ISSN: 1983 7402 ITA, 01 a 03 OUT 2024

Modeling of a Data Modification Cyber-Attack in an IEC 61850 Scenario Using Stochastic Colored Petri Nets

Milton Rafael da Silva
Indústria de Material Bélico do Brasil - Fàbrica de Itajubá (IMBEL-FI), Itajubá/MG – Brasil

***Abstract* - In the IEC 61850 standard, the transmission of the sampled values packets of measurement in processing communication are defined, and these parameters are really important and critical in the automation of power systems. Related to the security analysis of the communication networks, a really powerful tool is the Stochastic Colored Petri Net (SCPN), because it models asynchronous and concurrent processes, and it is useful to analyze delays in timed systems. So, based in this context and knowing that the correct value of sampled values measurements is really critical in transmitting messages in the IEC 61850 context; it is modeled in an IEC 61850 scenario a cyber-attack using SCPN that aims to modify the data to be transmitted before it is packed as a Sampled Value (SV) message, what is really critical for the operation of the system. The results corresponded to the modeled cyber-attack, showing the efficacy of the proposed modeling method.**

***Keywords* – IEC 61850; Smart Grid; Stochastic Colored Petri Nets; Security Analysis; Modeling of Cyber-Attack.**

I. INTRODUCTION

In the intelligent transmission and power distribution networks based on interactive communication between all parts of the power conversion chain, known as Smart Grids, there are communication networks that allow the transfer of data between their components. Data exchanges, network topology, decentralized control, security, are inherent characteristics to the communication systems and are also an important part of the smart grids in the electric power sector.

In order that the information is exchanged in a correct, reliable and efficient way, standardization in data communication is needed. So there's the IEC 61850 standard. Referenced in [1], IEC 61850 proposes standards for the services and data formats exchanged on a network of electrical system equipment.

Related to security, it has been widely recognized as a major issue with potentially catastrophic implications in the smart grids scenario [2]–[7]. Also, cyber-attacks may take advantage of accessibility through the neighborhood area networks (NANs) or home area networks (HANs) to attempt to remotely access, compromise, or control electronic resources [8]. With the Internet and modern telecommunications, it is now easy for geographically distributed groups to coordinate simultaneous attacks [8].

In the scenario of cyber-attacks modeling, Petri net and its variations have been powerful tools for studying various types of asynchronous and concurrent processes [9], [10], [11]. The usefulness of Petri nets for cyber-attack modeling was pointed out first perhaps by McDermott [12]. It was observed that Petri nets are better at capturing concurrent actions in the progression of an attack [8]. Dalton *et al.* suggested generalized stochastic Petri nets for cyber-attack modeling [13]. Stochastic Petri nets are a type of timed Petri nets where transitions occur ("fire") after random times. In their work, transition delays were assumed to be exponentially distributed which conveniently turned the stochastic Petri net into an equivalent continuous-time Markov Chain. The approach appeared to be motivated by the straightforward steady-state analysis possible for Markov chains, but the assumption of exponential transition delays was not clearly justified [8].

Colored Petri nets have attracted some attention for cyber-attacks because they are more expressive than basic Petri nets. In the basic Petri net, all tokens are indistinguishable from each other. In colored Petri nets, tokens carry data values represented by color which enables different attackers to be distinguished with separate identities in the model [8]. Wu *et al.* suggested colored Petri nets for hierarchical attack modeling [14]. An attack represented at a high level is a simple colored Petri net where certain transitions have hidden details. The hidden details of that transition can be viewed in an associated subpage which is a separate colored Petri net [8].

When it is related to the electrical power system, Petri nets have been applied to show interdependencies between the preexisting electrical power and communications infrastructures [15]–[17]. In addition, Calderaro *et al*. [18] presented a Petri net-based method to identify and localize failures in the smart grid. Chen *et al.* [8] proposed a new hierarchical method to construct a large Petri net from a number of small Petri nets for modeling the cyber-physical attacks on the smart grid [11]. Dahl and Wolthusen suggested the use of interval timed colored Petri nets where tokens carry timestamps as well as color and the firing delay of transitions are bounded by specified time intervals [19]. Their concern is timing-dependent attacks carried out by multiple attackers against possibly multiple targets [8].

In these Petri net models, places represent all possible states of both power and communication systems and transitions represent actions that affect state changes. That is, interdependencies are accounted for in a straightforward manner by combining both electrical and communication devices in a single Petri net [8].

So, in this work, based in all previous works and in a simple IEC 61850 scenario, it is proposed to model and analyze a cyber-attack in a simple architecture with one merging unit publishing Sampled Value messages, a switch for packet switching and storage, and a network analyzer to check the packets sent. This cyber-attack aims to modify the

Milton Rafael da Silva, milton.fi@imbel.gov.br.

transmission of the Sampled Value messages (Data Modification) and assess the impact of it in the electrical power system communications systems. Data modification, also known as data diddling or data injection, involves changing data before they are processed at their destination [20].

II. STOCHASTIC COLORED PETRI NET (SCPN)

The Petri net (PN), discussed in [21], is a graphical mathematical tool for studying systems characterized as competitors, asynchronous, distributed, parallel, non-deterministic and/or stochastic. Briefly, the PN is a bipartite graph (graphs that don't contain odd cycles) with graphical interpretation formed by two components: transition and place. Representation is as follows in Figure 1, in which spaces are the circles and thin rectangles are transitions. These two components, also called nodes, are connected by directed arcs.

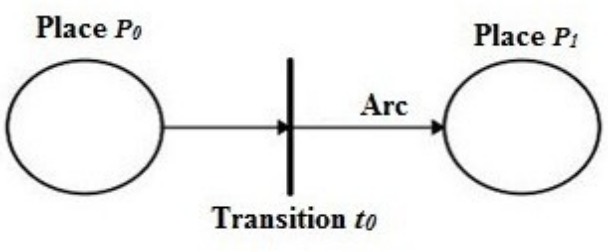

Figure 1. Basic Elements of a PN

For modeling and better interpretation of systems, it is used marks (tokens) assigned to the places that allow to represent the state situation. The movement of the marks through well-defined rules represents the system dynamics.

In the field of network protocol analysis, the Stochastic Petri Net (SPN), variants of PN, are constantly applied in the performance analysis in the computer networks and communication systems, since SPN is isomorphic and enables, together with the Markov chains [22], the state probability analysis of the system. However, even with these important characteristics, the SPNs are limited in complex models and in models with industrial dimensions.

The Stochastic Colored Petri Nets (CSPN) has higher abstraction capacity. This allows each place to have various types of marks and transitions that represent various types of functions, thereby reducing the number of nodes. A key point for the application of this type of Petri nets in the communication systems is precisely the connection with programming languages, as an example the Meta Language (ML) used in CPN Tools [23] software.

Formally, the definition for the SCPN is represented as follows and can be verified in [24] and [25]:

SCPN = {P, T, CB, C, W-, W+, Wh, Pri, M_0, θ}

• P is the finite set of places;
• T is the finite set of timed and immediate transitions, $P \cap T = \emptyset$, $P \cup T \neq \emptyset$;
• CB is the family of basic color classes: $CB=\{C_1,...,C_n\}$ with $C_i \cap C_j = \emptyset$;
• C is a $P \cup T$ function that associates to any r node a color domain $C(r)$ that is the Cartesian product of the CB elements;
• W^-, W^+, W^h: $W^-(p, t)$, $W^+(p, t)$, $W^h(p, t) \in [C(t) \rightarrow Bag(C(p))]$ are functions that label respectively the entrance, output and inhibitors arches between t transitions and p places;
• Pri is the priority function defined as follows: $\forall t \in T$, $Pri(t) : C(t) \rightarrow N.Pri(t)(c)$ is the priority of the instance$[t,c]$.
• M_0 is the initial marking that describes the initial state of the system;
• θ is the defined function in the set of transitions T given that $\theta(t)$ is the time function of the model.

III. IEC 61850 – GENERAL OVERVIEW

The IEC 61850 is an international standard that defines the communication and services form between different equipment present in the automation of power electrical systems [26]. It establishes the following objectives: Interoperability between manufacturers, free configuration (modeling), and long-term stability.

The most significant benefits of implementing this standard are the independence of future technology, ease of long-term maintenance, reduced wiring, and free specification and exchange of data at high speed.

A. Sampled Values

This type of message has the proposal of transmission of sampled values of measurement, according to [27], inserted into types of *unicast* or *multicast* messages. Commonly, this message is used to send analog data coming from the current and voltage meters (Current Transformers and Voltage Transformers).The IED (Intelligent Electronic Device) that implements the messages *Sampled Values* (SV) needs hardware that supports huge volume of Analog-to-Digital conversions that must be processed quickly and safe. This is only possible with the use of more resistant components, more reliable and more expensive. This is the burden that SV messages produce in the IEDs that implement them.

The sampled values are used by control and protection system. The frames of SV messages uses layer1 of the TCP / IP model and are extremely fast.

IV. SCPN MODELING OF AN IEC 61850 SYSTEM – *SAMPLED VALUE* (SV) MESSAGES AND CYBER-ATTACK

The following SCPN models seek to represent the main characteristics of the devices presented in the proposed architecture. So the proposed methodology concerns about analyze the performance of this network architecture using modeling only, when it is working normally or when it is attacked. According to the presented theoretical basis, it is started then the development of a SCPN modeling of the standard IEC 61850 together with a cyber-attack. For this, two guidelines are defined. The first one deals with the part of system concepts involving the definitions of the standard IEC 61850. The second one, structures the way how it should be

elaborate the models in SCPN, together with the modeled cyber-attack. In Figure 2 it can be seen the proposed architecture.

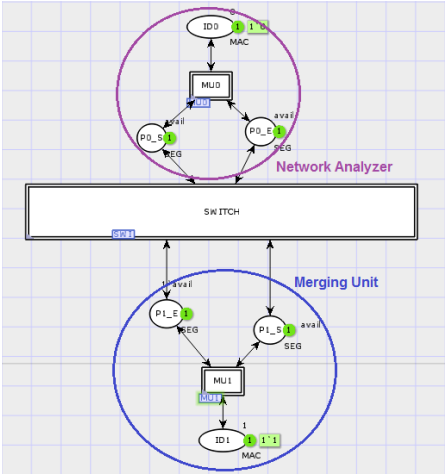

Figure 2. Proposed Architecture

A. *Switch Model*

The switch model has the main features of this device. The switching tables, packet buffer, switch processing and physical communication interfaces (input and output ports) are all defined. To better understand this model, only one communication port is defined. For the representation of other ports, a simply replication of such model is done. Figure 3 shows the main characteristics of this device. The switch model is based on the work developed in [28], in which this equipment is represented in CPN models.

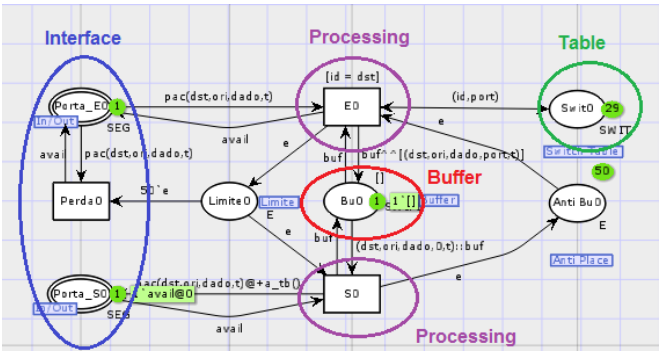

Figure 3. CPN Model of the Switch

Regarding the model representation, figure 5 indicates the dynamics of a SV packet within a real switching device. The message enters via the communication interface (place **Porta_E0**), then it is processed (transitions **E0** and **S0**), stored in the buffer (place **Bu0**) and then is transmitted according to the switching table to the respective destination (place **Swit0**). This whole process takes time, called by the norm as propagation time, and for this reason it is attributed to the time stamp @ + tb () in the transition **S0**.

B. *Merging Unit Model*

The model of Figure 4 represents the physical *merging unit* device that converts the analog signals into digital signals, and sends such signals in the format of *Sampled Value* messages.

The CPN representation of the *merging unit* characterizes the signal sampling, the processing of the samples by the logical nodes and the interfacing with the network.

The sampling process is done by reading a text file containing the current transformer samples, which simulates the data of a real transformer. The text file is read through the function defined in the **Inicio** transition, and through the **getPacketsTC** () function. After that, the file data is transformed into CPN tokens. **TCTR** and **MMXU** transitions, which represent the logical nodes defined in the IEC 61850 standard, translate the information from the samples (tokens) and pack them into the *Sampled Value* format. The right part of the model represents the communication interface of the device (**LAN_S** and **LAN_E** places). The **Origem** and **Destino** places indicate the communication interface of the source and destination of the packages (**Origem** and **Destino** places) generated by the *merging unit*. With this structure, the *merging unit* model is able to simulate real devices sending SV messages.

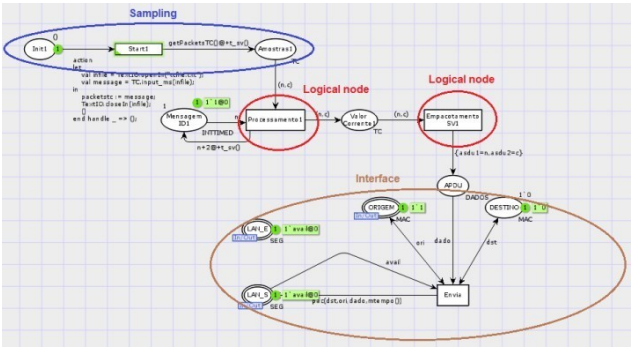

Figure 4. CPN Model of the Merging Unit

C. *Analyzer Model*

The analyzer model is characterized in a simple way according to Figure 5. The function of this model is to represent the device that verifies the latency time of the *Sampled Value* messages that is transferred in the network.

To do this, the model receives the messages through the communication interface (**LAN_E** place) and then verifies the origin of the packet (**Recebe** transition and **Origem** place) identifying the *merging unit* transmitter. After this, the message is sent to the **Buffer** transition where the transfer time of each SV packet is calculated.

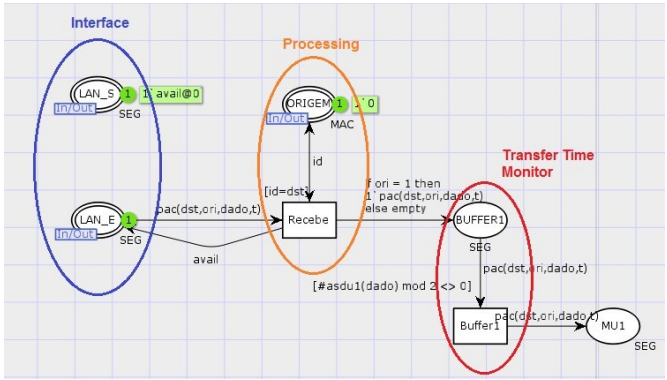

Figure 5. CPN Model of the Analyzer

D. Cyber Attack Model

In the cyber-attack model presented in color red in Figure 6, the aim of the modeled Data Modification attack is to modify the data to be transmitted before it is packed as a Sampled Value (SV) message. In this case, the value of analog data coming from the current and voltage transformers will be modified (attacked) before it is packed as a Sampled Value message.

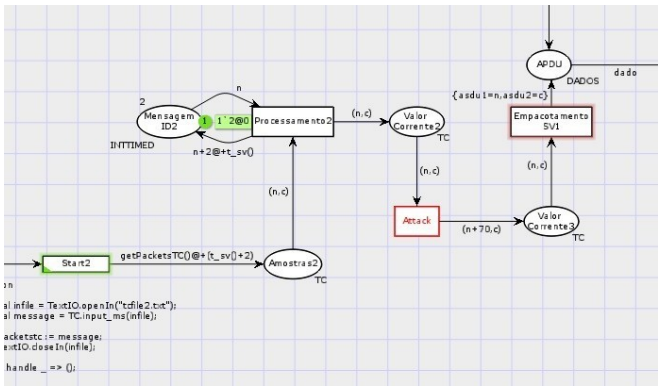

Figure 6. Cyber-attack Model

V. RESULTS AND DISCUSSION

For cyber-attack analysis, it is used the simulation tools available in the *CPN Tools software*. It follows some results generated from model simulations in Figure 7.

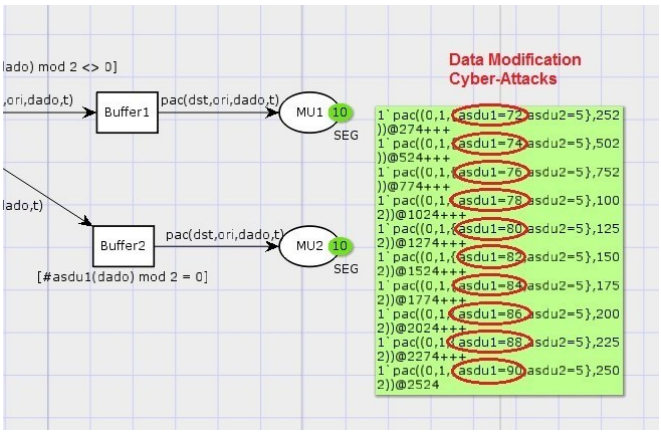

Figure 7. 1 Cyber-attack for 10 received packets

The structure of the packets is: pac (dst,ori, dado, t). This means that the first number is the destination of the datum; the second number is the origin of the datum; the third one is the value of the datum and the last one is the time spent for the datum to leave the origin and get to the final destination.

In this model, the read of the analog data coming from the current and voltage transformers comes from a txt file named *tcfile2*. In this txt file, the first ten values of the data are: (asdu1=2); (asdu1=4); (asdu1=6); (asdu1=8); (asdu1=10); (asdu1=12); (asdu1=14); (asdu1=16); (asdu1=18); (asdu1=20). As it can be noticed in Figure 9, the first ten received values of the data are: (asdu1=72); (asdu1=74); (asdu1=76); (asdu1=78); (asdu1=80); (asdu1=82); (asdu1=84); (asdu1=86); (asdu1=88); (asdu1=90). The offset between the first ten original values and the first ten received values is 70, which is in according to what was modeled in transition *Attack*, in color red in Figure 6, *n+70*, where *n+70* corresponds to asdu1 value. The presented values have been attacked by a Data Modification Attack, because the final objective of this kind of attack is to change data before they are processed at their destination, and this goal was achieved in this simple model.

So, presented results are in according to what was expected and modeled in this scenario. Knowing that any data modification of the SV messages may affect the protection and the control power systems, because its frames of messages uses layer1 of the TCP / IP model and are extremely fast, these modeled data modification in this simple IEC 61850 scenario could lead to misoperation of circuit breakers and relays, and could generate serious problems in power substations, because false data are being injected in the system.

VI.CONCLUSION

According to what is presented in this article, it is concluded that the SCPN modeling is perfectly applicable to the modeling of cyber-attacks of an IEC 61850 scenario. The presented methodology is simple, but can support some important details in the design of protection process of IEC 61850 architectures.

The results generated with simulations prove that the model responded correctly according to the functions created

to produce the cyber-attack. Also, knowing that any data modification of the SV messages may affect the protection and the control power systems, these modeled data modification in this simple IEC 61850 scenario could generate serious problems in power substations, because false data are being injected in the system.

Future projects include the modeling of new cyber-attacks that can become potential threats to substation networks. Also, those cyber-attacks can be improved and sophisticated, avoiding future possible problems with the security of the system.

VII. ACKNOWLEDGEMENTS

I would like to dedicate this work to my God, *Yahweh* (יהוה), for giving me strength to overcome difficulties.

REFERENCES

[1] IEC 61850-1, *Communication networks and systems in substations – Part 1: Introduction and overview,* Ed. 2.0., 2010.
[2] F. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. 2008 IEEE Power Energy Soc. Gen. Meet.—Convers. Del. Electr. Energy 21st Century*, Pittsburgh, PA, Apr. 2008, pp.1–5.
[3] F. Cohen, "The smarter grid," *IEEE Security Privacy*, vol. 8, pp. 60–63, Jan. 2010.
[4] H. Khurana, M. Hadley, L. Ning, and D. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, pp. 81–85, Jan. 2010.
[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, pp. 75–77, Mar. 2009.
[6] Smart Grid Interoperability Panel—Cyber Security Working Group Smart Grid Cyber Security Strategy and Requirements NIST, Gaithersburg, MD, Tech. Rep. draft NISTIR 76j, 2010.
[7] T. Chen, "Survey of cyber security issues in smart grids," in *Proc. Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II (part of SPIE DSS 2010)*, Orlando, FL, Apr. 2010, p. 77090D.
[8] T. Chen, J.C.S. Aarnoutse and J. Bufford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid", *IEEE Transactions on Smart Grid,* vol.2, no.4, pp. 741-749, Dec. 2011.
[9] R. David and H. Alla, *Discrete, Continuous, and Hybrid Petri Nets*. Berlin, Germany: Springer-Verlag, 2005, pp. j9–294.
[10] K. Jensen and L. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*. Berlin, Germany: Springer-Verlag, 2009, pp. 193–198.
[11] X. Liu, P. Zhu, Y. Zhang and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2435-2443, Sep. 2015.
[12] J. McDermott, "Attack net penetration testing," in *Proc. Workshop New Security Paradigms (NSPW),* Cork, Ireland, 2000, pp. 15–21.
[13] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing attack trees using generalized stochastic Petri nets," in *Proc. IEEE Workshop Inf. Assur.,* West Point, NY, USA, 2006, pp. 116–123.
[14] R. Wu, W. Li, and H. Huang, "An attack modeling based on hierarchical colored Petri nets," in *Proc. IEEE Int. Conf. Comput. Elect. Eng. (ICCEE),* Phuket, Thailand, 2008, pp. 918–921.
[15] K. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1123–1130, Aug. 2006.
[16] O. Gursesli and A. Desrochers, "Modeling infrastructure interdependencies using Petri nets," in *Proc. IEEE Int. Conf. Syst.,* vol. 2. Washington, DC, USA, 2003, pp. 1506–1512.
[17] J.-C. Laprie, K. Kanoun, and M. Kaaniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. 26th Int. Conf. Comput. Safety Rel. Security (SAFECOMP),* Nuremberg, Germany, 2007, pp. 54–67.
[18] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano, "Failure identification in smart grids based on petri net modeling," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4613–4623, Sep. 2011.
[19] O. Dahl and S. Wolthusen, "Modeling and execution of complex attack scenarios using interval timed colored Petri nets," in *IEEE Int. Workshop Innov. Archit. Future Gen. High-Perform. Proc. Syst.*, Kona, Hawaii, Jan. 2006, pp. 49–55.
[20] Tom Bartman and Kevin Carson, "*Securing Critical Industrial Systems with SEL Solutions"*, SEL (Schweitzer Engineering Laboratories, Inc.) White Paper LWP0013-01, Date Code 20150406, © 2015 by Schweitzer Engineering Laboratories, Inc. All rights reserved.
[21] T. Murata, "Petri Nets: Properties, Analisys and Application", Proceedings of the IEEE [0018-9219] Murata, Tadao yr:1989 vol:77 iss:4 pg:541 -580.
[22] J. R. Norris, "Markov Chains", Cambridge University Press, July 1998.
[23] CPN Tools: Available at: http://cpntools.org/. Accessed in 07/30/2014.
[24] N.Ghabi, C. Dutheillet and M. Ioualalen, "Colored stoschastic Petri nets for modelling and analysis of multicass retrial systems", Mathematical and Computer Modelling 49 (2009), pp. 1436-1448.
[25] G. Chiola, D. Dutheillet, G. Franceschinis and S. Haddad, "Stochastic Well-Formed Colored nets and symmetric modeling applications", IEEE Transactions on Computers 42 (1993), pp. 1343-1360.
[26] IEC61850-5 (2010). *Communication networks and systems in substations - Part 5:Communication requirements for functions and device model*, 2.0 edn, International Electrotechnical Commission, France.
[27] IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2:* Sampled values over ISO/IEC 8802-3,Ed. 2.0, 2010.
[28] Zaitsev, D. A. and Shmeleva, T. R. (2006). Switched ethernet response time evaluation via colored petri net model, Proc. of International Middle Eastern Multiconference on Simulation and Modelling, pp. 68-77.