https://doi.org/10.55972/spectrum.v27i1.453

ORIGINAL PAPER

Spectrum - The Journal of Operational Applications in Defense Areas

Journal homepage: https://spectrum.ita.br

Command & Control and Cyber Defense: Cyber Warfare

Modeling and Analysis of a Cyber Attack in an IEC 61850 Scenario Using Colored Petri Nets

Milton Rafael da Silva[1*]

[1]*Universidade Federal de Itajubá (UNIFEI), Itajubá/Minas Gerais – Brazil*

[*]*Corresponding Author: d2025100298@unifei.edu.br*

Keywords

Modeling of Cyber Attack
IEC 61850
Smart Grid
Colored Petri Nets
Security Analysis

Article Information

Received 10 August 2026
Revised 04 September 2026
Accepted 08 October 2026
Available 27 October 2026

Abstract

Some performance parameters of the IEC 61850 standard related to the electrical measurements in electrical power systems are defined, and these parameters are really important and critical in the automation of these systems. Related to network security analysis, a tool used is the Colored Petri Net (CPN) because it models both concurrent and asynchronous processes and is useful for analyzing data modifications in timed systems. Thus, based on this context and knowing that time is really critical in the transmission of messages in the context of the IEC 61850 standard, a cybernetic attack is modeled using CPNs to modify the data related to electrical measurements, which is really critical for the functioning of the system. The results corresponded to the modeled cybernetic attack, showing the effectiveness of the proposed modeling method.

1. Introduction

In the intelligent communication networks known as Smart Grids, important characteristics like data interchange, network topology, decentralized control and security ensure the correct and reliable operations in the electric power sector.

In order for information to be sent and received correctly, reliably and efficiently, standardization of data communication is required. To achieve this objective, the IEC 61850 standard was created, which proposes standards for the services and data formats exchanged in a network of electrical systems equipment [1].

The security of Smart Grids has been widely recognized as a major problem with potentially catastrophic implications in this scenario [2], [3], [4], [5], [6], [7]. In addition, cyberattacks can take advantage of accessibility through neighborhood area networks (NANs) or home area networks (HANs) to remotely commit or control electronic resources. With the Internet and modern telecommunications, it is now easy for geographically distributed groups to coordinate simultaneous attacks [8].

In the scenario of cyberattack modeling, Petri nets and their variations have become very important tools for studying various types of asynchronous and concurrent processes [9], [10], [11]. The usefulness of Petri Nets for cyberattack models was first pointed out perhaps by McDermott [12]. He observed that Petri nets are better at capturing simultaneous actions in the progression of an attack [8]. Dalton et al. suggested the use of generalized Stochastic Petri Networks for the modeling of cyberattacks [13]. Stochastic Petri nets are a type of timed Petri nets where transitions occur ("trigger") after random times. In their works, the transitional delays were assumed to be exponentially distributed, which conveniently transformed the Stochastic Petri Net into an equivalent continuous-time Markov Chain. The approach seems to have been motivated by the direct analysis of the possible steady state for the Markov Chains, but the fact of assuming exponential delays of transition was not clearly justified [8].

Colored Petri Nets have drawn attention to cyberattacks because they are more expressive than the basic Petri Nets. In the Basic Petri Net, all the tokens are indistinguishable from each other. In colored petri nets, tokens carry data values represented by colors that allow different attackers to be distinguished with separate identities in the model [8]. Wu et al. suggested the use of colored petri nets to model hierarchical attacks [14]. An attack represented at a high level is a simple colored Petri Net, where certain transitions have hidden details. The hidden details of this transition can be seen in an associated sub-page which is a separate-colored Petri Net [8].

In relation to the electric power system, the Petri Nets were applied to show interdependencies between the electric energy infrastructures and the pre-existing communications [15], [16], [17]. In addition, Calderaro et al. [18] presented a Petri Net-

The peer review process was coordinated, and the final publication approved, by Humberto Baldessarini Pires.

CC BY

based method to identify and locate faults in the intelligent network. Chen et al. [8] proposed a new hierarchical method to construct a large Petri Net from a series of small Petri nets to model cybernetic-physical attacks in the intelligent network. Dahl and Wolthusen have suggested the use of time-lapse colored Petri nets, where plugs carry time tags and the trigger delay of transitions are limited by specified time intervals [19]. Their concern is timed attack dependent on multiple attackers against possible multiple targets [8].

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

Related to all the previous works, and knowing the special characteristics of the standard IEC 61850, it is proposed to model and analyze the impact of a cyber-attack in a simple model with one merging unit that publish Sampled Values messages, one switch for packet exchange and storage, and one network analyzer to check and sort packets sent. This cyber attack aims to modify the transmission of sample data messages (cybernetic attack of data modification) and to evaluate their impact on the communication systems of the electric power system. The network analyzer determines which packets were attacked by the cyber attack, or which packets were not correctly sent to their final destination. Modifying data, also known as data diddling or data insertion, involves changing data before processing at their final destination [20].

This work is an extension of papers originally presented at the 2017 4th IEEE International Conference on Systems and Informatics (ICSAI), in Hangzhou, China [21], [22], [23], [24] and at XXVI SIGE (Symposium on Operational Applications for Defense), in São José dos Campos, Brasil [39].

2. Cyber Attacks

Cyber attacks are defined as the methods or means that hackers or attackers use, such as controlling communication systems, devices, programs and computer networks, and accessing certain data to achieve their goals with malicious intent. Knowledge of cyber attacks is very important to avoid or mitigate them. There are several types of cyber attacks that must be understood to ensure that an appropriate security methodology is applied.

Among the cyber attacks known in the literature, the cyber attack known as Man-in-the-Middle occurs when the attacker places himself between two points, to take control of the network, and for this attack to take place, the attacker needs to access the network physically. These types of attacks exploit the lack of authentication, and through these intrusions, the attacker can control the connection, spy on the data that passes, and insert false messages. As an example for this type of attack, attackers may manipulate a false status message from a circuit breaker or other protective equipment and send this message to the SCADA system, or modify the responses to the Human Machine Interface (HMI), presenting the operator with a false status of the system.

In the case of the direct access attack, or Insider, the attack comes from authorized personnel who deliberately manipulate the devices to produce an unauthorized condition. These types of attacks are motivated by revenge or personal gain, and are very difficult to be prevented because the attacker is a trusted user. The attacks known as malicious data insertion, data tampering, or data-diddling attacks consist of changing the data before they are processed at their final destination, and usually occur in data entry environments. In the case of repetitive attacks or data breaches, communications are spied on, intercepted and stored, to be reproduced at another time when the attacker deems appropriate.

For defense against such cyber-attacks, solid cryptography and authentication are suggested, used together to provide adequate defense. Defenses of data modification and insertion attacks also depend on authentication. An authentication method is a Hash Message Authentication Code (HMAC) used within IPsec, by using a hash function together with a key, thus generating a message authentication code, and how the authentication code is based on the content of the data, and if the data is changed, the authentication code will not match from source to destination, indicating that the data is not authentic. An HMAC is used to verify both integrity and authenticity of the data.

3. IEC 61850 and Sampled Values (SV) Messages

The integration of power systems through communication networks allows solving typical problems of conventional communication structures, such as interoperability problems of protocols, networks and devices, maintenance problems, protocol converters, and so on.

In 1995, the first efforts were made to standardize the communication aspects in the electric sector systems, specifically within the substations. Thus, two fronts have initiated this process, the Electric Power Research Institute (EPRI - USA) and the International Electrotechnical Commission (IEC - France) [25]. EPRI created specifications called Utility Communications Architecture (UCA) and the IEC formed a working group to develop a standardization project. After years of development, in 2002 an international standard for communication architectures in substations of power electrical systems, called IEC 61850, appeared.

The IEC 61850 standard is an international standard that defines the form of operation between the different equipment present in the automation of electrical power systems [26]. It models the interconnection of the automation elements, through the representation in a logical plane of the equipment. This standard has functions that interoperate in a distributed way, being able to be allocated in one or more IEDs connected in network, and this is used to integrate functions of measurement, control and protection. Physically, this makes it possible to replace control cables by communication networks, reducing the overall cost of installation, commissioning, monitoring, maintenance and diagnosis.

Some benefits obtained by using the IEC 61850 standard are cited in [27]:

- Decrease in integration efforts, since there is a standardization of equipment and communication interfaces, independent of the manufacturer;
- Direct communication with EMS / DMS / SCADA systems eliminating intercommunication devices (RTUs and Gateways);
- Direct access to all points of a power system, remotely or

CC BY

locally;

• Distributed solution that replaces centralized RTU systems increasing system reliability;

• Free allocation of functions in IEDs, offering greater flexibility;

• Plug and play solution, allowing future plant expansions;

• Significant cost reduction for implementation, integration, commissioning and maintenance.

The Sampled Values (SV) messages are inserted into the unicast or multicast transmission modes and are used to send digitized current and / or voltage data from the current and potential transformers respectively to the protective equipment and substation control.

Section 9-2 of the IEC 61850 standard defines how to transmit the sampled values over an Ethernet network through a merging unit (MU) or other electronic interface metering instrument [28].

Sampled Values (SV) messages use the link layer of the OSI (Open System Interconnection) model and the peer-to-peer communication interface and, moreover, are deterministic. At each time period, determined by the sampling frequency of the signal and the time resolution required for analog-to-digital conversion, an SV message is placed on the network [29]. This could cause increased traffic and eventual loss of packets and network conflicts and with this, SV messages are still a challenge for the full implementation of the IEC 61850 standard.

4. Modeling in Colored Petri Nets

Petri nets (PN) are a graphical mathematical tool for modeling and studying systems characterized as concurrent, asynchronous, distributed, parallel, nondeterministic and / or stochastic [30]. The PN is a bipartite graph formed by two sets: transition and place. These two components, also defined as nodes, are interconnected by directed arcs.

For the modeling and interpretation of systems, tokens assigned to the places are used, which represent the state of the system, and the movement of the tokens through the places, along with well-defined rules, represents the dynamics of the system to be modeled.

In relation to the analysis of network protocols, Stochastic Petri Net (SPN) are applied in the analysis of the performance of computer networks and communication systems, as it makes possible the analysis of probability of system states [31]. However, SPNs are limited in complex models, such as industrial size models, for example.

In the case of Colored Petri Nets (CPNs), which combine the Petri Nets (RdP) [32] with programming language, they are also a superset of ordinary Petri nets. In CPN, the tokens carry the information defined as the "color" (typification), which can be type, size, name, registry, state, etc. Places that accept "colored" tokens are also colored, for example, places that support “colors” of type “name” do not support “color” of type “size”. In relation to object-oriented languages, it is said that "colors" are the classes of objects. Transitions evaluate the tokens coming from their places of entry, and can modify the information of the token and load it to the place of exit.

In Colored Petri Nets, timing is another property used for different performance analyzes. In ordinary Petri nets, the firing is instantaneous, however, knowing that real systems have times involved, the timed tokens carry more information, which is the time stamp. The time stamp is the information of when the data will be available, so this can guarantee a stochastic analysis of the system.

Another important feature that the use of Colored Petri Nets enables is the hierarchy of networks. Some parts of the models can be grouped into modules (subsystems), called "replacement transitions", and can be reused multiple times in one model, facilitating the modeling process. They also model the complexity of user behavior allowing better understanding of the process as a whole. For a better understanding of the system, one can look inside the subsystem. With this, it is said that the modeling through the Colored Petri Nets has a greater capacity of abstraction.

Formally, the definition for the CPN is represented as $SCPN = \{P, T, CB, C, W^-, W^+, W^h, Pri, M_0, \theta\}$ [24][33][34], where: 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 $\forall t \in T$, $Pri(t)$: $C(t) \rightarrow N$.$Pri(t)(c)$ 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.

5. Modeling of an IEC 61850 System for Sending Sampled Values (SV) Messages and a Cyber Attack Using Colored Petri Nets

The following CPN models seek to represent the main characteristics of the devices presented in the proposed architecture [24]. For the development of a CPN modeling of the standard IEC 61850 together with a cyber-attack, 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 CPN, together with the modeled cyber-attack. In Figure 1, it can be seen the proposed architecture.

5.1. Switch Model

The switch model is composed by the switching table, the packet buffer, the switch processing and the physical communication interface (input and output ports). For a better understanding of this model, only one communication port is denoted. For the representation of other ports, simply replicate such a model. Figure 2 shows the main characteristics of a switch port. This model is based on the work developed in [35], in which the switch is represented by CPN models.

Figure 2 represents, in CPN, the dynamics of a packet within a real switching device. The message enters via the communication interface (port E0), then it is processed

(transitions E0 and S0), stored in the buffer (place Bu0) and then transmitted according to the switching table for the respective destination (place Swit0). This whole process takes time, called by the norm as propagation time, and for this reason it is attributed the time stamp @ + tb () in the transition S0 [24].

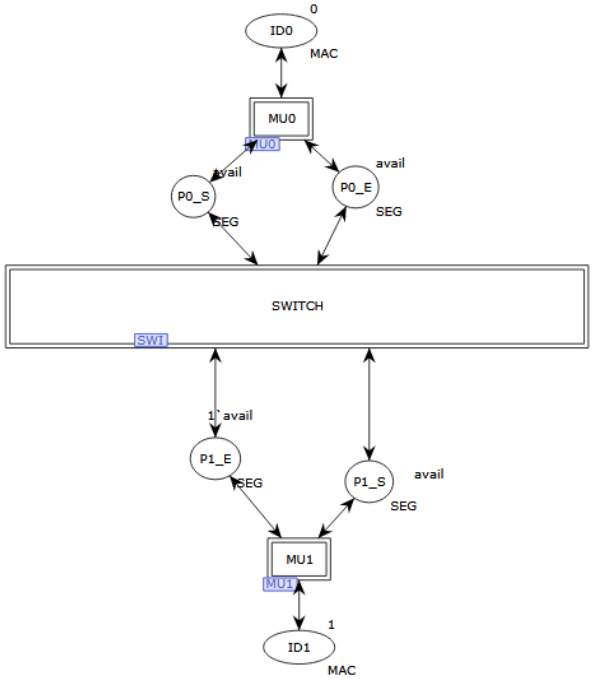


Fig. 1. Proposed Architecture

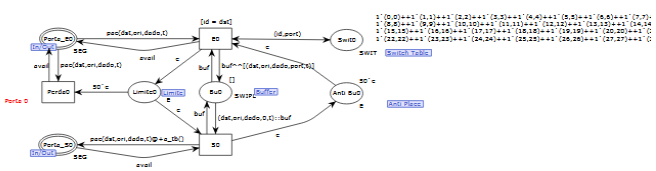


Fig. 2. Switch Model

To model these functionalities, the following color sets are defined [3], [24]: colset E = with e; colset PORT = int; colset SWIT = product INT*INT; colset SWIP = product MAC*MAC*DADOS*PORT*TEMPO timed; colset SWIPL = list SWIP. Color set E is a generic markup type for tab creation to limit the buffer. The PORT typing, of the integer class, indicates the switch port numbering. The SWIT, SWIP, and SWIPL typologies are specific to the switch model, and indicate the switch table, packets within the switch, and queue formation respectively.

5.2. Merging Unit Model

The model of Figure 3 depicts the physical merging unit device which converts the analog signals into digital signals and sends such signals in the Sampled Values message format [24]. In this figure, the most relevant aspects of this equipment are revealed. The CPN representation of the merging unit characterizes the sampling process, the processing of the samples by the logical nodes and the interface with the network.

The sampling process is done by reading a text file, called "*tcfile2.txt*" in this model, which contains the modeled current analog data that will be sampled with values ranging from 2 to 2000, simulating the data of a transformer. The text file is read through the function defined in the *Init2* transition, and through the *getPacketsTC()* function the data of the files are transformed into CPN type tokens and sent to the place of Samples. Transitions *Processing2* and *PackagingSV2*, which represent the logical nodes defined in the standard, translate sample information, or tokens, and package them in the Sampled Values format. LAN_E and LAN_S represent the communication interface of the device. The ORIGIN and DESTINY places serve to indicate to the communication interface the origin and destination of the packages generated by the merging unit. With this structure, the merging unit model is able to simulate real devices sending SV messages.

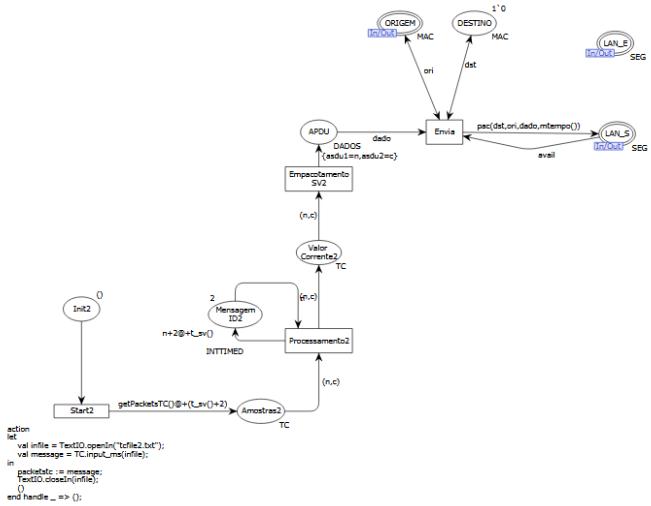


Fig. 3. Merging Unit Model

5.3. Analyzer Model

The analyzer model is characterized in a simple way according to Figure 4. The function of this model is to represent the actual device that verifies the latency time of the Sampled Values messages that travel in the network [24].

This model receives the messages through the communication interface (place LAN_E) and then verifies the origin of the package (transition Receives and place Origin) identifying the transmitting merging unit. Verified the source of the packet, the message is sent to the Buffer transition where the transfer time of each SV packet is calculated.

5.4. Cyber Attack Model

In the cyber attack model shown in red in Figure 5, the purpose of the modeled Data Modification attack is to modify the data to be transmitted before that data is packaged as Sampled Values (SV) messages. In this case, the value of the analog data coming from the current transformer will be modified (attacked) before they are packaged as messages SV.

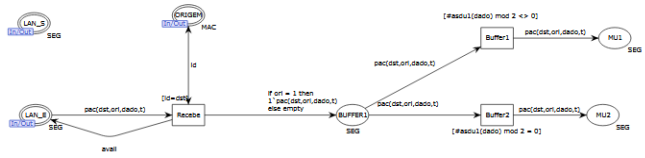


Fig. 4. Analyzer Model

It is known that data modification usually takes place in data entry environments, since merging units are electronic devices that collect and send data, which clearly characterizes a data entry environment.

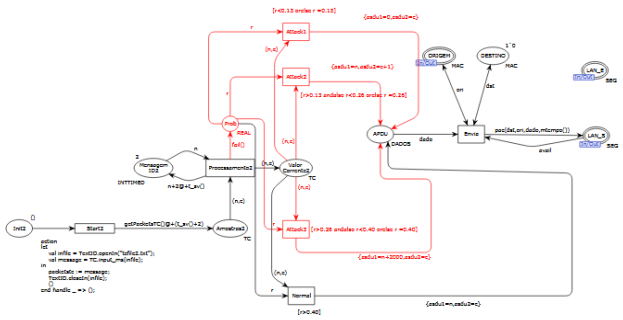


Fig. 5. Cyber Attack Model in Colored Petri Nets

For the cybernetic attack modeling proposed in this paper,in the *Transition2* the function *fail()* was created, a uniform distribution function that generates a random value between 0 and 1. As soon as this random value is generated, that value goes to *Prob*. Depending on this value, assumed by the variable *r* in the model, the *Normal* transition, the transitions *Attack1*, *Attack2* or *Attack3* will be enabled. To enable the *Attack1* transition, the randomly generated *r* value must be less than or equal to 0.13. To enable the *Attack2* transition, the randomly generated *r* value must be greater than 0.13 and less than or equal to 0.26. To enable the *Attack3* transition, the randomly generated *r* value must be greater than 0.26 and less than or equal to 0.40. Finally, to enable the *Normal* transition, the randomly generated *r* value must be greater than 0.40. This indicates a cyber attack probability of 40%. This probability of cyberattack of 40% was obtained based on a survey made in 2016 by Kaspersky Lab ICS CERTS [36].

For the correct functioning of the model and signal sampling, after processing the *Attack1*, *Attack2*, *Attack3* or *Normal* transitions, it was necessary to reset the variables *n* and *c* to *asdu1* and *asdu2*, respectively. This reset serves to ensure the correct marshaling of the data in place APDU as Sampled Value messages.

If *Normal* transition is enabled, message processing occurs normally. The subscript of the normal transition arc {*asdu1* = *n*, *asdu2* = *c*} only resets the variables *n* and *c* to *asdu1* and *asdu2*, but does not make any other changes, transmitting the packets normally. However, if any of the *Attack1*, *Attack2* or *Attack3* transitions are enabled, the value of the current analog data from the current transformers will be modified (attacked).

In case *Attack1* transition is enabled, according to the randomly generated *r* value, the values will be canceled. To trigger this transition, the value of *r* must be less than or equal to 0.13. If this situation occurs, the *Attack1* transition will pick up the packet in the *Current Value2* location and by inscribing in its trigger arc {*asdu1* = 0, *asdu2* = *c*}, the current value will be nulled (*asdu1* = 0) and the message identifier number will be maintained (*asdu2* = *c*).

For the case of the *Attack2* transition to be enabled, according to the randomly generated *r* value, the message identifier will be changed. To trigger this transition, the value of *r* must be greater than 0.13 and less than or equal to 0.26. If this situation occurs, the *Attack2* transition will pick up the packet in place of *Current Value2* and by inscribing in its trigger arc {*asdu1* = *n*, *asdu2* = *c* + 1}, the message identifier number will be changed (*asdu2* = *c* + 1) and the current value will be maintained (*asdu1* = *n*).

In case *Attack3* transition is enabled, depending on the randomly generated *r* value, the values will be changed to other values outside the ranges of the expected electrical measurements. To trigger this transition, the value of *r* must be greater than 0.26 and less than or equal to 0.40. If this situation occurs, the *Attack3* transition will pick up the packet in place *Current Value2* and through the inscription in its firing arc {*asdu1* = *n* + 2000, *asdu2* = *c*}, the values will be changed to other values outside the bands of the electrical measurements (*asdu1* = *n* + 2000), in this case the current value measurements will present an offset of 2000 of the original values and the message identifier number (*asdu2* = *c*) will be maintained.

After the *Normal*, *Attack1*, *Attack2* or *Attack3* transitions are triggered and the correct marshaling of the data in place APDU as Sampled Value messages occur, where the variables *asdu1* and *asdu2* are joined through the given variable, the pattern in which the message will be sent is set by the color set SEG, after the transition trigger sends the packet destination (place DESTINATION), its origin (place ORIGIN), the data with the current value and the message identifier number (given variable), and the stamp of time indicating the moment the message left the device (variable t). The LAN_E and LAN_S ports represent the device's input and output interfaces and are also connected to the ports representing the switch ports.

According to the "*tcfile2.txt*" file, which contains the current analog data modeled for this simulation, current values range from 2 to 2000. The Data Modification attack developed in this simulation will change (modify) this analog data by nulling the current value (through the *Attack1* transition), by changing the message identifier (through the *Attack2* transition) or by adding an offset of 2000 to the original values (through the *Attack3* transition).

Although these small modifications in the data to be transmitted may initially seem simple, they are very effective in relation to the objectives to be achieved by the cyber attack, since completely tampered data may imply in the control and protection systems of the energy substations as well as improper actuation of circuit breakers and protective relays, which can seriously damage substations.

It can be verified that in addition to being a cybernetic attack of Data Modification, this modeled cyber attack can also be characterized as a Man-in-the-Middle attack, as the attacker intercepts or subverts the communications and provides false data to the system user. Another possible classification for this cyber attack would be an insider cyber attack or direct access attack, as only authorized personnel have access to the merging units to perform this modeled attack and in this case the attacker deliberately manipulates the power system devices to

produce an unauthorized condition, since it is considered a trusted user.

5.5. Results

For the analysis of the cyber attack proposed in this work, the simulation tools available in the CPN Tools software were used. Four different simulations were performed, with different numbers of messages. It follows the Tables I to IV, and Figures 6 to 9, with the results generated by the simulations of the proposed model.

Table I. Transmission of Messages and Modified Data – 1st simulation.

Tranmission of Messages	Number of Messages
Normal	7
Null Data	2
Change of Message Identifier	0
Out of Range Values	1

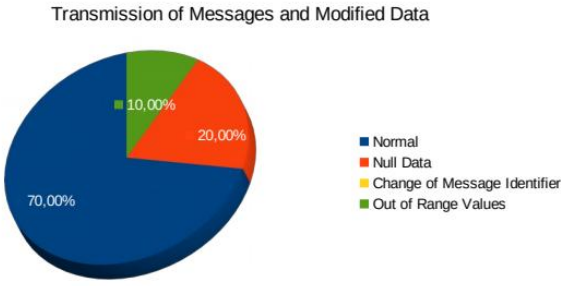


Fig.6. 3 modified data in 10 data received.

Table II. Transmission of Messages and Modified Data – 2nd simulation.

Tranmission of Messages	Number of Messages
Normal	14
Null Data	2
Change of Message Identifier	0
Out of Range Values	4

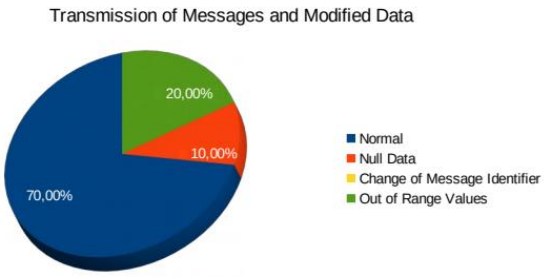


Fig. 7. 6 modified data in 20 data received.

Table III. Transmission of Messages and Modified Data – 3rd simulation.

Tranmission of Messages	Number of Messages
Normal	101
Null Data	19
Change of Message Identifier	24
Out of Range Values	16

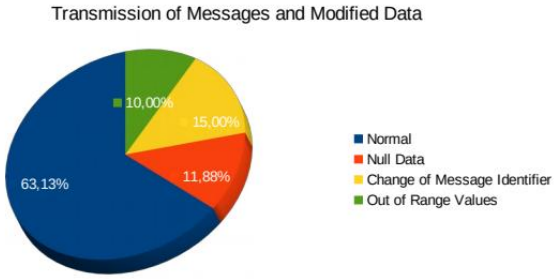


Fig. 8. 59 modified data in 160 data received.

Table IV. Transmission of Messages and Modified Data – 4th simulation.

Tranmission of Messages	Number of Messages
Normal	588
Null Data	127
Change of Message Identifier	144
Out of Range Values	141

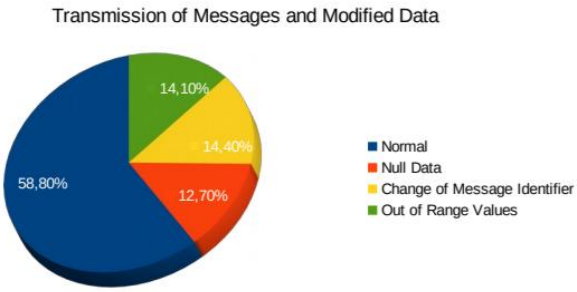


Fig. 9. 412 modified data in 1000 data received.

As it can be seen in Table I and Figure 6, 7 packets of messages were sent correctly to the final destination, 2 packets had their values nulled (*asdu1* = 0), there were no packets with message identifiers adulterated from (*asdu2* = 5) to (*asdu2* = 6), as it was modeled in this work and 1 package had its value adulterated for a value outside the ranges of electrical measurements (*asdu1* value above 2000).

In the case of Table II and Figure 7, 14 packets of messages were correctly sent to the final destination, 2 packets had their values nulled (*asdu1* = 0), there were no packets with message identifiers adulterated from (*asdu2* = 5) to (*asdu2* = 6), as it was modeled in this work and 4 packages had their values adulterated for values outside the ranges of electrical measurements (*asdu1* values above 2000).

In the case of Table III and Figure 8, 101 packets of messages were correctly sent to the final destination, 19 packets had their values nulled (*asdu1* = 0), 24 packets had the message identifier adulterated from (*asdu2* = 5) to (*asdu2* = 6), as it was modeled in this work and 16 packages had their values adulterated to values outside the ranges of electrical measurements (*asdu1* values above 2000).

In the case of Table IV and Figure 9, 588 packets of messages were correctly sent to the final destination, 127 packets had their values nulled (*asdu1* = 0), 144 packets had the message identifier adulterated from (*asdu2* = 5) to (*asdu2* = 6), as it was modeled in this work and 141 packages had their values adulterated to values outside the ranges of electrical measurements (*asdu1* values above 2000).

The presented values were attacked by a data modification attack, as it was proposed in this work, because the final objective of this type of attack is to change the data before being processed at the final destination, and this objective was reached. In the case of the last simulation, for 1000 packets sent, 41.2% of the packets were attacked by the modeled cyber attacks, which is in agreement with the probability of cybernetic attack of 40% proposed in this model.

In addition, the classification proposed in the Network Analyzer acted correctly, confirming the solid modeling of the system initially defined in this work.

It is also noted that in addition of being classified as a cybernetic Data Modification attack, this modeled cyber attack can also be defined as a man-in-the-middle attack, as the attacker intercepts or subverts communications and provides false data to the system user. Another possible classification for this cyber attack would be an insider attack or direct access attack, since only authorized personnel have access to merging units to perform this action and in this case the attacker deliberately manipulates the power system devices to produce an unauthorized condition, since it is considered a trusted user.

The results presented are in line with what was expected and modeled in this scenario. Knowing that any modification of data from Sampled Value messages can affect protection and power control systems because their message frames use layer 2 of the TCP / IP model and are extremely fast, these models of data modification in this simple scenario IEC 61850 could lead to incorrect operation of circuit breakers and relays and could cause serious problems in power substations because false data is being entered into the system.

Related to the extension of previous papers [21], [22], [23], [24] and [39], in this reasearch, for the cybernetic attack modeling proposed in this article, the function *fail()* was created, a uniform distribution function that generates a random value between 0 and 1. Depending on this value, assumed by the variable *r* in the model, the *Normal* transition, the transitions *Attack1*, *Attack2* or *Attack3* will be enabled. To enable the *Attack1* transition, the randomly generated *r* value must be less than or equal to 0.13. To enable the *Attack2* transition, the randomly generated *r* value must be greater than 0.13 and less than or equal to 0.26. To enable the *Attack3* transition, the randomly generated *r* value must be greater than 0.26 and less than or equal to 0.40. Finally, to enable the *Normal* transition, the randomly generated *r* value must be greater than 0.40. This indicates a cyber attack probability of 40%. This probability of cyberattack of 40% was obtained based on a survey made in 2016 by Kaspersky Lab ICS CERTS [36]. If *Normal* transition is enabled, message processing occurs normally. However, if any of the *Attack1*, *Attack2* or *Attack3* transitions are enabled, the value of the current analog data from the current transformers will be modified (attacked).

In case *Attack1* transition is enabled, according to the randomly generated *r* value, the values will be nulled. To trigger this transition, the value of *r* must be less than or equal to 0.13. For the case of the *Attack2* transition to be enabled, according to the randomly generated *r* value, the message identifier number will be changed. To trigger this transition, the value of *r* must be greater than 0.13 and less than or equal to 0.26. In case *Attack3* transition is enabled, depending on the randomly generated *r* value, the values will be changed to other values outside the ranges of the expected electrical measurements. To trigger this transition, the value of *r* must be greater than 0.26 and less than or equal to 0.40.

6. Mitigation Techniques of the Proposed CyberAttack

Considering the case of the Data Modification cyber attack, the use of data authentication and encryption together can provide adequate defense in this type of attack. According to [20], the risk of data modification is mitigated in cryptographic Ethernet protocols. In addition, the hash-based messaging (HMAC) authentication algorithm can be used as a mitigation technique for this type of attack.

Considering both the cases of Man-in-the-Middle and Insider (Direct Access or Unauthorized Access) cyber attacks, the mitigation technique for these types of attacks is the use of strong encryption through protocol (IPsec) with PKI, which provides a method of encryption and authentication, as well as access control and firewall state checking [20].

However, in the case of the IEC 61850 environment, knowing the critical time in the transmission of Sampled Value (SV) messages, it is practically unfeasible to insert an encryption processing to authenticate the messages to be transmitted, since the processing time of this encryption prevent the correct sending of messages Sampled Value (SV). According to [37], the processing times of two HMAC algorithms, such as HMAC-MD5 and HMAC-SHA-1, are in the order of 90 ms and 148 ms, while the transmission times of the Sampled Value messages are in the order of 3 milliseconds (high-speed messages).

Thus, the best solution to mitigate these cyber attacks would be through the control of access to the medium and the use of firewalls, as long as this does not impact the transmission of the Sampled Value messages.

7. Conclusion

According to what is presented in this work, it is concluded that the modeling in Colored Petri Nets is perfectly applicable to the modeling of cyber attacks of an IEC 61850 scenario. The presented methodology can support some important details in the design process of protection of the architectures IEC 61850.

The results generated with simulations prove that the model responded correctly according to the functions created to produce the cyber attack. In addition, knowing that any data modification of Sampled Values messages may affect the protection and control power systems, this cybernetic data modification modeled in this simple IEC 61850 scenario can generate serious problems in power substations, since data are being entered into the system.

Note also the correct classification of the data received by the Network Analyzer. This modeling can be useful for real-time measurement and control devices in substations, alerting operators about incorrect measurements and possible intrusions in the electrical system's communication systems.

It is also observed that through the development of automated threat models, as proposed in this work, one can identify the most probable steps for the execution of a cybernetic attack in these situations. This can interrupt a threat

or the evolution of a potential attack by proposing a security methodology for the system.

Finally, it can be seen that the mitigation techniques proposed in this paper, based on the literature consulted, may not be as effective. In the case of the Data Modification and Man-in-the-Middle attacks, it was proposed to use data encryption to provide adequate defense in these types of cyber attacks. However, according to what has been discussed in [38], the encryption times are much longer than the critical times for the transmission of Sampled Value messages.

According to [29], at each time period, determined by the sampling frequency of the signal and the time resolution required for the analog-digital conversion, an SV message is placed on the network. With this, there is an increase in traffic and eventual loss of packets and network conflicts. For these reasons, SV messages are still a challenge for the full implementation of the IEC 61850 standard.

This prevents the application of encryption and authentication in the transmission of Sampled Value messages. For any of the attack cases, whether Data Modification, Man-in-the-Middle or Insider, the best protection option is through access control to the medium.

Conflicts of interest

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author contributions

Milton Rafael da Silva: Conceptualization, Methodology, Writing - original draft, Software, Validation, Writing - review and editing, Supervision. All authors have read and agreed to the published version of the manuscript.

Data availability

The data that support the findings of this study are available in the references cited in this study and during the simulations executed.

Funding information

This research was supported by CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) under PhD Fellowship. Also, this research was supported by Google, through the 2025 Google PhD Fellowship Program, in the category of Privacy, Safety and Security.

Acknowledgment

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] MCDANIEL, Patrick; MCLAUGHLIN, Stephen. Security and privacy challenges in the smart grid. IEEE Security & Privacy, v. 7, n. 3, p. 75-77, 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] Bartman, T.; Carson, K. Securing critical industrial systems with sel solutions.

[21] M. R. da Silva, P. H. F. Machado, L. E. de Souza and C. W. de Souza, 2017, November. Modeling of a cyber-attack in an IEC 61850 scenario using stochastic colored Petri Nets. In *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 985-990). IEEE.

[22] M. R. da Silva, L. E. de Souza and C. W. de Souza, 2017, November. Modeling of a data modification cyber-attack in an IEC 61850 scenario using stochastic colored Petri Nets. In *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 991-995). IEEE.

[23] M. R. da Silva, P. H. F. Machado, L. E. de Souza and C. W. de Souza, 2017, November. Colored Petri Net modeling of communication systems based on IEC 61850. In *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 1001-1006). IEEE.

[24] M. R. da Silva. Modelagem de um Ataque Cibernético em um ambiente IEC 61850 usando Redes de Petri Coloridas. 2018.

[25] I. Canales *et al*. Interuca project: Uca interoperability for distributed

control within electrical substations. Cigré 2004, n. B5-204, p. 1–8, 2004.
[26] P. Code. Communication networks and systems in substations–Part 5: Communication requirements for functions and device models. 2003.
[27] J.-C. Tan; V. Green, J. Ciufo. Testing iec 61850 based multi-vendor substation automation systems for interoperability. In: IEEE.Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES. [S.l.], 2009. p. 1–5.
[28] IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2:* Sampled values over ISO/IEC 8802-3,Ed. 2.0, 2010.
[29] D. M. Ingram *et al*. Performance analysis of iec 61850 sampled value process bus networks. IEEE Transactions on industrial informatics, IEEE, v. 9, n. 3, p. 1445–1454, 2013.
[30] T. Murata, "Petri Nets: Properties, Analysis and Application", Proceedings of the IEEE [0018-9219] Murata, Tadao yr:1989 vol:77 iss:4 pg:541 -580.
[31] J. R. Norris, "Markov Chains", Cambridge University Press, July 1998.
[32] C. A. Petri. Kommunikation mit automaten. 1962.
[33] N. Ghabi, C. Dutheillet and M. Ioualalen, "Colored stochastic Petri nets for modelling and analysis of multicasts retrial systems", Mathematical and Computer Modelling 49 (2009), pp. 1436-1448.
[34] 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.
[35] 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.
[36] Kapersky, [online] Available: https://www.kaspersky.com.br/about/press-releases/2017_cerca-de-40-dos-computadores-industriais-enfrentaram-um-ciberataque-no-2-semestre-de-2016
[37] T. Xiaoyong *et al*. A novel security-driven scheduling algorithm for precedence-constrained tasks in heterogeneous distributed systems.IEEE Transactions on Computers, IEEE, v. 60, n. 7, p. 1017–1029, 2011
[38] P. Mahajan, A. Sachdeva. A study of encryption algorithms AES, DES and RSA for security. Global Journal of Computer Science and Technology, 2013
[39] M. R. da Silva, 2024, October. Modeling of a Data Modification Cyber-Attack in an IEC 61850 Scenario Using Stochastic Colored Petri Nets. In *XXVI SIGE (Symposium on Operational Applications for Defense)*. Available: https://www.sige.ita.br/edicoes-anteriores/2024/st/240427_1.pdf?x11208