ESTELLE: A Method to Analyze Automatically the Performance of Telecontrol Protocols in SCADA Systems

Verónica Medina, Isabel Gómez, Joaquín Luque, *Member, IEEE*, and Sergio Martín

***Abstract*—This paper presents the use of ESTELLE, a formal description technique, as a method to calculate automatically the performance of telecontrol protocols in SCADA systems. Some specific primitives are added to the ESTELLE description language in order to achieve that goal. As an example, we analyze the performance of a telecontrol protocol. The results from this method are compared to performance measurements obtained from analytical and simulated solutions**

***Index Terms*—Performance analysis, performance modeling, protocol specification, SCADA systems, telecontrol protocols, throughput, transmission delay.**

I. Introduction

IN THE last few years, the role of power utilities in the world of telecommunications has undergone rapid changes which affect not just technological aspects, but also issues of regulation, access to new markets, the creation of new services, etc. This situation creates urgent technological demands that have to be satisfied to be able to keep on competing successfully [1]–[9].

One of the most important aspects for updating technology is to manage the operation of a power utility network. That is why several telecontrol systems have been applied to operate on such a network in a safe and economical way since the 1960s [10]–[12].

These telecontrol systems are based on processor architecture installed throughout the hardware of the power utility network. The processors are mainly located in both the energy generation plant and the energy distribution and transformation stations. These plant processors are called "remotes" [they are also called remote terminal units (RTUs)] and make it possible to work on the power network. Remotes communicate with one or several centers (also called control centers), sending the network status information and receiving commands. Communication protocols, which are applied to control these power networks, should be studied thoroughly, because the expense of setting up such systems can be reduced just by optimizing them. These protocols are called *telecontrol protocols*.

A formal description technique (FDT) is chosen when a protocol has to be specified in a formal way. Although there are many FDTs, three of them are the most popular. These are extended state transition language (ESTELLE) [13] and specification and description language (SDL) [14], based on extended finite state machines, and language for temporal ordering specification (LOTOS) [15], based on process algebra. All three are international standards and the selection of one or the other depends on the specific needs of the user or designer. No single FDT satisfactorily fulfills all of the requirements.

Several studies [4], [16] have shown that ESTELLE adapts better to the electrical sector than the other specification languages, since it does not require much learning or specialization effort. A tool, called a universal protocol converter or convertidor universal de protocolos (CUP), was designed to implement and integrate telecontrol protocol from its specification in ESTELLE [17].

Our recent work has focused on adding performance measurement capability to the CUP tool. This way, the performance of telecontrol protocols can thus be analyzed from its specification in ESTELLE, and an efficient implementation can be made of them. To achieve this, some specific primitives are added to the specification in ESTELLE of a telecontrol protocol [18], [19].

In this paper, we present an alternative method for studying the performance of a telecontrol protocol without using analytical or simulated solutions. In ESTELLE, we specify the performance analysis model of the telecontrol protocol (existing or new) including the performance primitives. The performance measures are then automatically calculated. The performance analysis model is needed because it is possible to study only one part (a layer) of a whole protocol.

In order to validate this method, we study the same telecontrol protocol analyzed in [20] and [21], where the performance was calculated by both an analytical and a simulated solution. We show all the steps that are necessary to obtain the performance of such a protocol automatically and the results of that analysis are compared to those obtained in the aforementioned work.

II. Performance Analysis

Performance analysis (an activity included into protocol engineering, i.e., to the set of activities which, based on some communication requirements, are able to generate a protocol executable code in an efficient and reliable way), is used to analyze a protocol in order to predict and optimize its behavior. There are different techniques to measure performance that are not only applied to protocols but also to systems in general. Most systems

[22] are studied by making models of the same systems in terms of logical and quantitative relationships. They are then manipulated and changed to see how the model reacts, and thus how the system would react, obviously, if the model were a valid one. If the model is simple enough, it may be possible to work with its relationships and quantities to get an exact, analytical solution. However, many systems are so complex that their valid mathematical models are also very complex, making it necessary to resort to other study techniques, such as simulation; that is, numerically exercising the model for the inputs in question to see how they affect the output measures of performance. Although simulations are often referred to as a "method of last resort," they are in fact almost always the only effective way to measure system performance. This is due to the sheer complexity of the systems involved and of the models necessary to represent them in a valid way.

We propose another solution to determine the performance of a telecontrol protocol (our systems) by using FDTs. First, the telecontrol protocol, which could be a new or an already existing one, is specified in ESTELLE, including the suitable performance primitives. Then, an executable code is generated, called the *simulating code*, which, when it is run, calculates the performance of such a protocol. The advantage of this proposal is that the performance of the telecontrol protocol is automatically determined while its specification in ESTELLE is made. This way, performance can be predicted and some parameters can be set up.

The difference between a simulated solution and ours is that the simulated one simulates a model of the protocol and we only simulate to predict performance automatically, because we actually specify in ESTELLE the very protocol (with some specific primitives for the purpose of performance analysis). Therefore, we both determine the performance and specify in ESTELLE the telecontrol protocol, and also, the executable code of such a protocol can automatically be generated using the appropriate tools.

III. Estelle Performance Model

The performance of a layer (see Fig. 1), in line with the open system interconnection model (OSI) [23] or a similar one, is going to be studied using two parameters, namely, the throughput and transmission delay. The throughput is defined as the number of successfully transmitted messages per mean transmission time of a message, and the transmission delay, is defined as the time interval, in units of the average transmission time of a message, from the moment a message is generated to the instant it is correctly received.

For the purpose of analysis, the behavior of the N and lower layers is typified, from the point of view of the $N+1$ layer, as a virtual channel (see Fig. 2). That channel sends a set of D_n bits at a rate of C_n and there is a delayed V_n due to the N layer propagation time. The throughput of the N layer is then defined as

$$E_n = \frac{C_n}{C_{n-1}}. \tag{1}$$

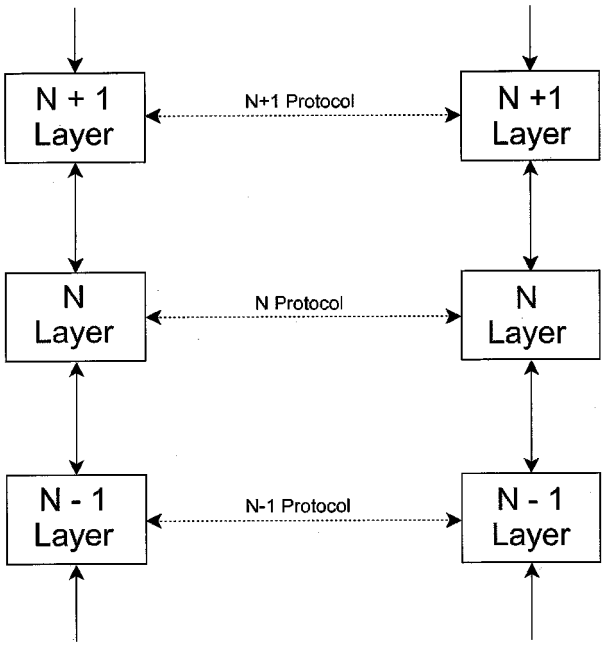

Fig. 1. Layered model.

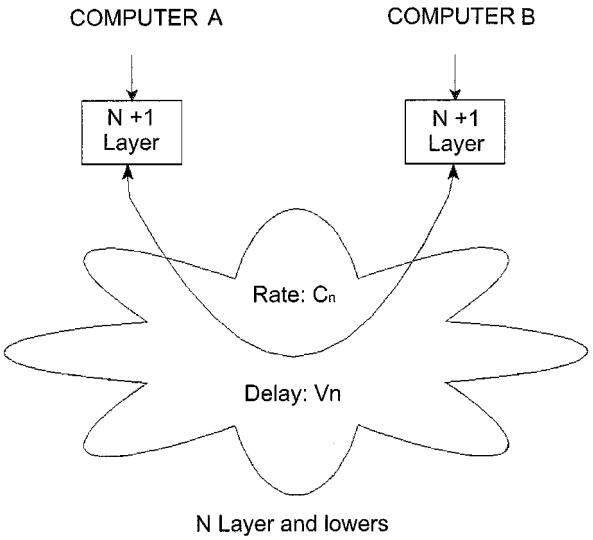

Fig. 2. Lower layers model.

Let t_a be the time in which the N layer COMPUTER **A** (see Fig. 2) receives a message from the $N+1$ layer to be sent. Furthermore, let t_b be the time in which the COMPUTER **B** $N+1$ layer receives such a message from the N layer. Then, the transmission delay is given as

$$R_n = t_b - t_a. \tag{2}$$

When a telecontrol protocol is specified in ESTELLE, there is no information about which modules belong to the same layer. The messages are sent using interaction points among modules (different layers) that are connected or attached, but there is no possible knowledge about the peer entities (or modules) that are really exchanging messages. Thus, some additional information has to be added to the specification in

ESTELLE to obtain the transmission delay and the throughput in order to use the previous performance analysis model in the ESTELLE simulating model, as defined in (1) and (2). Others parameters, such as the medium, minimum, and maximum message waiting time of a queue in a module, the number of messages received, etc., are automatically calculated without adding extra information.

Three kinds of primitives have been added to the ESTELLE specifications, which are explained in detail in [18]. The first two are for the throughput, and the third one is for the message delays. These primitives are listed as follows.

1) **CUP_PETICION_TRANSMISION:** This primitive is used when the N layer receives a request from the $N+1$ layer to send a set of bits.
2) **CUP_TRANSMISION_VALIDA:** This primitive is used when the N layer sends a set of bits using the services provided by the $N-1$ layer. This set of bits consists of two parts—the set of bits of the $N+1$ layer and the extra bits of the N layer.
3) **CUP_CATEGORIA:** The messages of a layer are classified to have their own transmission delay. This primitive is used for this purpose.

A protocol designer who wants to measure the performance of a telecontrol protocol has to work in the following way.

a) First, he specifies the telecontrol protocol in ESTELLE, adding the aforementioned primitives to his specification. The primitives are included in the body definition of a module at the adequate transition, depending on the measurement the designer needs. As the time is simulated, the ESTELLE TIMESCALE clause is used to determine its unit.
b) Once the designer has specified the protocol in ESTELLE with the performance primitives in the appropriate place, he can compile it and make its executable code. Some files are saved with the performance information when the executable code is executed (the designer can set the execution time) to analyze results.

IV. Applying the Model

In order to validate our method for calculating the performance, we study the same telecontrol protocol analyzed in [20]. That paper presented a method for calculating the capacity of a multipoint communications channel when a polling protocol is used. An exact solution, an approximate but easier to use solution, and simulated solution were obtained to respond to the following question: "How many remotes (RTUs) can share a link without degrading system performance?" Obviously, the answer would depend upon various parameters such as link velocity, message length, the amount of information generated by each RTU, etc. However, it also would depend significantly upon the communications protocol, called *medium access control (MAC) protocol*, used to communicate between the control center and the remotes [24]. This protocol takes a question-answer form in many control centers, also

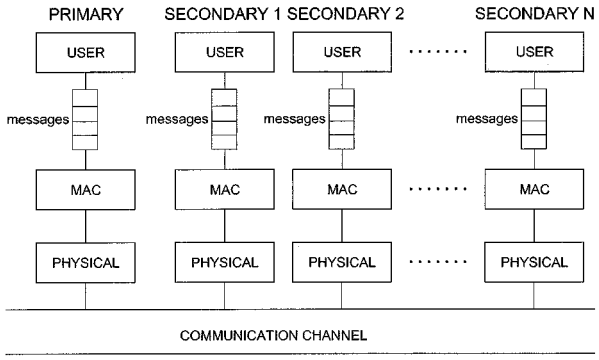

Fig. 3. Layered medium access protocol.

called *polling protocol*. The control center polls the first remote on the link; if the remote has messages to send, it does so, and if not, it sends a null message. The control center goes on to the poll, the second remote, and so on, successively until it has contacted all the remotes on the link, at which time it starts over again with the first RTU. This is the typical protocol used in the MAC layer in telecontrol protocols.

Let us analyze such a MAC protocol (polling protocol) to measure its performance using its specification in ESTELLE and compare results. As described in the previous paragraph, there are two kinds of stations, namely, a primary station (control center) and one or more secondary stations (remotes). The secondary stations have to be polled by the primary station before acquiring the channel, that is to say, the primary station controls the communication channel. Fig. 3 illustrates the protocol communication model. This protocol is divided into three layers and there is an additional one to join all the communicating entities for the purpose of performance analysis. We are only interested in the MAC layer so the upper and the lower layers are specified to behave as the real ones (the ones used in the telecontrol protocol stack).

There are only seven different modules in ESTELLE to specify this protocol: a primary USER module, a primary MAC module, a primary PHYSICAL module, a COMMUNICATION CHANNEL module to interconnect the primary station to the secondary stations, a secondary USER module, a secondary MAC module, and a secondary PHYSICAL module. Each module interchanges interactions only with the modules to which it is connected by means of interaction points. The interaction points are defined in the module header definition and its description is associated with the channel definition. Each module also needs a body definition to describe its behavior. The behavior of a module in ESTELLE is described by an extended finite state machine; there is a specific syntax to do so.

The stations exchange four kinds of messages: 1) event; 2) measurement; 3) command; and 4) command acknowledgment. There are four possible transmissions delayed; one for each class. The transmission delayed is measured at the USER layer and the throughput is measured at the MAC layer.

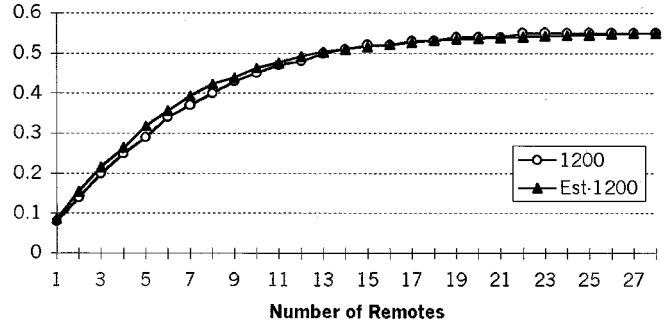

Fig. 4. Protocol efficiency.

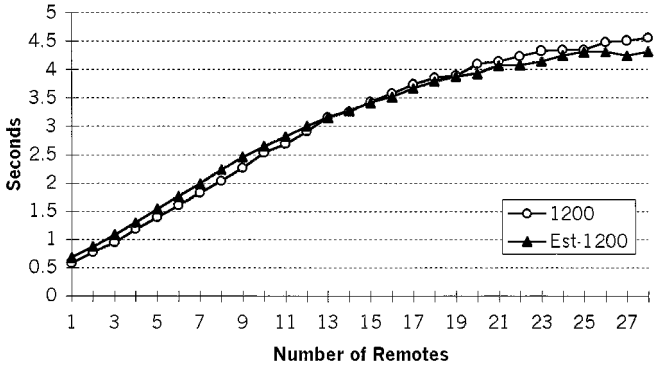

Fig. 5. Measurement transmission delay.

Once the specification of the MAC protocol[1] is compiled and error free, the executable code is generated. A file is saved with the performance information when the executable code is executed; the execution time can also be set up. Section V consists of the analysis of results.

V. Analyzing Results

We make the same conjecture as in [20], i.e., each secondary station generates messages exponentially (a Poisson process) with an average time of 4 s, and the primary station generates command messages exponentially with an average time of 8 s. A secondary station is less likely to generate an event message than a measurement message. The switching time is 10 ms. The length of measurement and event messages is 380 b and the length of command messages is 60 b. The simulating time is 1 h and the maximum number of RTUs (secondary stations) is 28.

The transmission delay is automatically calculated using (2) for each kind of message sent. Equation (3) shows the efficiency (throughput) of the MAC layer, i.e., the bit-rate of the MAC layer (C_{MAC}) per transmission bit-rate (bit-rate of the physical layer) only substituting n for MAC into (1). Equation (4) shows C_{MAC}, which is related to the total bits sent from the USER layer and the simulating time. The efficiency of the MAC layer is then automatically calculated using (5) by only substituting (4) into (3). The throughput is a number between one and zero

$$E_{\mathrm{MAC}} = \frac{C_{\mathrm{MAC}}}{\text{bit-rates}} \tag{3}$$

$$C_{\mathrm{MAC}} = \frac{\text{total number of bit sent from user layer}}{\text{simulating time}} \tag{4}$$

[1]The specification in ESTELLE is not shown for brevity.

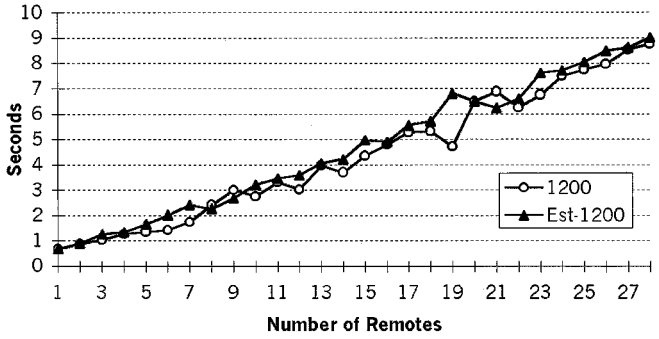

Fig. 6. Event transmission delay.

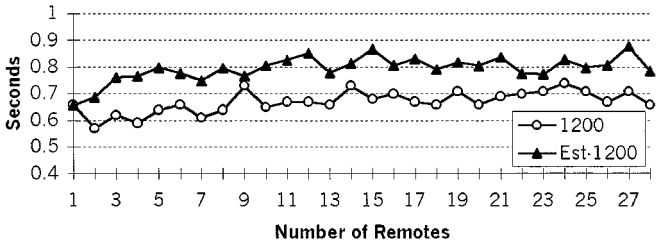

Fig. 7. Command transmission delay.

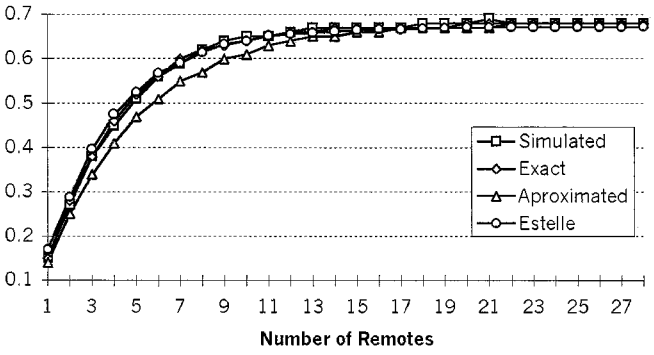

Fig. 8. Protocol efficiency.

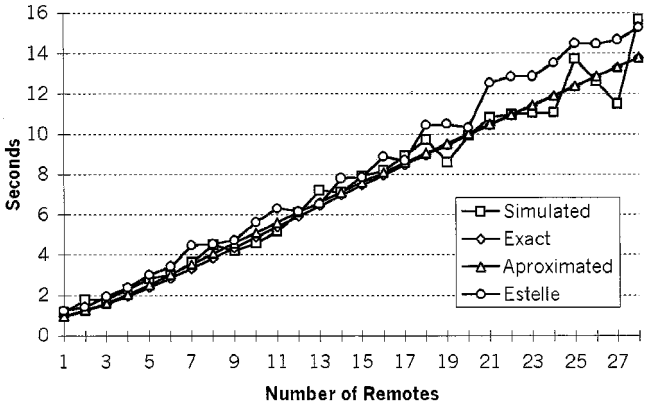

Fig. 9. Event transmission delay.

$$E_{\mathrm{MAC}} = \frac{\text{total number of bit sent from user layer}}{\text{simulating time} * \text{bit-rate}}. \tag{5}$$

Figs. 4–7 compare our results of efficiency, measurement transmission delay, event transmission delay, and command transmission delay with those obtained in [19] by means of a

simulated solution for a bit-rate of 1200 b/s.[2] The ESTELLE results are labeled "Est-speed," being speed the number of bits sends per second (b/s). The efficiency results in a simulated solution are the same as in the ESTELLE solution for all bit-rates. However, there are different results for the transmission delay. The reason for this behavior is that messages are generated randomly so that transmission delay can fluctuate between an error gap. For instance, let us take the transmission delay of the command message for 4 RTUs. There is a difference of 0,2 s between our result and a simulated one because the transmission delay of the command message always fluctuates between 0,4 s and 0,8 s. This depends on whether the command message is sent as soon as it is generated or after the arrival of the answer to the previous querying message.

Finally, the throughput and event transmission delays calculated by the ESTELLE solution are compared to both the analytical solution (exact and approximate) and the simulated solution, as shown in Figs. 8 and 9.

VI. Conclusions

The optimization of telecontrol protocols can reduce the installation costs of telecontrol systems in power utilities. FDTs are used to specify protocols, for which ESTELLE is more suitable than other methods in the electrical sector. Primitives added to ESTELLE make it possible to measure the performance of such protocols; therefore, telecontrol protocols can be improved. These improvements could simply consist of setting up some new parameters for an existing telecontrol protocol or replacing them with better ones (for instance, standardized ones).

In this paper, this alternative method for studying the performance of a telecontrol protocol has been presented. Furthermore, in order to validate it, we have studied successfully the same telecontrol protocol analyzed in [20] and [21], where the performance was calculated by both an analytical and a simulated solution.

References

[1] D. R. Ambrose, "Inter-utility communications within WSCC," *IEEE Trans. Power Syst.*, vol. 6, Nov. 1991.

[2] A. Barnegea, D. Ferrari, B. A. Mah, M. Moran, and D. C. Vernaand Hui Zhang, "The Tenet real-time protocol suite: Design, implementation, and experiences," *IEEE/ACM Trans. Networking*, vol. 4, Feb. 1996.

[3] J. P. Bernard and D. Durocher, "An expert system for fault diagnosis integrated in existing SCADA systems," *IEEE Trans. Power Syst.*, vol. 9, Feb. 1993.

[4] *Convertidor Universal de Protocolos de Telecontrol*: Dept. Tecnologia Electónica, 1992, vol. 132.181.

[5] T. E. Dy-Liacco, "Modern control centers and computer networking," *IEEE Comput. Appl. Power*, October 1994.

[6] G. Ericson and A. Johnsson, "Examination of ELCOM-90, TASE.1, and ICCP/TASE.2 for inter-control center communication," *IEEE Trans. Power Delivery*, vol. 12, Apr. 1997.

[7] G. Glijnis, "European utilities open lines of communications," *IEEE Comput. Appl. Power*, vol. 9, Oct. 1996.

[8] Y. H. Kim, N. Fukushima, and T. E. Dy Liacco, "KEPCO's national control center with an advanced energy management system," *IEEE Trans. Power Syst.*, vol. 5, Nov. 1990.

[9] H. Lee Smith, "Substation automation problems and possibilities," *IEEE Comput. Appl. Power*, Oct. 1996.

[10] J. I. Escudero, J. Luque, and F. Gonzalo, "Quality of service in the NOMOS TMN system," in Proc. Int. Conf. Power Sector Telecommunication System for 21st Century, Nueva Delhi, India, Jan. 1997.

[11] J. I. Escudero, F. Gonzalo, and J. Luque, "The challenge of managing new communications technologies," in Proc. SC35 CIGRE Colloquium, Beijing, China, Sept. 1997.

[12] C. León, J. B. Casado, J. Luque, and F. Gonzalo, "SER: Expert system in the fault management of a radio-delay network," *IEEE Stockholm Power Tech.*, June 1995.

[13] *Estelle—A Formal Description Technique Based on an Extended State Transition Model*, ISO Standard OSI 9074, 1989.

[14] *Specification and Description Language (SDL)*, Standard Z.100 CCITT, 1992.

[15] *LOTOS—A Formal Description Technique Based on the Temporal Ordering of Observational Behavior*, ISO Standard OSI 8807, 1989.

[16] J. Luque, F. Gonzalo, F. Pérez, and M. Mejías, "Formal techniques improve connectivity in supervisory systems," *IEEE Comput. Appl. Power*, Apr. 1994.

[17] A. V. Medina, I. Gómez, F. Pérez, J. Luque, and S. Martin, "Code generator to integrate telecontrol protocols," in Proc. MELECOM, Tel-Aviv, Israel, 1998.

[18] V. Medina, I. Gómez, S. Martín, and J. Luque, "Applying estelle to automatically determine the performance of telecontrol protocols in SCADA systems," in Proc. CIGRÉ, Cracovia, Polonia, 1999.

[19] V. Medina, I. Gómez, G. Sánchez, A. Barbancho, and S. Martin, "Using protocol engineering techniques to improve telecontrol protocol performance," in Proc. Power and Energy System, IASTED Conf., Marbella, Málaga, Spain, Sept. 2000.

[20] J. Luque, I. Gómez, and J. I. Escudero, "Determining the channel capacity in SCADA systems using polling protocols," *IEEE Trans. Power Syst.*, vol. 11, May 1996.

[21] J. Luque and I. Gómez, "The role of medium access control protocols in SCADA systems," *IEEE Trans. Power Delivery*, vol. 11, July 1996.

[22] A. M. Law and W. D. Kelton, *Simulation Modeling and Analysis*. New York: McGraw-Hill, 1991.

[23] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model*, ISO Standard 7498, 1984.

[24] I. Gómez, J. Luque, and J. I Escudero, "Medium access control protocols for electrical power network control," in *Proc. Bilkent Int. Conf. Lightwave Technology and Communications*, Ankara, Turkey, July 1992, pp. 23–29.

[2]Results from 300 and 600 simulations are not shown in the figure for clarity.