A Testbed for Smart Grid Communications over the Internet

Dexin Wang and Qiang Cui

Abstract

In this paper, we present a testbed for smart grid communications over the Internet and investigate the influence of communication latency and the selection of protocols on the operation of the smart grid. The simulations are based on the open-source discrete event simulator OMNeT++ and the INET framework. Although the INET framework includes most protocols used on the Internet, the implementation of some of the standards, including the open shortest path first (OSPF) and the border gateway protocol (BGP), is incomplete and may cause problems in some network topologies. We fixed this issue by implementing the missing part of cases defined in the standard. The hardware-in-the-loop simulation technique will be employed to test the communication performance between the control center and phasor measurement units (PMUs) over the simulated network.

I. Introduction

With the development of the smart grid, the traffic generated by communications between devices located in various parts of the power system, such as operation centers, substations, and generators, increases dramatically. On the other hand, building a dedicated communications network is not cost effective. Therefore, the performance of the smart grid communications over the existing ubiquitous network, i.e. the Internet, becomes increasingly important for the smart grid to function properly. For wide acceptance and deployment of the smart grid, it is necessary to investigate whether the Internet is suitable for the communication between various parts of the smart grid.

The smart grid is a typical cyber-physical system due to the tight coupling between communication technologies and physical power systems. The widely deployed smart grid technologies, such as wide area monitoring systems (WAMS), advanced metering infrastructure (AMI) and smart grid assets, are implemented based on bi-directional data communications [1, 2]. Control commands, measured values, and other types of data are sent and received between smart grid control centers and power system hardware via the Internet. With these measurements, the control center must react with proper actions to protect the assets and to balance the smart grid system. Hence, to study the communications network's influence on the operation of the smart grid is crucial. For this reason, we investigate the impact of various real-world network conditions on smart grid systems such as communication delays caused by network traffic. To achieve this goal, we simulate a real world communications network with widely used Internet protocols such as TCP/IP, HTTP, BGP and OSPF with OMNeT++.

An intuitive way to run power system simulations is to set a fixed time resolution and process the corresponding events at each time step. For communications networks, which are discrete in nature, however, it is hard to set an appropriate time resolution and achieve accurate results efficiently. If the time resolution is set too coarse, some events will not be processed in time. On the other hand, the processor will be idle in many steps if the time resolution is set too fine. Therefore, simulation of communications networks is usually implemented as driven by discrete events, in which the simulation time hops from one event to another after it is processed.

OMNeT++ is an extensible, modular, component-based C++ simulation library and framework. It is mainly used for building discrete-event-driven network simulators such as the communications network we are interested in. The INET Framework is an extension of OMNeT++ that provides a set of basic Internet protocols, such as IPv4, TCP, UDP, and HTTP, etc. It also provides the system-in-the-loop capability to connect real-world devices into the virtual network through network interfaces of the simulation host.

II. Standards Applied

The standards applied in this project includes:

a) RFC 793 - Transmission Control Protocol (TCP)

b) RFC 768 - User Datagram Protocol (UDP)

c) RFC 4271 - Border Gateway Protocol (BGP)

d) RFC 1247 - Open Shortest Path First (OSPF) Version 2

Details of the application of the standards are laid out in the following.

III. Network Topology

The network in our simulation is more flexible and more realistic than those existing ones in the literature [3, 4]. For example, the network in [3] only comprises four switches, two clients as Intelligent Electronic Devices (IED) and a LAN as a control room. The simulations in [4] investigate the communication performance of smart grid devices in one WiMAX cell. Therefore, the research is limited in a small geographic area, and network latency beyond the cell is not studied. The network topology in our simulation better resembles the network on the Internet with configurable scalability. Our system simulates a realistic wide area network (WAN) covering a town consisting of 16 Autonomous Systems (ASs). Each AS includes several Local Area Networks (LANs), and each LAN includes multiple hosts, as shown in **Error! Reference source not found.**. We can extend the number of hosts per LAN easily to adjust the scale of our simulated network.

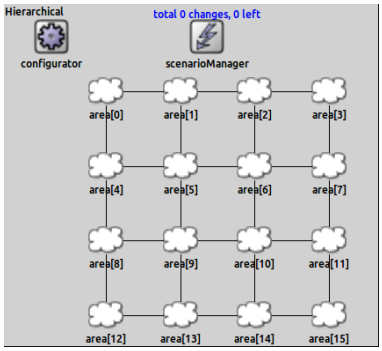

Figure 1 Network with 16 Autonomous Systems

A. Autonomous System (AS)

In the context of the Internet, an autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators [6], such as NREL or CSU, etc. In our simulated network, the 16 ASs are arranged as a 4-by-4 matrix, and they are connected with their neighbors.

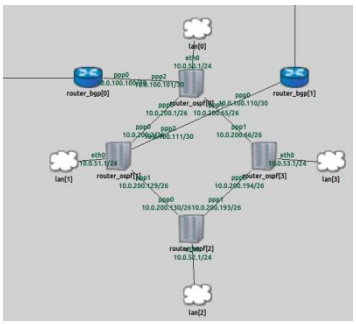

Figure 2 Autonomous System

B. Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, or office building [7]. In each AS in our simulated network, there are several Open Shortest Path First (OSPF) routers connecting the BGP routers and the same number of LANs. Moreover, each LAN consists of one switch and multiple hosts. A LAN could represent a home, a laboratory or an office, depending on the actual number of hosts in it.

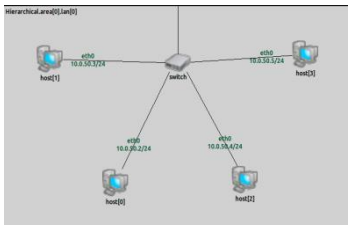

Figure 3 Local Area Network

C. Routing Protocols

After establishing the topology of the WAN, we configure the routing protocols for the routers. There are typically two types of routers on the Internet, namely Interior Gateway Protocol (IGP) routers and Exterior Gateway Protocol (EGP) routers. Dynamic routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) are widely used for them respectively. In order to make our simulator more realistic, both of the protocols are implemented in the simulator with the support of the INET framework.

1. Interior Gateway Protocol (IGP): OSPF

IGP is a type of protocol used for exchanging routing information between routers within an AS [8]. The most widely used interior gateway protocol (IGP) in large enterprise networks is

OSPF. OSPF is a link-state routing protocol. Each OSPF router maintains an identical database describing the topology of the AS. From this database, a routing table is calculated by constructing a shortest-path tree.

2. Exterior Gateway Protocol (EGP): BGP

EGP is a type of protocols used for exchange routing information between autonomous systems. BGP is a standardized EGP widely used in the Internet. The primary task of BGP routers is to exchange network reachability information with BGP routers in other ASs. The reachability information, which includes the list of ASs that information traverses, will be used to avoid routing loops and to enforce certain policies at the AS level [9]. The implementation of BGP in the INET framework is incomplete. Among the cases defined in the standard, only a few cases are covered. This causes some errors in some scenarios in our simulations. We fixed this issue by modifying the C++ code of the BGP module in the INET framework, covering the cases encountered in our simulations that were not covered in the original INET framework release.

IV. A Smart Grid Test Bed

The smart grid test bed we established in this project consists of three SEL series power devices such as Adaptive Multichannel Source (AMS), Phasor Measurement Unit (PMU), and Phasor Data Concentration (PDC). SEL-AMS is a device designed for testing protective relays that have low-level test capabilities. The included SEL-5401 Test System Software provides a virtual front panel to set and generate customized voltages and currents at the SEL-AMS.

Figure 4 SEL-AMS

For PMU, we use SEL-351A protection system because it provides a package of protection, monitoring, and controlling which is similar as PMU. It measures and monitors the power signals from SEL-AMS.

Figure 5 SEL-351A (PMU)

For Phasor Data Concentration, we use a SEL-3373 device which can connect to any compliant phasor measurement unit (PMU) through the Ethernet and arch all PMU data on the built-in solid-state drive (SSD). The PDC-Assistant Software is convenient for us to configure the parameters and monitor the real-time magnitude and phasor data from the remote PMU devices.

Figure 6 SEL-3373 (PDC)

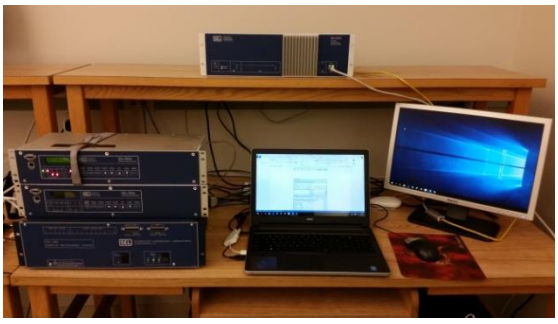

Figure 7 Smart Grid Test Bed with the Internet

With these SEL devices, we constructed a smart grid test bed by connecting an AMS, a PMU, a computer, and a PDC with Ribbon Cables and Ethernet Cables. We set up the IP address for each device appropriately to make sure they can communicate with each other well. There are three steps in the whole running process. First, we set and generate the customized voltages and currents at the AMS. At the same time, the PMU measures the values including VA, VB, VC, IA, IB, and IC from the AMS and display them on the monitor.

Secondly, we run the network simulator on the computer and the virtual routers establish their routing tables to make sure the successful connection between each pair of end-nodes. At the final step, the PDC sends TCP request packets to the PMU through the simulated network, and the PMU responds with data. The application protocol used in PMU and PDC is Synchrophasor, which uses TCP as its transport layer protocol. That is

why the PMU data can be transmitted through the virtual network. Figure 7 is a picture of the smart grid test bed along with the simulation host. As we can see in Table 1, the AMS sent certain voltage and current values, and the PDC collected their estimated values correctly. It means that the power signals was sent to the remote power devices through the Internet correctly which is important in Smart Grid System.

Table 1 SEL AMS and SEL PDC Test Results

	AMS (SEL-AMS)		PDC (SEL-3373)	
	Magnitude	Angle	Magnitude	Angle
IA	1	0	0.986	0.548
IB	2	0	1.973	0.644
IC	3	0	2.969	0.507
VA	67	0	66.995	0.273
VB	68	0	68.176	0.269
VC	69	0	68.926	0.268

V. Case Studies

In the real world, there are a series of phenomenon in the Internet that could affect the communications of smart grid systems because the power signals are wrapped inside TCP packets and sent via the Internet. For example, if the processing delay of several routers increases due to device replacement, and the smart grid system communication would be delayed. Also, some incidents, such as natural disaster, may affect the channel delay between two nodes, and then the power system will also be affected. We calculated the transmission time between PMU and PDC with Wireshark and Regular Expression. Below are the simulations of two cases, and we visualize their impacts on the Smart Grid System.

A. End-to-End Delay vs. Processing Delay

The first scenario is several routers encountered some problems, and their processing delays increase a lot. We changed the processing delay (of some of the routers) from 0ms, 0.25ms, 0.5ms, 0.75ms, 1ms, 1.7ms, and see their impacts on the transmission delay between PMU and PDC.

From the Figure 8, the transmission time becomes larger with the increasing of processing delay. It is a reasonable result because if the routers are processing the TCP packet from the PMU later than before, then it takes more time for passing the simulated network.

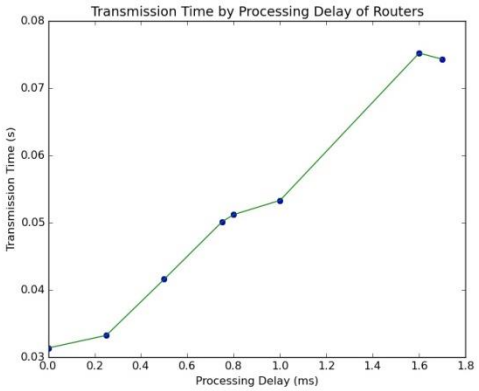

Figure 8 Transmission Delay vs. Processing Delay

B. End-to-End Delay vs. Channel Delay

The second scenario is that the channels between routers in area 0 encounter problems and the channel delays increase a lot. We set the channel delay to 0ms, 5ms, 10ms, and 15ms, and measured their impact on the transmission delay between the PMU and the PDC.

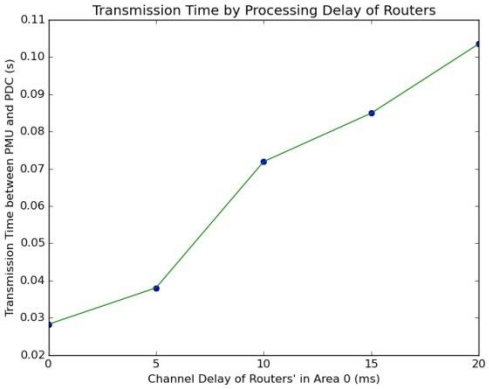

Figure 9 Transmission Delay vs. Channel Delay

From Figure 9, the transmission delay becomes larger with increasing channel delay. It is a reasonable result because if the channels between routers transmit the packets from the PMU later than before, then the packets take more time to pass through the simulated network.

C. UDP vs. TCP

In the simulated network, we implemented UDP and TCP Client-Server activities and compared their communication paradigms. In Figure 10, for the UDP case, the client send a request, and the server responds the client from the beginning. For the TCP case, at first, the client sends the server the request signal for opening the

connection and starts handshake process.

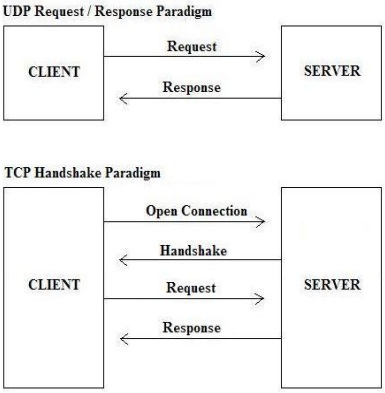

Figure 10 UDP vs. TCP

After that, the client sends the request, and the server will respond it. From this figure, we know the difference is TCP has a connection open and a handshake but UDP not. However, this is a big picture of two protocols and we will now simulate them in the network and confirm this paradigm and more difference between two protocols. In Figure 3, there is a UDP client in the area [1] and a UDP server in the area [2].When the UDP client sent the Video Stream Requirement packet, then the UDP server would be continuously sending the Video Stream Fragment packets until the full video were sent. It is the same as the UDP paradigm in Figure 10, and if some packets that the server sent are dropped during the journey, the server will not send that packet again.

```
309847   100.00027423          area[1] --> area[2]     VideoStrmReq
310000   100.00105885          area[2] --> area[1]     VideoStrmPk
314466   101.00093203          area[2] --> area[1]     VideoStrmPk
314924   102.00093203          area[2] --> area[1]     VideoStrmPk
315406   103.00093203          area[2] --> area[1]     VideoStrmPk
315864   104.00093203          area[2] --> area[1]     VideoStrmPk
316322   105.00093203          area[2] --> area[1]     VideoStrmPk
316820   106.00093203          area[2] --> area[1]     VideoStrmPk
317278   107.00093203          area[2] --> area[1]     VideoStrmPk
317760   108.00093203          area[2] --> area[1]     VideoStrmPk
318218   109.00093203          area[2] --> area[1]     VideoStrmPk
318676   110.00093203          area[2] --> area[1]     VideoStrmPk
323142   111.00093203          area[2] --> area[1]     VideoStrmPk
323600   112.00093203          area[2] --> area[1]     VideoStrmPk
324082   113.00093203          area[2] --> area[1]     VideoStrmPk
324540   114.00093203          area[2] --> area[1]     VideoStrmPk
```

Figure 11 UDP Protocol Activities Simulation

For the TCP demo, we can find the difference with the UDP case in Figure 12. For TCP protocol, the client and the server will establish a connection by the handshake process that consists of synchronization and acknowledgment for both directions. At first, the client will send the synchronization packet, and the server will send back the acknowledgment packet if the server received the sync packet. After that, the client will send acknowledgment packet again to establish the connection. It is called the 3-way handshake in the TCP protocol. After finishing the 3-way handshake, the TCP client will send request data whose length is 350 bytes. In TCP, every time the client and the server received the packets from the other side, it must send the ACK packet to tell the other they received it. So after the server sends the TCP data segment, it will wait for the ACK from the client. Only then, the server will send another TCP data segment.

```
293322   80.000351189998       area[1] --> area[2]     SYN
293488   80.000903329993       area[2] --> area[1]     SYN+ACK
293573   80.001388389991       area[1] --> area[2]     ACK
293677   80.002580389991       area[1] --> area[2]     data(l=350,1msg)
293742   80.00372832999        area[2] --> area[1]     ACK
293789   80.00458112999        area[2] --> area[1]     tcpseg(l=488,0msg)
293859   80.007040909989       area[1] --> area[2]     ACK
293922   80.008140689988       area[2] --> area[1]     tcpseg(l=488,0msg)
293939   80.008603089988       area[2] --> area[1]     tcpseg(l=488,0msg)
294025   80.010600469987       area[1] --> area[2]     ACK
294125   80.011062869987       area[1] --> area[2]     ACK
294168   80.011700249986       area[2] --> area[1]     tcpseg(l=488,0msg)
294176   80.012137849986       area[2] --> area[1]     data(l=96,1msg)
294299   80.014160029985       area[1] --> area[2]     ACK
294325   80.014277469985       area[1] --> area[2]     ACK
```

Figure 12 TCP Protocol Activities Simulation

With TCP and UDP client-server activities, we can compare the differences in their implementation process and analyze them. There are three differences as below. First, TCP has a 3-way handshake for opening a connection, but the UDP does not have any process for establishing a connection. Secondly, once the UDP server receives the request packet from the client, it will send the new resource packets continuously even though previous packets are dropped on its way to the client. However, TCP server will resend the dropped packets if it did not receive the corresponding ACK packets from the client. Finally, UDP is faster than TCP, whereas TCP is more reliable and offers higher quality than UDP.

VI. Conclusion

We construct a smart grid test bed with a virtual network that simulates the network conditions in the Internet. The AMS generates power signals and the PMU at the same location can monitor them. The remote PDC can collect data from the PMU through the simulated Internet successfully. In the network, we can simulate several situations such as increasing of router's processing delay and channel delay and TCP and/or UDP Client-Server activities. We conclude that when the router's processing delay and channel delay in the network rise, the communications between distributed smart grid system devices will be delayed. Moreover, that leads to unfavorable effects on total smart grid system balance and control. Also, TCP has a 3-way handshake mechanism for opening a connection but UDP does not. TCP clients and servers will send acknowledgment packets right after receiving the packets, and it makes the communication more

reliable and secure. However, in the UDP protocol, the server will continuously send the resources without confirming the previous packets' status.

REFERENCES

[1] NIST, NISTIR 7628: Guidelines for Smart Grid Cyber Security, *National Institute for Standards and Technology (NIST)*, 2010.

[2] K. Mets, J.A. Ojea, C. Develder, Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis, *IEEE Communications Surveys & Tutorials*, vol.16, no.3, pp.1771-1796, Third Quarter 2014

[3] Bo Chen, K. L. Butler-Purry, A. Goulart, D. Kundur, Implementing a real-time cyber-physical system test bed in RTDS and OPNET, in *Proceedings of North American Power Symposium (NAPS)*, pp.1-6, September 7-9, 2014

[4] P.P.S. Priya, V. Saminadan, Performance analysis of WiMAX based Smart grid communication traffic priority model, in *Proceedings of International Conference on Communications and Signal Processing (ICCSP)*, pp.778-782, April 3-5, 2014

[5] K. Mets, T. Verschueren, C. Develder, T.L. Vandoorn, L. Vandevelde, "Integrated simulation of power and communication networks for smart grid applications," in *Proceedings of International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp.61-65, June 10-11, 2011

[6] Network Working Group - Internet Engineering Task Force (IETF), RFC 1930 - Guidelines for creation, selection, and registration of an Autonomous System (AS), March 1996, Available Online at http://tools.ietf.org/html/rfc1930

[7] Gary A. Donahue, *Network Warrior*. O'Reilly. pp. 5, June 2007

[8] Network Working Group - Internet Engineering Task Force (IETF), RFC 2328 - OSPF Version 2, April 1998, Available Online at http://tools.ietf.org/html/rfc2328

[9] Network Working Group - Internet Engineering Task Force (IETF), RFC 4271 - A Border Gateway Protocol 4 (BGP-4), January 2006, Available Online at http://tools.ietf.org/html/rfc4271