Modeling and simulation of electric power substation employing an IEC 61850 network

Jeyasingam Nivethan  
Tandy School of Computer Science  
800 South Tucker Drive  
Tulsa, Oklahoma, USA  
nivethan@utulsa.edu

Mauricio Papa  
Tandy School of Computer Science  
800 South Tucker Drive  
Tulsa, Oklahoma, USA  
mauricio-papa@utulsa.edu

Peter Hawrylak  
Department of Electrical and Computer Engineering  
800 South Tucker Drive  
Tulsa, Oklahoma, USA  
peter-hawrylak@utulsa.edu

ABSTRACT
The timely delivery of messages is an important requirement in networks used to control physical processes such as those found in the Critical Infrastructure. These systems are also known as Process Control Systems (PCS) or Supervisory Control and Data Acquisition (SCADA) systems. In the electric power sector, the IEC 61850 family of standards defines the network protocol for communication between devices inside an electric substation and the interface the substation presents to the Internet (outside world) in the Smart Grid. IEC 61850 uses IEEE 802.3 Ethernet for the physical and data link layers as opposed to the previous generation substations, which used dedicated point-to-point connections between devices. IEC 61850 (and other industrial protocols) operate in an environment where messages must arrive in time to be processed and action taken by control equipment. Discrete event simulation is a widely used technique to evaluate performance of such systems. Cyber attacks on process control systems often aim at overloading a communications link. This type of cyber attack may negatively affect such physical processes by introducing delays in messages that carry control actions. Ultimately, this type of attack may also result in a complete DoS situation. Therefore, from a security perspective, it is important to understand the impact that link load changes may have on the control system. This paper presents an OPNET Modeler simulation library to help analyze network traffic in electric power substations that employ the IEC 61850 standard for communication and control. This library is then used to examine sample substation network architectures to determine if they meet the message delivery performance requirements.

Categories and Subject Descriptors
H.4 [Information Systems Applications]: Miscellaneous; I.6 [Simulation and Modeling]: Model Development, Applications; C.4 [Performance of Systems]

General Terms
Performance, Design

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

Copyright is held by the owner/author(s).

CISR ’14, Apr 08-10 2014, Oak Ridge, TN, USA  
ACM 978-1-4503-2812-8/14/04  
http://dx.doi.org/10.1145/2602087.2602096

Keywords
Substation Automation, Network Performance, Simulation and Modeling

1. INTRODUCTION
IEC 61850 is a family of standards developed by the International Electrotechnical Commission (IEC) for the electrical substation automation and communication, leveraging popular computer networking technologies [1], [2].

In an electrical substation, critical information about electrical signals and the current state of the substation needs to be transferred within a short period of time; for instance, the response time of certain protection relays needs to be less than 4 milliseconds for power systems operating at 60Hz [3]. In IEC 61850 deployments, signals measured by instrument transformers (or other measurement devices) are sent via Sampled Value (SV) packets. Trip, blocking and status signals are transferred as Generic Object Oriented Substation Event (GOOSE) or generic substation status event (GSSE) messages [4]. IEC 61850 requires that SV, GOOSE and GSSE messages be encapsulated into Ethernet frames and transactions be completed within 4ms [5]. Because of this time requirement, IEC 61850 transports SV, GOOSE and GSSE directly over Ethernet [6].

Therefore, when designing an IEC 61850 based substation it is important to make sure that the underlying Ethernet network is capable of transferring those messages within the required period of time. This requirement may be difficult to satisfy since the transmission time needs to be estimated between various devices under various traffic loads. Timing and performance analysis of an IEC 61850 electric substation network can be conducted using network simulation. However, in order to effectively simulate an IEC 61850 based substation, it is necessary for a simulation tool to have a fully featured simulation library. The standard has been tested by several US utilities and they have observed benefits [7], [8] and can also be used in other sectors [9], [10], [11].

The objective of this research is to develop a fully functional framework/library for simulating Ethernet based (IEC 61850) substations in the OPNET Modeler [12] with all the devices and messages, with encoding, decoding and other processing features. OPNET Modeler has been chosen as the network simulation tool because it is widely used for network simulation and provides built-in support for the underlying Ethernet network. OPNET Modeler provides a wide range of networking devices and
protocols. A network can be built in OPNET Modeler by dragging, dropping, connecting with appropriate connectors or buses, and configuring the parameters using the graphical user interface. An IEC61850 library had to be created since OPNET does not include support for the standard at this time.

This library provides message encoding and the most common simulation devices found in an IEC 61850 substation including Bay, Merging Unit/Measurement Unit, Protection and Control Intelligent Electronic Devices (P&C IEDs), and Circuit Breakers. These devices send and receive GOOSE and Sampled Value (SV) messages defined by IEC 61850 [13]. Messages are encoded using the Abstract Syntax Notation One (ASN.1) [14] Basic Encoding Rules (BER) [15]. The GOOSE and SV messages are the application protocol data unit (APDU). The final Ethernet packet payload contains the APDU.

2. Related Work

Research in this area has focused on analyzing the performance of IEC 61850 based substation networks and the results indicate that the IEC 61850 network fulfills the time requirements of the GOOSE and SV messages under general conditions. Some experiments have shown cases where end-to-end delays exceed the time limit.

Sidhu et al. [16] conducted a performance evaluation of IEC 61850 based substation communication systems and concluded that IEC 61850 meets the 4ms time requirement under general conditions. As opposed to our approach, their model does not consider the encoded GOOSE or SV message APDU in the Ethernet payload, because they represented APDU with empty message blocks without any IEC 61850 fields or values inside it and they did not process the message after reception.

Juárez et al. [17] developed a framework for simulating the IEC 61850 substation on OMNET++ discrete event simulator. They modeled all substation devices with appropriate operations. However, their platform does not perform encoding or decoding of the IEC 61850 messages. Also, our library is developed for the OPNET Modeler, a widely used network simulation tool which currently does not have any library to simulate a substation network.

Skeie et al. [18] simulated single and multi-level Ethernet network models for IEC 61850 using the OPNET Modeler, and showed that switched Ethernet meets the timing requirements of IEC 61850. They also showed that when using hubs instead of switches to connect the substation devices, it is often difficult to meet performance requirements due to the extra traffic. However, their simulated IEC 61850 network does not perform any message processing and it was the UDP messages which were used as GOOSE/SV messages rather than pure Ethernet messages.

Gao et al. [19] performed a simulation study on end-to-end delays for protective relaying in substations using OPNET Modeler. End-to-end delay was measured for different message sizes and for the different inter-message delays. Their results showed that under normal conditions messages could be delivered within the 4ms limit, but that a slight increase in utilization caused message delays to exceed the 4ms limit. They only simulated a typical computer network using OPNET Modeler and special profiles rather than IEC 61850 devices.

Yang et al. [20] conducted a performance evaluation study of an IEC 61850 based substation on a gigabit Ethernet network using the ns-2 simulator. They modeled GOOSE messages as UDP packets which were set to expire after 4ms. Expired packets were dropped. The average end-to-end delay at the station level, the average end-to-end delay at the bay level and the packet drop rate were analyzed over a period of time. They used UDP rather than Ethernet as transport for GOOSE messages and used normal computer network devices rather than IEC-61850 devices.

3. Simulation Implementation

This section describes our experimental procedure, presents timing analysis and discusses results.

3.1 Modeling of Merging Unit (MU) in OPNET modeler

The MU sends current and voltage samples to the protection and control IED using SV messages. The MU component has two layers: Application layer and Ethernet layer. In the Application layer, a sinusoidal voltage signal generator function and a sinusoidal current signal generator generate example voltage and current signals. These signals are sampled at a user specified sampling rate and each sample pair (voltage and current) is obtained. The amplitude, frequency, phase angle and the sampling rate for the signals can be specified from the graphical user interface. Each generated sample pair is encoded into a sampled value APDU. The Application Layer sends the sampled value APDU to the OPNET Ethernet Module, The Ethernet Module adds the sampled value APDU as its payload and sets the specified destination address. The destination address can be assigned using the graphical user interface provided by the OPNET Modeler.

3.2 Modeling of Protection and Control (P&C) IED in OPNET modeler

The P&C IED receives the SV messages, decodes them, and examines the received samples, issuing a GOOSE trip message if needed. The Ethernet Module receives the Ethernet frames that contain the SV APDU and delivers it to the Application Module. The Application Module decodes the received message and check if the current or voltage reading contained in the message is within the user defined limits (above minimum and below maximum). If the voltage is below the minimum limit or above the maximum limit, the P&C IED issues a GOOSE trip message for the voltage breaker. Similarly if the current is below the minimum limit or above the maximum limit, the P&C IED issues a trip command for the current breaker.

3.3 Modeling of Circuit Breaker in OPNET modeler

The circuit breaker receives trip GOOSE messages, decodes them and opens the physical circuit breaker (if needed). A circuit breaker takes action based on the received trip command. Finally, the circuit breaker broadcasts its status if it trips (opens) to all IEDs in the substation. After tripping, (opening of the circuit breaker) the circuit breaker sends its status via GOOSE messages to all P&C IEDs in the substation. These GOOSE messages are sent out as broadcast Ethernet messages. Like other modules, the Application Module encodes the status of the device into the
GOOSE message and delivers it to the Ethernet Module where the destination address is set and the message is finally sent to the network (destination) via the MAC interface module.

4. Evaluation of Substation Network Topology

Example substation models have been set up using the devices we created and the transfer time has been analyzed for the time critical messages (GOOSE and SV), under various operating conditions and common network topologies. The end-to-end delay of (1) the SV messages, (2) the trip GOOSE messages and (3) the status GOOSE messages have been recorded as they are the key time critical messages in an IEC 61850 network. IEC 61850-5 specifies that the transfer time of a trip GOOSE message (GOOSE Type 1) should not be more than 3ms [5]; that the transfer time of a SV message should not be more than 4ms [5]; and that the transfer time of a status GOOSE (GOOSE Type 1A) should not be more than 10ms [5]. The status GOOSE message (GOOSE Type 1A) is less time critical compared to the trip GOOSE messages.

The main objective of the simulation scenarios was to demonstrate the ability of the IEC 61850 simulation framework that was developed. Experiments were designed to determine the maximum number of bays tripping that the substation network can handle without violating the end-to-end delay requirements of the SV, trip GOOSE and status GOOSE messages. This allows the designer to evaluate design improvements and other network topologies. High network traffic occurs in a substation when excessive tripping occurs and numerous broadcast GOOSE messages (containing the tripped circuit breaker’s status) are generated. This event overloads the network and may cause additional delays.

Table 1 gives the average, minimum, maximum, variance and standard deviation of the SV messages respectively during each test case which met the end-to-end delay requirements of the IEC 61850. In the failure case the end to end delay immediately exceeded the maximum limit and kept increasing over time.

<table>
<thead>
<tr>
<th>Tripped bays</th>
<th>Average</th>
<th>Min</th>
<th>Max</th>
<th>Var</th>
<th>StdDev</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, Star</td>
<td>0.0432</td>
<td>0.0288</td>
<td>0.1119</td>
<td>0.0001</td>
<td>0.0090</td>
</tr>
<tr>
<td>1, Ring</td>
<td>0.0892</td>
<td>0.0490</td>
<td>0.1801</td>
<td>0.0002</td>
<td>0.0137</td>
</tr>
<tr>
<td>2, Star</td>
<td>0.0586</td>
<td>0.0464</td>
<td>0.1214</td>
<td>0.0002</td>
<td>0.0129</td>
</tr>
<tr>
<td>2, Ring</td>
<td>0.0966</td>
<td>0.0464</td>
<td>0.2156</td>
<td>0.0009</td>
<td>0.0296</td>
</tr>
<tr>
<td>3, Star</td>
<td>0.0874</td>
<td>0.0464</td>
<td>0.2519</td>
<td>0.0006</td>
<td>0.0244</td>
</tr>
<tr>
<td>3, Ring</td>
<td>0.1421</td>
<td>0.0464</td>
<td>0.4558</td>
<td>0.0036</td>
<td>0.0602</td>
</tr>
</tbody>
</table>

Table 1: Average, Minimum, Maximum, Variance and Standard Deviation (Std. Dev.) delay times for SV messages in milliseconds

The experimental procedure follows a well-defined sequence. First, one bay was made to trip for each sample it received (each sample was outside the acceptable limits). The end-to-end delay of the SV, trip GOOSE and the status GOOSE messages were recorded. The number of tripped bays was increased by one for each subsequent test case and it has been found that the substation network can handle up to three bays tripping at the same time. When the fourth bay was tripped, the messages exceeded the delay limits specified by IEC 61850-5 [5]. Both the star and ring network topologies exhibited similar behavior. A substation with twelve bays has been used for this experiment. Figure 1 shows the ring topology substation we used.

When the substation fails to meet the end-to-end delay requirements due to excessive traffic, changes in network topology might improve the situation and protect all or part of the substation network from failure. The improved substation topology for the ring topology is shown in Figure 2. The four bays in the left half of the substation was set to trip at the same time (which was the worst case of the subnet) and it was observed that the end-to-end delay of SV messages did not exceed 0.1ms in the right half of the substation, which was well within the 4ms maximum limit.

Figure 1: Substation with a ring topology network

Figure 2: Improved ring substation topology

With this improved topology the end-to-end delay of SV messages did not exceed the 4ms limit. Although the other half of the substation failed, this topology improved the situation by protecting a group of bays from the excessive traffic generated from the other group of bays. In this topology, as the two parts of substations are connected by two single links connected to switch A, the entire excessive broadcast traffic generated from one side of the substation cannot flow to the other portion of the substation. Thus, part of the substation can remain operational.
5. Conclusion
An OPNET library for simulating an IEC 61850 network has been developed, implemented and tested. This library contains the devices required to simulate IEC 61850 based substations and its main components: Merging Unit (MU), a P&C IED and a Circuit Breaker. Device models have been developed with full protocol stack functionality, including message encoding using the ASN.1 BER standard. This library provides support for SV and GOOSE (Type 1 and Type 1A) messages following the encoding and decoding recommendations specified by IEC 61850.

The library has been used to simulate and analyze a substation with twelve bays. In particular, end-to-end delays of the SV messages, trip GOOSE messages (Type 1) and status GOOSE messages (Type 1A) were observed and recorded under different tripping conditions. Both a star and ring network topology was evaluated. The SV or GOOSE messages did not exceed their maximum specified end-to-end delay in a 100 Mbps network as long as no more than three bays experienced a trip condition simultaneously. If four or more bays experienced a trip condition simultaneously the network no longer met the end-to-end delay requirements. When the substation network failed to meet the specified delivery time requirements, an improved topology was then proposed and simulated and we were able to verify that the changes helped mitigate the negative effects of the failure. Thus, the library may also assist system designers in analyzing what-if scenarios; particularly the cyber attacks which are intended to delay the messages can be simulated. This in turn will help them improve performance, security and ensure that requirements are satisfied.

6. References