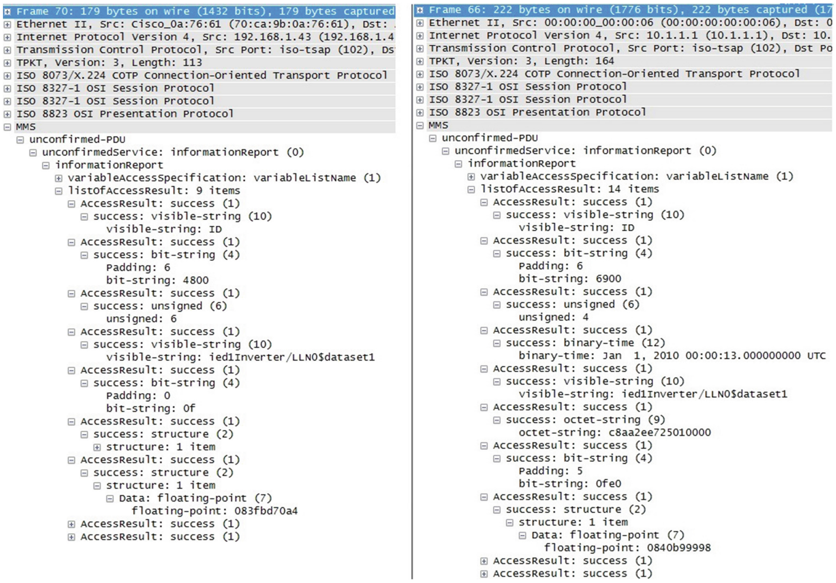


```
⊞ Frame 27: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits)
⊞ Ethernet II, Src: AcerTech_67:3b:4a (00:00:e2:67:3b:4a), Dst: Cisco_0a:76:61 (70:ca:9b:0a:76:61)
⊞ Internet Protocol Version 4, Src: 158.47.121.32 (158.47.121.32), Dst: 192.168.1.43 (192.168.1.43)
⊞ Transmission Control Protocol, Src Port: 60378 (60378), Dst Port: iso-tsap (102), Seq: 23, Ack: 23, Len: 210
⊞ TPKT, Version: 3, Length: 210
⊞ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
⊞ ISO 8327-1 OSI Session Protocol
⊞ ISO 8823 OSI Presentation Protocol
⊞ ISO 8650-1 OSI Association Control Service
⊞ MMS

⊞ Frame 33: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
⊞ Ethernet II, Src: 00:00:00_00:00:06 (00:00:00:00:00:06), Dst: 00:00:00_00:00:05 (00:00:00:00:00:05)
⊞ Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1), Dst: 10.1.3.1 (10.1.3.1)
⊞ Transmission Control Protocol, Src Port: iso-tsap (102), Dst Port: 49153 (49153), Seq: 4450, Ack: 343, Len: 47
⊞ TPKT, Version: 3, Length: 47
⊞ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
⊞ ISO 8327-1 OSI Session Protocol
⊞ ISO 8327-1 OSI Session Protocol
⊞ ISO 8823 OSI Presentation Protocol
⊞ MMS
```

**Fig. 4.** MMS packet structure from the testbed (top) and the model (bottom)

structure (Fig. 5): in both case the report fields of the packet are exactly those specified by the IEC 61850 standard.



```
⊞ Frame 70: 179 bytes on wire (1432 bits), 179 bytes captured
⊞ Ethernet II, Src: Cisco_0a:76:61 (70:ca:9b:0a:76:61), Dst:
⊞ Internet Protocol Version 4, Src: 192.168.1.43 (192.168.1.4
⊞ Transmission Control Protocol, Src Port: iso-tsap (102), Ds
⊞ TPKT, Version: 3, Length: 113
⊞ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
⊞ ISO 8327-1 OSI Session Protocol
⊞ ISO 8327-1 OSI Session Protocol
⊞ ISO 8823 OSI Presentation Protocol
⊟ MMS
  ⊟ unconfirmed-PDU
    ⊟ unconfirmedService: informationReport (0)
      ⊟ informationReport
        ⊞ variableAccessSpecification: variableListName (1)
        ⊟ listOfAccessResult: 9 items
          ⊟ AccessResult: success (1)
            ⊟ success: visible-string (10)
                visible-string: ID
          ⊟ AccessResult: success (1)
            ⊟ success: bit-string (4)
                Padding: 6
                bit-string: 4800
          ⊟ AccessResult: success (1)
            ⊟ success: unsigned (6)
                unsigned: 6
          ⊟ AccessResult: success (1)
            ⊟ success: visible-string (10)
                visible-string: ied1Inverter/LLN0$dataset1
          ⊟ AccessResult: success (1)
            ⊟ success: bit-string (4)
                Padding: 0
                bit-string: 0f
          ⊟ AccessResult: success (1)
            ⊟ success: structure (2)
              ⊞ structure: 1 item
          ⊟ AccessResult: success (1)
            ⊟ success: structure (2)
              ⊟ structure: 1 item
                ⊟ Data: floating-point (7)
                    floating-point: 083fbd70a4
          ⊞ AccessResult: success (1)
          ⊞ AccessResult: success (1)
```

```
⊞ Frame 66: 222 bytes on wire (1776 bits), 222 bytes captured (17
⊞ Ethernet II, Src: 00:00:00_00:00:06 (00:00:00:00:00:06), Dst: 0
⊞ Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1), Dst: 10.
⊞ Transmission Control Protocol, Src Port: iso-tsap (102), Dst Po
⊞ TPKT, Version: 3, Length: 164
⊞ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
⊞ ISO 8327-1 OSI Session Protocol
⊞ ISO 8327-1 OSI Session Protocol
⊞ ISO 8823 OSI Presentation Protocol
⊟ MMS
  ⊟ unconfirmed-PDU
    ⊟ unconfirmedService: informationReport (0)
      ⊟ informationReport
        ⊞ variableAccessSpecification: variableListName (1)
        ⊟ listOfAccessResult: 14 items
          ⊟ AccessResult: success (1)
            ⊟ success: visible-string (10)
                visible-string: ID
          ⊟ AccessResult: success (1)
            ⊟ success: bit-string (4)
                Padding: 6
                bit-string: 6900
          ⊟ AccessResult: success (1)
            ⊟ success: unsigned (6)
                unsigned: 4
          ⊟ AccessResult: success (1)
            ⊟ success: binary-time (12)
                binary-time: Jan  1, 2010 00:00:13.000000000 UTC
          ⊟ AccessResult: success (1)
            ⊟ success: visible-string (10)
                visible-string: ied1Inverter/LLN0$dataset1
          ⊟ AccessResult: success (1)
            ⊟ success: octet-string (9)
                octet-string: c8aa2ee725010000
          ⊟ AccessResult: success (1)
            ⊟ success: bit-string (4)
                Padding: 5
                bit-string: 0fe0
          ⊟ AccessResult: success (1)
            ⊟ success: structure (2)
              ⊟ structure: 1 item
                ⊟ Data: floating-point (7)
                    floating-point: 0840b99998
          ⊞ AccessResult: success (1)
          ⊞ AccessResult: success (1)
```

**Fig. 5.** MMS packet content from the testbed (top) and the model (bottom)

## 4.2 Models for the Flooding Attack Scenarios

Starting from the legal communication model validated with the testbed traces, now we introduce a variable number of additional nodes representing one or more attackers connected to the DER HV/MV substation Wide Area Network as displayed in Fig. 6. Each attacker runs the flooding attack tool taken from the testbed that sends illegal packets with source one or more attackers (node 8

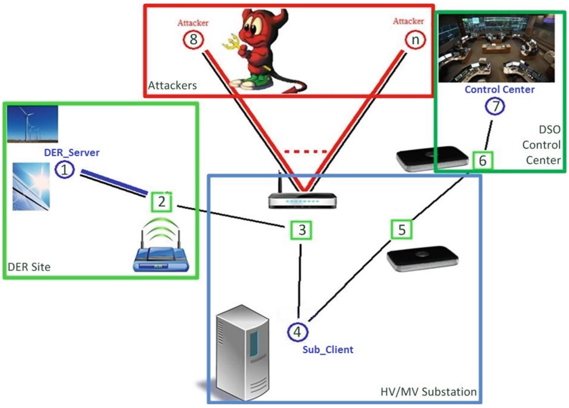
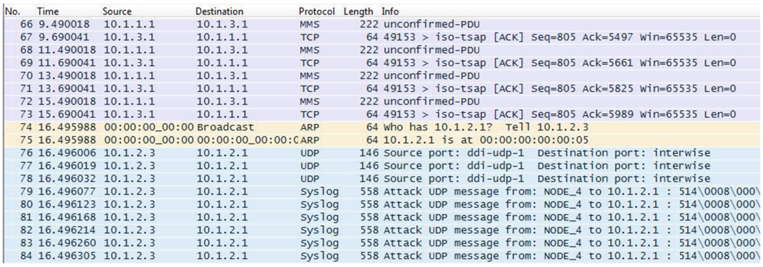


**Fig. 6.** Flooding attack

to n) and target the substation router (3), i.e. the same interface that receives the legal MMS packets from the DER.

In Fig. 7 the pcap trace is displayed where we see the MMS report and, after the beginning of the attack, the malicious UDP packets masqueraded as Syslog messages, a legal message type in the communications for ICT monitoring.



| 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:C | 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\ |

**Fig. 7.** Trace of attack scenario

Thanks to the parameters of the attack tool, we perform a sensitivity analysis of the effects of the attack on the MMS communication performance by varying the number of attackers, the packet rate and payload size of the illegal traffic.

### 4.3 Model of the LTE Technology

An important aspect that characterizes the communication between the primary substation and the DERs is the heterogeneity of the technologies deployed. The DER sites can be placed in areas where the wired connections are absent. Thanks to the new developments, the mobile technologies may represent a valid solution for the communication of the power grid components such as the DERs. The LTE technology may be used as access network for the DER and the HV/MV substation communications and is currently under evaluation in the lab testbed [15]. For this reason the simulated model has been enriched with the inclusion of the ns-3 LTE module. The messages outgoing the LTE router reach the destination through the different nodes of the LTE architecture included in the LTE module. In the new model nodes (2) and (3) in Fig. 1 are represented by LTE routers.

## 5 Results

This section shows how the simulation models presented in the previous sections can be deployed in order to define the attack scenarios for the experimental setup with the testbed. The simulated scenarios are selected considering the attack applications running on the testbed in order to investigate as the attack parameter configuration affects the legal communications. Moreover the strength of the simulation environment is that it allows studying larger scenarios than those feasible in the testbed, for example scaling up the number of connected DER.

### 5.1 Setup Parameters

In this subsection different flooding attack parameters are considered and the attack impact on the DER primary substation communication delay is shown. In the first analysis the focus is on evaluating the impact of the number of attackers on the MMS communication delay, in particular considering the transmission time taken by the DER measurements to reach the Primary substation. At time 1 the MMS client /server applications are activated and at time 8 the UDP flooding attack process starts. Figure 8 shows the delay values in normal and attack scenarios. It is possible to note how, varying the number of attackers, the effect on the legal communication changes. If only one attacker is involved, the communication delay has a deviation from the normal behavior, but the two parties are able to exchange messages. Increasing the number of the attackers the delay time is increasing until the point in time when the connectivity is lost (e.g. time 21 with 2 attackers). The connectivity loss occurs when the protocol timeouts expires and it is not possible to maintain the current session active. This happens earlier by increasing the number of attackers. Another important parameter to be taken in consideration for the setup of the testbed experiments is the frequency of the malicious packet emissions. In Fig. 9 the delay values considering different time between two consecutive packet emissions (10000, 1000 and 100 microseconds) are plotted. All the attack scenarios lead to a connection loss, but earliest with higher frequency. It is possible to note that in case of frequency set to 100 microseconds there is not a peak but an adjustment of the delay value. In the last set of experiments, the malicious packet size is taken as parameter under observation. In Fig. 10 the plot of the delay values in normal and

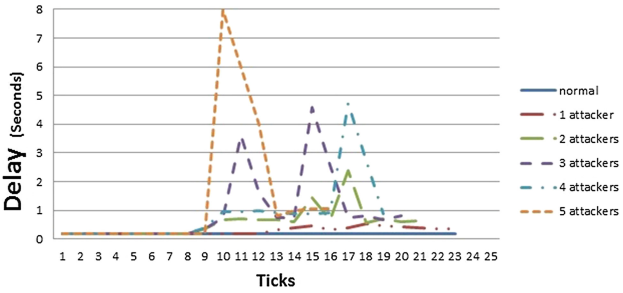


**Fig. 8.** Attack effect on delay changing the number of attackers

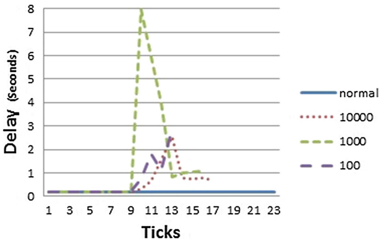


**Fig. 9.** Attack effect on delay changing the frequency

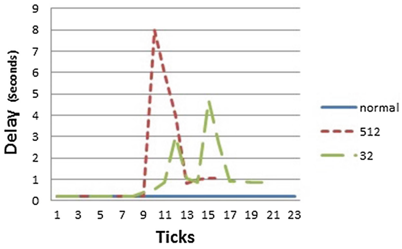


**Fig. 10.** Attack effect on delay changing the attack packet size

under attack conditions are shown. In particular two packet sizes are considered: 32 bytes and 512 bytes. The legal packet containing the DER measurements has a size around 200 bytes, so a smaller and a bigger malicious packet size have been taken in the simulations. If the packet size is double respect of the legal one it is possible to see an early connection loss, this happens also in case of the smaller attack packet size, but later with more dilated time.

### 5.2 Scaling up the Model Architecture

The simulation model can be deployed in order to explore the scenarios not addressable by the testbed experiments, for example scaling up the number of DER connected to grid. Indeed in order to satisfy the European targets of DER

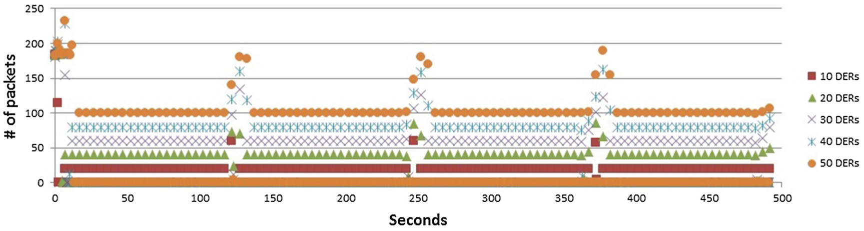


**Fig. 11.** DERs - primary substation exchanged packet/sec

penetration the full roll out of active grids requires that a single primary substation is able to control tens of distributed energy resources connected to the medium voltage grid. It is important to analyze the performance of communication in such a distributed scenario. For this reason the simulation model has been extended including 10, 20, 30 40 and 50 DERs. In Fig. 11 the amount of packet/sec exchanged between the DERs and a primary substation is shown considering different model size. The simulation time is of 500 s and it is possible to identify a first phase in which the profile of each DER is exchanged. This requires a large amount of exchanged packets and then each DER sends periodically, every 2 s, a MMS report containing its measurements. Some of these packets need to be retransmitted in order to reach the application in the primary substation, and the number of retransmissions increases with the number of DERs.

### 5.3 Experiments with Heterogeneous Communication Technologies

The setup of the model including the LTE module allows analyzing the performance of the mobile technology versus the results achieved with the wired layout. In Fig. 12 the results achieved considering the round trip time (RTT) as indicator are plotted. From the simulation outcome it is possible to argue that the RTT values achieved deploying the LTE module are comparable with the base line communication, also considering a short plus delta resulting by the LTE model. In case of DER measurements (in Fig. 12 from packet 26 to the end of the simulation) the increase is of 17.757 ms.

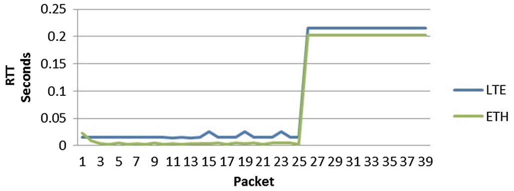


**Fig. 12.** RTT in wired vs wireless communications

## 6 Conclusion

The use of ICT network simulators for the assessment of the attack effects on smart grid communications is a promising approach for studying critical scenarios, whose results present synergies and interrelationships with experimental activities. However it still is a challenging research objective to achieve simulation results that are mostly aligned with the performance indicators measured in the real ICT architecture. The simulation tool has to incorporate into the model all the aspects of real architecture, i.e. the protocol aware information flows, the security countermeasures, the network topology and the malicious processes. In this paper the DER-substation information flow of a voltage control function for active grids has been modeled by a network simulator integrating a real client/server application implemented in a testbed setup. This approach allowed representing realistic traffic profiles in the simulation runs. The simulation outcomes have been validated with the testbed traces verifying a full alignment between the real and the simulated traffic profile. The results from the sensitivity analysis of the flooding attack effects by varying the attack parameters are discussed and used in order to identify the relevant scenarios for the testbed experiments. In the future work the effect of other attack tools will be evaluated with the simulator over a communication architecture enhanced with the security measures for the node authentication and the data encryption already implemented in the testbed, in compliance with the end-to-end security standard IEC 62351-3.

**Acknowledgments.** The work has been supported by the European FP7 project SmartC2Net (under grant agreement no. 318023). Further information is available at www.smartc2net.eu.

## References

1. http://www.opnet.com
2. Mller, S.C., Georg, H., Rehtanz, C., Wietfeld, C.: Hybrid simulation of power systems and ICT for real-time applications. In: 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Berlin (2012)
3. Georg, H., Wietfeld, C., Mller, S.C., Rehtanz, C.: A HLA based simulator architecture for co-simulating ICT based power system control and protection systems. In: 3rd IEEE International Conference on Smart Grid Communications (2012)
4. http://web.scalable-networks.com/content/qualnet
5. Ullo, S.L., Vaccaro, A., Velotto, G.: Performance analysis of IEEE 802.15. 4 based sensor networks for smart grids communications. J. Electr. Eng. Theory Appl. **1**(3), 129–134 (2010)
6. http://www.omnetpp.org/
7. Mets, K., Verschueren, T., Turck, F.D., Develder, C.: Exploiting V2G to optimize residential energy consumption with electrical vehicle (dis) charging. In: First International Workshop on Smart Grid Modeling and Simulation (SGMS), pp. 7–12, Brussels, October 2011

8. http://nsnam.isi.edu/nsnam/index.php/Main_Page
9. NS3 network simulator. https://www.nsnam.org/
10. Jung, J.-S., Lim, K.-W., Kim, J.-B., Ko, Y.-B., Kim, Y., Lee, S.-Y.: Improving IEEE 802.11s wireless mesh networks for reliable routing in the smart grid infrastructure. 2nd Workshop on Smart Grid Communications, pp. 1–5, Kyoto (2011)
11. Godfrey, T., Mullen, S., Dugan, R.C., Rodine, C., Grith, D.W., Golmie, N.: Modeling smart grid applications with co-simulation. In: 1st IEEE International Conference on Smart Grid Communications, pp. 291–296, Gaithersburg, October 2010
12. Moneta, D., Mora, P., Belotti, M., Carlini, C.: Integrating larger RES share in distribution networks: advanced voltage control and its application on real MV networks in Integration of Renewables into the Distribution Grid, CIRED 2012 Workshop, Lisbon, May 2012
13. SmartC2Net European Project, Deliverable D1.1 SmartC2Net Use Cases, Preliminary Architecture and Business Drivers, September 2013. http://www.smartc2net.eu
14. Int. Standard IEC 61850-8-1 (ed. 2) Communication networks and systems in substations - Part 8–1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506–1 and ISO 9506–2) and to ISO/IEC 8802–3, June 2011
15. SmartC2Net European Project, Deliverable D6.2 ”Integrated test beds - Description”, May 2015. http://www.smartc2net.eu
16. libIEC61850 open source libarary for IEC 61850. http://libiec61850.com/
17. RSE PCS-ResTest Lab (Power Control Systems Resilience Testing Laboratory). http://www.rse-web.it/laboratori.page?RSE_originalURI=/laboratori/laboratorio/10&RSE_manipulatePath=yes&country=eng