Computer Science and Engineering 2022, 12(1): 1-14
DOI: 10.5923/j.computer.20221201.01

Petri Net-Based (PN) Cyber Risk Assessment and Modeling for Zambian Smart Grid (SG) ICS and SCADA Systems

Lukumba Phiri*, **Simon Tembo**

Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia

Abstract Supervisory Control and Data Acquisition (SCADA) networks are used across the globe to manage commercial and industrial control systems connected to energy, water, and telecommunications infrastructures. The connectivity provides immense benefits such as reliability, scalability, and remote connectivity, but at the same time exposes an otherwise isolated and secure system, to global cybersecurity threats. This inevitable transformation to highly connected systems thus necessitates effective security safeguards to be in place as any compromise or downtime of SCADA systems can have severe economic, safety, and security ramifications. To enhance the reliability and resilience of power grid networks there is a paradigm shift from legacy networks to smart grid networks. The Zambian power grid operator and mining companies in tandem with global players are transitioning from legacy-based protocols to Internet Protocol-based (IP-based) communications. Therefore, estimating possible cyberattack impacts and identifying system vulnerabilities are a concern in SCADA management and operations. However, it is quite difficult to plan, execute and review vulnerability analysis in critical infrastructure systems as well as in industrial control systems (such as SCADA systems) due to the complexity, and heterogeneity of these systems. A consistent domain-specific conceptual model is required to consequently establish a generic framework for cybersecurity analysis to examine and investigate security threats on smart grid systems. This paper proposes the use of Petri nets to model a framework for cyberattack response for smart grid infrastructure.

Keywords Petri Nets, Cyberattacks, Modeling, Risk assessment, SCADA

1. Introduction

Industrial control systems (ICS) are a major segment within the operational technology sector. It comprises systems that are used to monitor and control industrial processes. SCADA are industrial systems that use control devices, network protocols, and graphical user interfaces for gathering and analyzing real-time data. SCADA systems are utilized to monitor and command a plant or other critical infrastructures such as hydropower plants, telecommunications, water and waste control, oil and gas refining, and energy in general. Currently, cloud computing and the Internet of Things (IoT) offer a paradigm shift rapidly increasing innovation, flexible resources, and help in lowering operating costs. ICS is transitioning to cloud computing and IoT to improve supervisory and control processes by sharing real-time information among machines, manufacturing chains, suppliers, and customers. SCADA systems feature unique cyber and physical interaction and were originally built as air-gapped or isolated systems, connecting them to the internet potentially creates a security problem (Awad et al., AlGhazo, Davis, et al., and Handa et al.) [1]-[4].

A huge wave of global cyber security events on electric grids has been observed since the Stuxnet was first reported. Black Energy, compromised the industrial control systems (ICSs) of numerous national critical infrastructures in the U.S in 2011. Shamoon, a self-replicating computer malware-infected three-quarters of Windows-based corporate PCs at Saudi Aramco, one of the world’s largest oil companies [5]. An analogous attack on Saudi Aramco was initiated in August 2017. In February 2013, JEA was hit by a distributed denial-of-service (DDoS) attack, which led to a crash of online and telephone payment systems for a few days [6].

The rapid growth in the use of internet-based technologies has resulted in various organizations being subjected to cyberattacks [7]. The classical security measures, such as a firewall, have proved to be inadequate, as hackers deliberately avoid firewall protection as demonstrated in [8] by Coffey K. et al. It is, therefore, of paramount importance to find effective solutions that can dynamically and adaptively defend the network systems [9].

* Corresponding author:
phirilukumba@gmail.com (Lukumba Phiri)
Received: Dec. 29, 2021; Accepted: Jan. 8, 2022; Published: Jan. 21, 2022
Published online at http://journal.sapub.org/computer

The case studies are based on the Zambian grid system. Simulations are performed to evaluate the scenario vulnerabilities.

A. Case study and Implementations

We will consider a single firewall and password as an implemented intrusions prevention mechanism. For single-area, we look at the integrity of measurement data delivered over a local area communication network (Substation). For multi-area state estimation, we look at the integrity of data exchanged between the control centers of NCC and KGL (Power station) in face of a targeted trojan that compromises an endpoint of the secure communication tunnel.

B. Simulation Results

The attacks launched from different locations will result in different levels of vulnerability. Two cases are considered for evaluation:

i. Passive attack
ii. Active attack

The paper has been designed in the following way: the (II) second section gives a literature review of the techniques used for cyberattack intrusion and detection, the (III) third section introduces the concept of Petri nets, the (IV) fourth section deals with performance modeling, the (V) the fifth section gives the simulation details and results and finally with conclusions in the (VI) sixth section.

2. Related Work

In the literature, several studies have discussed cyber-physical security and the dependability of power systems. In [10] they simulated one real-world use case and two planned extensions of a factory environment using a Modular Petri Net Approach. Their model depicted information-based dependencies within smart factory networks and allowed for the simulation and analysis of threat propagation. A Susceptible-Exposed-Infectious-Recovered (SEIR) model and a new model Susceptible-Exposed-Infectious-Recovered-Delayed Quarantined (Susceptible/Recovered) (SEIDQR(S/I)) along with hybrid quarantine strategy was proposed in [11] and analyzed using Stochastic Petri Nets and Continuous Time Markov Chain.

The authors in [12,13,14] proposed the use of Petri nets in industrial control systems and smart grid as opposed to attacking trees because Petri nets offer more flexibility and expressiveness than traditional attack trees to represent the actions of simultaneous attackers. Mahmoudi and Payam [15] posits that the primary step to analyze the types of cyber-attacks is the ability to define the attacks in an adjustable way in a parametric model so that one can explicitly test different forms of attacks and subsequently offer methods to deal with them. In their study, a multi-stage attack was extracted and modeled with a timed Petri net and colored Petri net (CPN), and then the results were compared with those of similar articles.

Attacking IEC-60870-5-104 SCADA Systems [17], in this paper, attention was on the security issues of the IEC 60870-5-104 (IEC-104) protocol, which is widely utilized in the European energy sector. In particular, a SCADA threat model based on a Coloured Petri Net (CPN) was provided and four different types of cyberattacks against IEC-104 were emulated. Lastly, AlienVault's risk assessment model was used to evaluate the risk level that each of these cyber attacks introduces to the proposed system. [18] The most common cyber threats targeting end-users and terminals are caused by malicious software, called malware. The malware detection process can be performed either by matching their digital signatures or analyzing their behavioral models. As the obfuscation techniques make the malware almost undetectable, the classic signature-based anti-virus tools must be supported with behavioral analysis. The proposed approach to modeling malware behavior is based on colored Petri nets [18,20]. Our research approach will be similar to [19], who proposed the derivation of steady-state probabilities of the power communication infrastructure based on today's cybersecurity technologies. The elaboration of steady-state probabilities is established on (i) modified models developed such as password models, (ii) new models on digital relays representing the authentication mechanism, and (iii) models for honeypots/honeynet within a substation network. A generalized stochastic Petri net (GSPN) is utilized to formulate the detailed statuses and transitions of components embedded in a cyber-net. Comprehensive steady-state probabilities are quantitatively and qualitatively performed.

In contrast to [18,19,20], authors in [16] proposed the use of a program model based on FIPN to control DES and the method for generation of this model using the graphical representation of the net. FIPN offers a better visualization in comparison to discrete PNs and it allows for the quick creation of program code through the application of a simulator called FIPN-SML. [21] evaluated the risk of cyberattacks for hazardous liquid loading operations, [23] illustrated how cause-effect relationships can be conveniently expressed for both analysis and extension to large-scale smart grid systems using graph-based dynamical system model simulated in MATLAB/Simulink using the fourth-order Runge-Kutta method. The authors in [23] furthermore reevaluated the earlier framework in [24], where they illustrated through a case study of the Western Electricity Coordinating Council 3-machine, a 9-bus system using MATLAB and PSCAD simulations to validate the approach.

However, through the literature review, we can see that every framework tried to address a few challenges of the different important constituents of the smart grid infrastructure framework. We shall use GSPNs [61,62,63,64] to model for the proposed cyber framework. Since the state space grows exponentially as the number of components increases, we adopt a technique to reduce the state space and show that the technique is feasible in analyzing the steady-state availability for the proposed framework.

3. System Model

The SCADA or Industrial Control Systems (ICS) network comprises a database server, a human-machine interface (HMI), an engineering workstation, a SCADA Master, a DMS & EMS, a remote terminal unit (RTUs), and intelligent electronic devices (IED) [27]. The ICS topology is shown in Fig. 1.

3.1. SCADA Attacks

The vulnerability of a smart grid network is the weak spot at which an attacker may enter the network and attack the system. The smart grid connects with multiple domains using different protocols, making it vulnerable to numerous cyberattacks. In this section, we explore the conditions that might increase the vulnerability of the grid to cyber intrusion. However, first, we discuss the types of cyberattacks. There are mainly two kinds of attacks: (1) passive attacks and (2) active attacks. Passive attacks are those in which no harm to the data is done, but the attacker only monitors the data, whereas the active attacks are more dangerous compared to active attacks, as the attacker modifies the data or stops the receiver from receiving the data [28].

The National Institute of Standards and Technology (NIST) describes major causes that make the smart grid vulnerable to cyberattacks are as follows:

1. Increased installation of intelligent electronic devices (IEDs): As the number of devices in the network rises, the number of attack sites for attackers increases as well. Even if the security of a single point is compromised, the entire network system would be impacted.
2. Installation of third-party components: Third-party components that are not advised by experts increase the network's vulnerability to cyberattacks. These devices may be infected with trojans, which can then infect other devices on the network.
3. Inadequate personnel training: Proper training is necessary to operate any technology. When staff is not sufficiently taught, they might easily fall victim to phishing attempts.
4. Using Internet protocols: Not all protocols are secure when it comes to data transmission. Certain protocols transfer data in an unencrypted format. As a result, they are easy candidates for data extraction via man-in-the-middle attacks.
5. Maintenance: While the primary goal of maintenance is to keep things functioning properly, it can become a vector for cyberattacks at times. While doing maintenance, operators often disable the security system to conduct testing. In 2015, electric power companies in eastern Europe reported one similar occurrence [34].

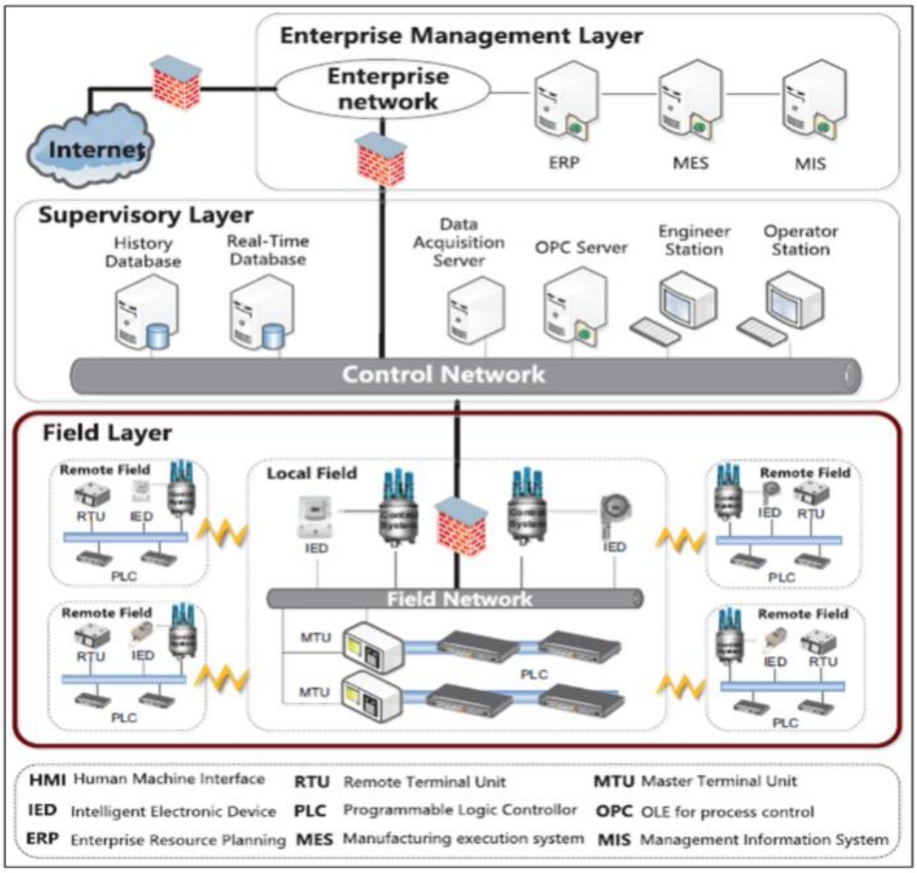

Figure 1. Sample SCADA network for a case study [27]

There are five main goals of cybersecurity in smart grids that are described below. Table 1 provides the summary of the attack category and security goal they compromise.

1. Authentication: The verification of the user. The system verifies whether the credentials provided by the user are correct or not. Various authentication techniques in the smart grid network are presented in [35].
2. Authorization: The user is authenticated when he provides the correct credentials. Now, the user becomes authorized to use the services and to transmit and receive data packets. In an unencrypted authentication process, credentials inserted by the users are exposed to the attacker, and later, the attacker uses the credentials and pretends to be an authorized user.
3. Confidentiality: This ensures that only authorized users have the access to the data. There is an abundance of sensitive data circulating throughout the smart grid network. This information comprises client energy consumption statistics, a customer identification number, and a list of appliances in use by consumers. An attacker can use this information to investigate the customer's energy use patterns. Additionally, if unauthorized users have access to the data, an ICMP (Internet Control Message Protocol) flood attack can be launched and the reading can be tampered with or altered [22]. As a result, utilities may face severe financial difficulties or customers may get excessively high bills.
4. Integrity: This protects the recipient against data tampering by ensuring that the data is not changed or corrupted during transmission. Parity check, checksum error, and several other similar techniques are utilized at the receiving end to verify that the data have not been modified. False data injection attack (FDIA) is one of the most frequently used forms of attack. An injection attack adulterates the genuine data with fake data.
5. Availability: Availability ensures that whenever the user requires resources or/and data, they are always available. Various factors can affect the availability such as fault at the data center, but in terms of cybersecurity, it is affected by cyberattacks such as denial of service (DoS) attacks. During a DoS attack, the resources are hijacked by the attackers and user requests are not served due to a lack of resources.

3.2. Defence Mechanisms

SCADA systems typically have specially designed firewall rules and password policies to achieve a high level of computer security [59]. A firewall is a technology of cyber security defense that regulates the packets flowing between two networks [59], [19]. As there may be different security trust levels between networks, a set of firewall rules is configured to filter out unnecessary traffic. These rules are written with the following criteria for acceptance or rejection [59]:

1) Type of protocols
2) Incoming and outgoing traffic
3) Specific port service or a port service range
4) Specific IP address or an IP address range

These audit fields are recorded in a firewall and are used offline by a system administrator to analyze malicious behaviors [59] [60]. Due to the high volume of daily network traffic, it is not practical for a system administrator to monitor the network with the available datasets. Thus, an add-on commercial firewall analyzer is required to detect anomalies in these datasets [60].

Therefore, malicious packets flowing through a firewall must be identified together with the traffic denied by the firewall, such data can determine the probability of cyber attack occurrences either being granted access or being attempted. These datasets can be analyzed from the firewall logs in two ways:

1) The number of records rejected compared to the total number of firewall traffic records, and
2) The number of malicious records bypassing compared with total records for each rule.

4. Performance Modeling

4.1. Petri Nets and GSPNs

The SPN [62] model is composed of three components: places (circles), transitions (rectangular bar), and arcs (arrows). The places represent the states or resources of the system. The transitions represent the events that enable the system's state transfer. The arcs illustrate the relationship between the places and transitions. Compared with other schemes like prototype design, the SPN is more efficient in conserving resources such as time and energy. Accordingly, we decide to adopt the SPN in the system modeling and analysis.

Firstly, we need to construct the performance evaluation model of the target system. That depends on the system under analysis. Therefore, we directly give a sample model as shown in Figure 2.

Secondly, we can construct the Markov Chain (MC) that is isomorphic to the SPN model. At first, we can easily get the reachable graph of the SPN model (as shown in Figure 3). Then, we assume the transition firing rate average is $\lambda = \{\lambda 1, \lambda 2, \lambda 3, \lambda 4, \lambda 5\}$. Lastly, we get the MC by replacing the transition ti with the corresponding λi. The reachable markings set and the MC of the simple SPN model above are shown in Table 2 and Figure 3.

Table 1. Summary of the attack category and security goal

Attack Category	Security Goal Compromised	Description	Reference
Flooding attack	Availability	Deterring users from utilizing the resources	[38,39]
Denial of service	Availability	Stop serving of users' request	[40-43]
Jamming	Availability	Jamming the network	[44-45]
Buffer overflow,	Availability, Confidentiality	Overwriting the memory of the buffer	[46]
False Data Injection	Integrity	Tampering the real data	[47-51]
Social Engineering Attack	Integrity, Confidentiality	Attacking humans instead of machines or networks	[51-53]
Man-in-the-middle	Confidentiality	Extracting packet information between sender and receiver	[54]
Packet Sniffing	Confidentiality	Analyzing the packet	[56]
Session hijacking attack	Integrity, Confidentiality	Obstructing the user from resources for a particular amount of time	[56]
Data manipulation	Integrity	Data tampering	[57]
Replay Attack	Integrity	Send data, again and again.	[58,59]

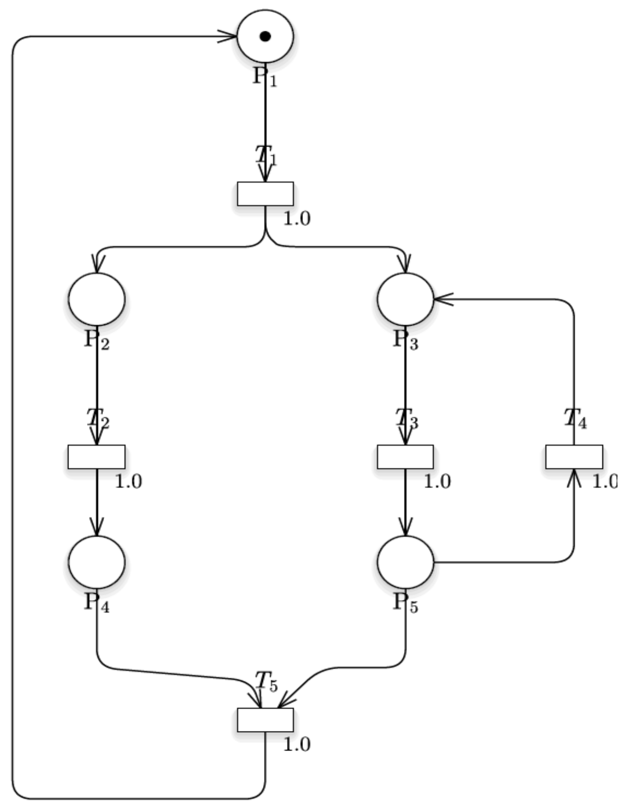

Figure 2. A sample of the Stochastic Petri Nets (SPN) model

Table 2. Reachable markings' set of the sample

	P1	P2	P3	P4	P5
M0	1	0	0	0	0
M1	0	1	1	0	0
M2	0	1	0	0	1
M3	0	0	1	1	0
M4	0	0	0	1	1

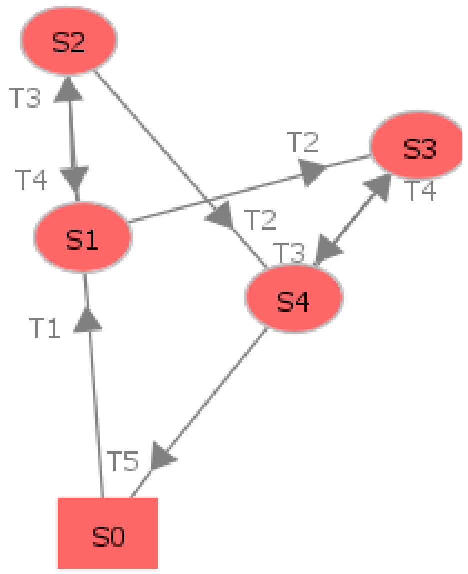

Figure 3. The reachability graph of the sample SPN

Thirdly, we can work on the system performance evaluation with the steady-state probability based on the MC. Some formulas help the theoretical inference. They are as follows.

We assume that there are n states in the MC. The transition matrix can be defined as: Q = [qi,j], i ≤ i, j ≤ n; where:

$$qi,j = \begin{cases} the\ rate\ on\ the\ arc\ from\ Mi\ to\ Mj\ when\ i \neq j \\ 0, no\ arc\ from\ Mi\ to\ Mj\ when\ i \neq j \\ -\sum_k \lambda k, i = j \end{cases} \tag{1}$$

Then, we assume the steady-state probability is a row vector P = {p1, p2, p3, _ _ _, pn}.

According to the Markov process, we can get the system of linear equations as follows:

$$\begin{cases} PQ = 0 \\ \sum_i Pi = 1, 1 \leq i \leq n \end{cases} \tag{2}$$

We can get the steady probability of each state by resolving the system of linear equations above.

Ulteriorly, we can get further parameters, such as:

(1) Residence time in each state M:

$$\tau(M) = (-r_{i,j})^{-1} = (\textstyle\sum_{tj \in H} \lambda j)^{-1} \tag{3}$$

Where H is the transitions' set that can be enforceable at M.

(2) Token density function:

$$P[M(P) = i] = \textstyle\sum_j P[M_j] \tag{4}$$

Where, $M_{j \in}[M(p) = i], M_j(p) = i$

(3) Average number of tokens on a place:

$$\bar{u}_i = \textstyle\sum_j xP[M(p_i) = j \tag{5}$$

The average number of tokens of a place set Pi is the sum of each place's average number of tokens.

It can be expressed as:

$$\bar{N} = \textstyle\sum_{Pi \in Pi} \bar{u}_i \tag{6}$$

Where the place is Pi $\in$ Pj.

(4) Utilization rate of the transition:

$$U(t) = \textstyle\sum_{M \in E} PM \tag{7}$$

There, E represents the set of all reachable markings that make t enforceable.

(5) Token velocity of the transition:

$$R(t, s) = W(t, s)xU(t)x\lambda \tag{8}$$

There, λ stands for the average transition firing rate of t. Based on all the performance parameters mentioned above, we can do further research on the system response time and so on.

4.2. The SPN Model of Scenario I: Firewall Model

We construct the SPN model for Defense Scenario I, using a single server and depicting a substation interface with another remote SCADA substation network shown in Figure 1. We denote λ = {λ0, λ1, λ2, λ3, λ4, λ5, λ6, λ7, λ8, λ9, λ10} as the average transition triggering rate and P = {P0, P1, P2, P3, P4, P5, P6, P7} as the steady-state probability. We can get the set of reachable markings as M = {M0, M1, M2, M3, M4, M5, M6, M7} and the isomorphic model together with the Markov Chain (MC) and the process of SPN. The isomorphic model is shown in Figure 5.

Table 3. Places and Transitions for the GSPN Model

Places	Description	Rates
Po	Intrusion attempts begin P_Begin	
P1	Intruder cracks rule 1 P_Rule1a	
P2	Intruder fails rule 1 P_Rule1a	
P3	Intruder cracks rule 2 P_Rule1a	
P4	Intruder fails rule 2 P_Rule1a	
P5	Intruder cracks rule 3 P_Rule1a	
P6	Intruder fails rule 3 P_Rule1a	
P7	The system is breached P_SysBreach	
Transition	**Description**	**Rate**
T0	Crack rule number 1 T_crack1a	λa (0.01)
T1	Fail Firewall rule number 1 T_fail1b	λb (0.99)
T2	Crack Firewall rule number 2 T_crack2a	λc (0.01)
T3	Fail Firewall rule number 2 T_fail2b	λd (0.99)
T4	Crack rule number 3 T_crack3a	λe (0.01)
T5	Fail Firewall rule number 3 T_fail3b	λf (0.99)
T6	Firewall execution rate1 T_rate1	λg (10^{-6})
T7	Firewall execution rate2 T_rate2	λh (10^{-6})
T8	Firewall execution rate3 T_rate3	λi (10^{-6})
T9	Firewall execution rate4 T_rate4	λj (10^{-6})
T10	Firewall recovery rate T_Recover	λk (0.5E-6)

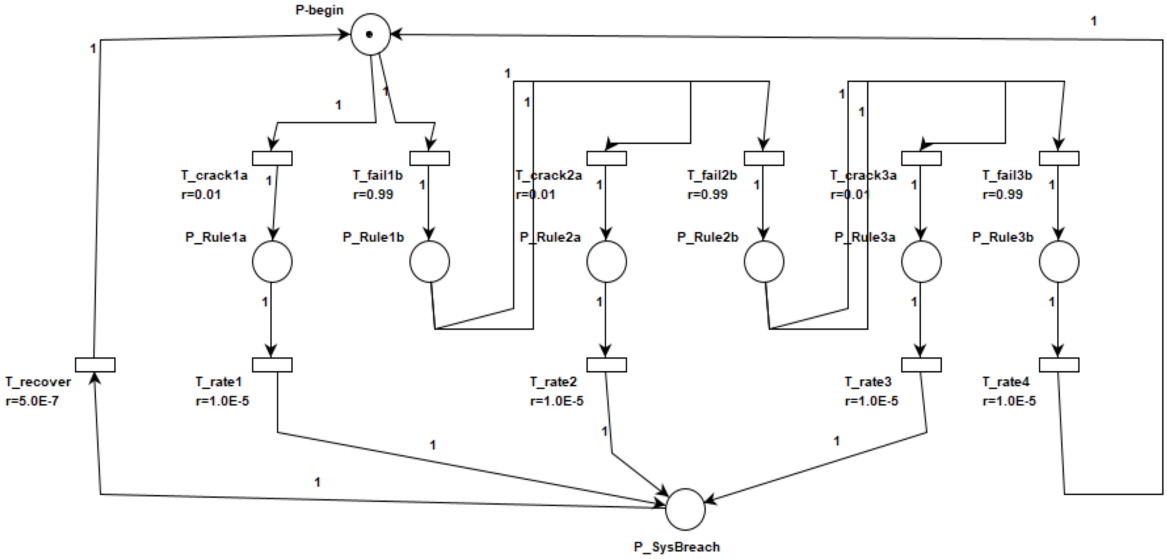

Figure 4. The SPN Model of Scenario I: Firewall model

Table 4. Reachable markings' set of the Firewall Model

	P_Begin	P_Rule1a	P_Rule1b	P_Rule2a	P_Ru1e2b	P_Rule3a	P_Rule3b
M0	1	0	0	0	0	0	0
M1	0	0	1	0	0	0	0
M2	0	1	0	0	0	0	0
M3	0	0	0	0	1	0	0
M4	0	0	0	1	0	0	0
M5	0	0	0	0	0	0	0
M6	0	0	0	0	0	0	1

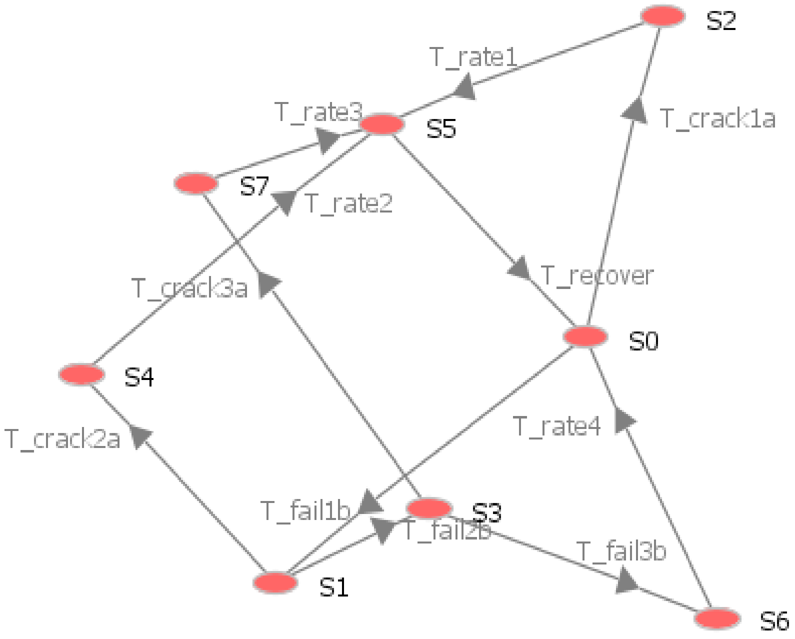

Figure 5. Reachability graph for firewall model

Starting from the initial marking shown (S0) in Fig. 5, a possible evolution of the GSPN state may be evaluated. As shown in Figure 4, and table 2 the places P0 to P7 represent the system states, and the transitions T0 to T10 represent the events that enable the transfer of the system state. Initially, the system is in a normal state. When the transition T_crack1a is enabled, the system transfers to the state P_Rule1a indicating that an intrusion attempt is in progress and rule number 1 is being circumvented. T_fail1b to T_fail3b indicates failed attempts to breach firewall results. A successful attack is achieved if any or all the transitions T_rate1, T_rate2, or T_rate3 are enabled. A system recovery is achieved through enabling transition Trecover, thereby enabling the initial marking P0 (in our case S0, since that's the default nomenclature in PIPE). According to the definition of the transition matrix and other performance metrics in [equation 1], we can estimate the SPN model as follows. The transition matrix Q is obtained by solving the Markov Chain equivalent of the reachability graph in figure 5. Q is thus, an 8 x 8 matrix presented in equation 9. Furthermore, we solve equation 2; by multiplying Q X vector π (π0, π1, π2, π3, π4, π5, π6, π7) to get the steady-state probability.

$$[Q =]\begin{bmatrix} 0 & \lambda b & \lambda a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda d & \lambda c & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda g & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda f & \lambda e \\ 0 & 0 & 0 & 0 & 0 & \lambda h & 0 & 0 \\ \lambda k & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda j & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda i & 0 & 0 \end{bmatrix} \quad (9)$$

Substitution the values for all rates (i.e. λa to λk) from table 3, and normalize the sum of each row to one. Applying equation 2 described in section 4.1; gives the steady-state probability P as:

P= π (π0, π1, π2, π3, π4, π5, π6, π7) x

$$[Q =]\begin{bmatrix} 0 & 0.99 & 0.01 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.99 & 0.01 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.99 & 0.01 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (10)$$

Steady-state probabilities as follows: π0 = 0, π1= 0, π2=

0.0049, π3 = 0, π4 = 0.0048, π5 = 0.95109, π6 = 0.0475, π7 = 0.00048.

4.3. The SPN Model of Scenario II: Password Model

a. The place, P0 denotes the initiation of the password cracking of local SCADA systems.
b. The place, P1 denotes the successful login.
c. The place, P2 denotes the failed login to the local SCADA.
d. The place, P3 denotes the knowledge discovered from the SCADA.
e. The place, P4 denotes the executed sequence of disruptive switching attacks from the SCADA.
f. The place, P5 denotes the failure to sequentially execute switches due to interlocking blocks.

Variables, T0, T1, T3, and T4 denote the transition probabilities of the successful login to the SCADA, of failure to login to the SCADA, of failing to execute, and of successful execution of the sequential switching in the targeted substation, respectively.

Variables, T2, T5, T6, and T7 denote the transition rates of learning to discover the cyber-physical relation, the response to attackers indicating the failed login, response to attackers about successful switching attacks, and response to attackers indicating the failure of the sequential switching due to interlock rules, respectively.

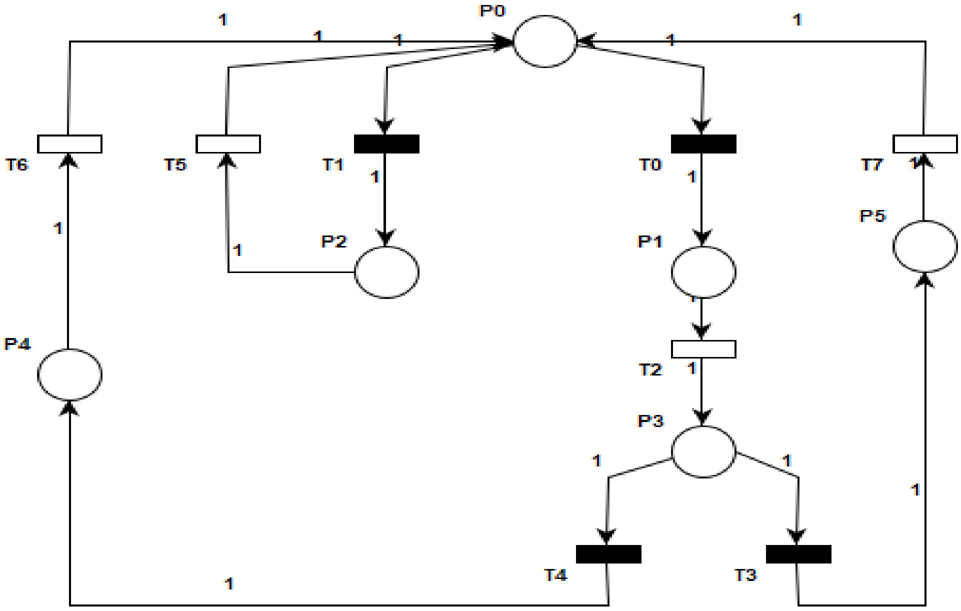

Figure 6. The SPN Model of Scenario II: Password Model [68]

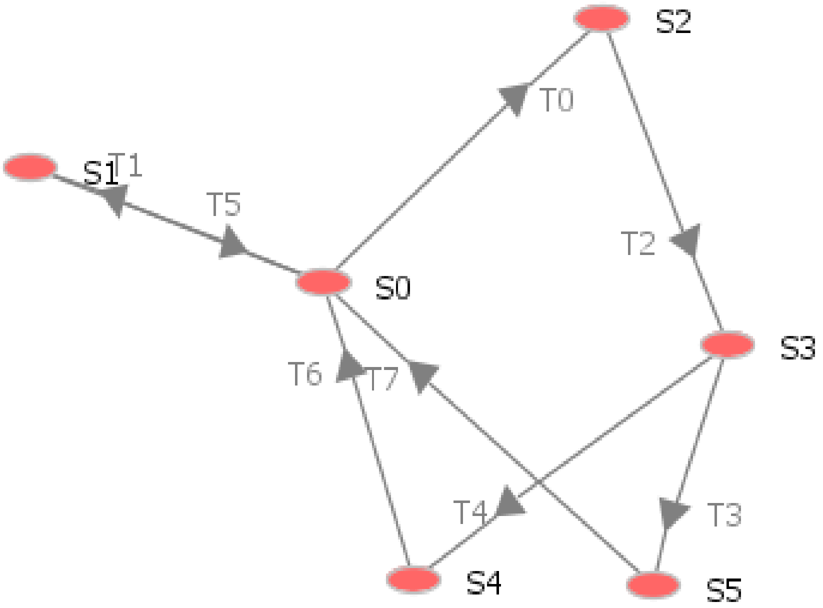

Figure 7. Reachability graph of Password Model

Table 5. Transitions descriptions and rates for Model II

Transition	Description	Rates
T0	Failure to crack password	λa (0.01)
T1	Successful cracking of password	λb (0.99)
T2	Successful login to SCADA	λc (0.0000001)
T3	Failure to execute an active attack	λd (0.9987)
T4	Success in executing sequential attack	λe (0.0013)
T5	Response to failed login	λf (0.00001)
T6	Response after successful attack	λg (0.0000005)
T7	Response to failed executing of sequential attack	λh (0.001)

Table 6. Reachability markings' set of the Firewall Model

	P0	P1	P2	P3	P4	P5
M0	1	0	0	0	0	0
M1	0	0	1	0	0	0
M2	0	1	0	0	0	0
M3	0	0	0	1	0	0
M4	0	0	0	0	1	0
M5	0	0	0	0	0	1

Using a similar argument as in Section 4.2, the steady-state probability, are derived as follows: π0 = 0.00001, π1 = 0.00966, π2 = 0.95592, π3 = 0.00001, π4 = 0.02485, π5 = 0.00955.

4.4. The SPN Model of Scenario III: Combined Firewall and Password Models within a Substation

The third scenario is modeled by combining the firewall and password models in sections 4.2 and 4.3. The description for transitions and places remains as defined in the preceding sections.

As from the previous arguments in 4.2 and 4.3, the reachability set and graph are obtained in figure 9 and table 7. Further, the steady-state probability is calculated.

Using similar argument as in Section 4.2, the steady-state probability and the rates in tables 3 and 5, are derived as follows:

π0 = 0, π1 = 0, π2 = 0.0022, π3 = 0, π4 = 0.00218, π5 = 0.00001, π6 = 0.21379, π7 = 0.00216, π8 = 0.64737, π9 = 0.13078, π10 = 0.00001, π11 = 0.00065, π12 = 0.00084.

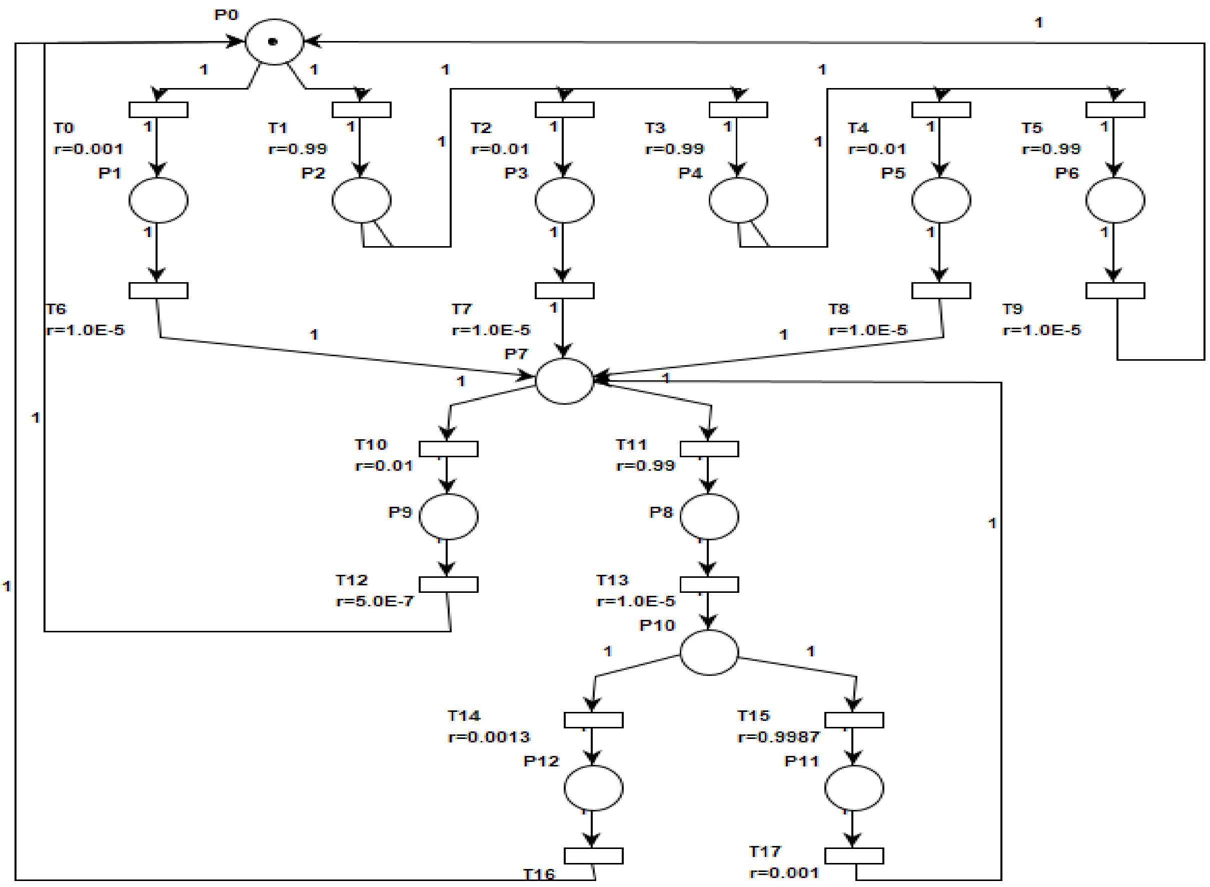

Figure 8. Scenario III: Combined Firewall and Password models

Table 7. Reachability Set for Scenario III

	P0	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**
M0	1	0	0	0	0	0	0	0	0	0	0	0	0
M1	0	0	1	0	0	0	0	0	0	0	0	0	0
M2	0	1	0	0	0	0	0	0	0	0	0	0	0
M3	0	0	0	0	1	0	0	0	0	0	0	0	0
M4	0	0	0	1	0	0	0	0	0	0	0	0	0
M5	0	0	0	0	0	0	0	1	0	0	0	0	0
M6	0	0	0	0	0	0	1	0	0	0	0	0	0
M7	0	0	0	0	0	1	0	0	0	0	0	0	0
M8	0	0	0	0	0	0	0	0	1	0	0	0	0
M9	0	0	0	0	0	0	0	0	0	1	0	0	0
M10	0	0	0	0	0	0	0	0	0	0	1	0	0
M11	0	0	0	0	0	0	0	0	0	0	0	1	0
M12	0	0	0	0	0	0	0	0	0	0	0	0	1

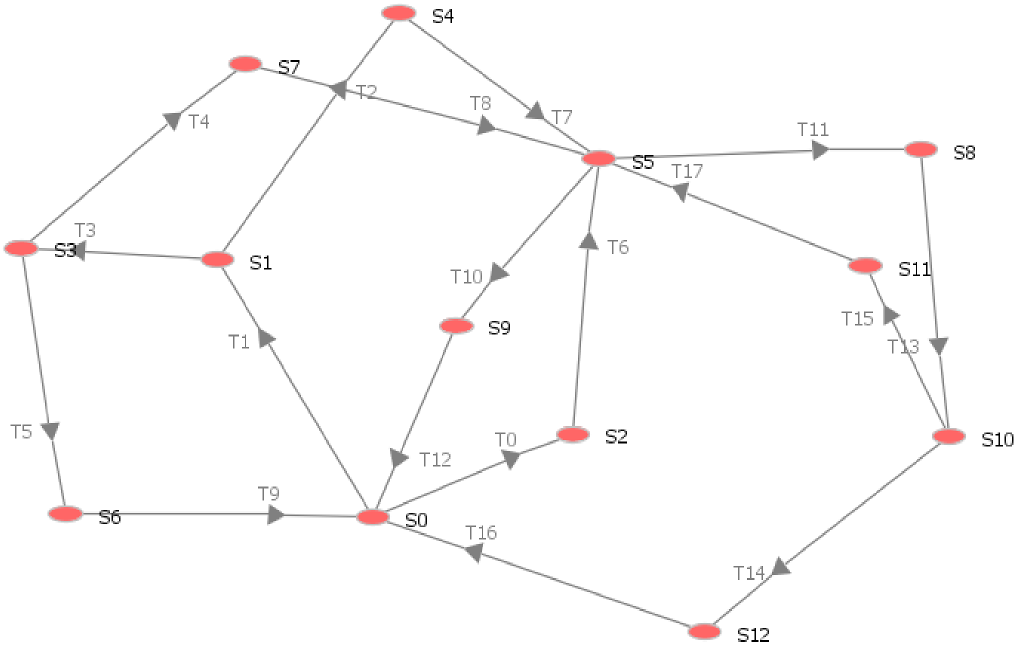

Figure 9. Reachability graph of Scenario III

5. Numerical Results and Analyses

We used PIPE (Platform-Independent Petri Net Editor) [61] and Great Stochastic Petri nets [62] to model and analyze the GSPN attack model of the SCADA network. Both tools are open-source tools that support creating and analyzing Petri Nets. They have an easy-to-use graphical user interface that allows a user to create standard Petri Net and Stochastic Petri Net models. It also allows a user to animate the model with the random firing of transitions or interactive user manipulations. The analysis environment in these tools includes different modules such as steady-state analysis, steady space analysis, and GSPN analysis [62].

First, we implemented the DoS model in PIPE as shown in Figures 4, 6, and 8. Next, we assigned a weight to each of the transitions as shown in Table 3 and 4.

The designed GSPN model of the DoS attack was simulated fifty times using a different number of initial random firings: 100, 300, 500, 700, 1000, and 1200. The variation of the token distribution with the same number of initial random firings is recorded.

5.1. Simulation Results

The transition triggering rates of the Défense Scenario's I, II, and III SPN models are shown in Table 8 below.

Firstly, we obtain the transition triggering rate (shown in Table 8). Then, we conduct the simulations, we can get the reachable markings' set as shown in figures 5, 7, and 9 of the three scenarios respectively. results of which are illustrated in Table 8, Table 9, and Figure 14.

We obtain the steady-state probability for further performance evaluation as illustrated in Table 9 below.

Table 8. Summary Transition Rates

Model	λa	λb	λc	λd	λe	λf	λg	λh	λi	λj	λk	λl	λm	λn	λo	λp	λq	λr
I	0.01	0.99	0.01	0.99	0.01	0.99	1E-5	1E-5	1E-5	1E-5	0.5E-7	-	-	-	-	-	-	
II	0.01	0.99	1E-5	0.9987	0.0013	1E-6	0.5E-7	0.02	-	-	-	-	-	-	-	-	-	
III	0.01	0.99	0.01	0.99	0.01	0.99	1E-6	1E-6	1E-6	1E-6	0.01	0.99	0.5E-7	1E-6	0.00130	0.9987	1E-5	0.01

Table 9. Steady-state probabilities for all scenarios

Model	π0	π1	π2	π3	π4	π5	π6	π7	π8	π9	π10	π11	π12
I	0	0	0.0049	0	0.0048	0.95109	0.0475	0.00048	-	-	-	-	-
II	0.00001	0.0097	0.95592	0.00001	0.02485	0.00955	-	-	-	-	-	-	-
III	0	0	0.0004	0	0.00043	0.00001	0.04176	0.00042	0.78902	0.1594	0.00001	0.00788	0.00103

5.2. Performance Comparison

With the data, we get from the above simulations and the equations of the three scenarios in Section 4, we can figure out the system breach probability (Psysbreach), failure rate to crack the password, and several parameters. Scenario I target state is Psystem breach which is achieved by circumventing any or all of the three firewall rules. The number of successful attempts to open a port relative to the total attempts to open the port is based on operating system event logs, while response times are based on specification of server performance and security events logs of servers. In our case, a 10 percent for success rate and a 90 percent fail rate were applied. Cybersecurity audits or vulnerability assessments are not frequently conducted in Industrial Control Systems (ICS/SCADA) as compared to the IT infrastructures due to availability issues.

By analyzing the data in Table 9, we can see that with the probability of breaching the system in the scenario I was 0.48% and after adding the password mechanism, the security probability of the system and the defense level are both increasing gradually. The probability of the system being intruded when secured by the password was assumed at 1% and this resulted in a steady-state probability of system attack of 2.485%. Indicating that a password is not an ideal defense mechanism to secure a SCADA system.

6. Future Scope and Conclusions

In this paper, we focused on the performance analysis of the SCADA firewall and password as implemented intrusion detection and prevention mechanisms in the case setting. Firstly, we proposed three system defense scenarios and constructed performance evaluation models based on stochastic Petri nets. Then, we theoretically analyzed the proposed three SPN models. After that, we conducted extensive simulations on the PIPE [61] platform, the results of which illustrate the effectiveness in security enhancement of the SCADA Simulation (SCADASim) under the proposed SPN models.

This paper provides a novel framework to evaluate the performance of the SCADA systems in Smartgrid and critical infrastructure in Zambia. In some information fields with higher requirements of confidentiality, such as the army combat command system, government office network, large enterprise servers, etc., we can decide whether to choose a honeypot to strengthen the defense and protection of the system according to the actual needs and then estimate the system safety probability, defense success probability, etc. The work can guide further cybersecurity deployment and improve the comprehensive protective performance of the system. In future work, we will model the SCADA from a power station to the control to determine the impact of cyber attacks launched from the public network. Furthermore, we shall use combinatorial techniques, i.e., GSPN and Bayesian networks, to model the security and dependability issues of control systems in ICS.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. Simon Tembo, Assistant Dean - Technical, Department of Electrical & Electronic Engineering, School of Engineering at the University of Zambia, Special thanks also go to my wife Edna, my sons, Dad, Mum in memory, my siblings, and my friends. I love you guys. May God Continue Blessing you!

REFERENCES

[1] Awad, A.; Bazan, P.; German, R. SGsim: A simulation framework for smart grid applications. In Proceedings of the 2014 IEEE International Energy Conference (ENERGYCON), Cavtat, Croatia, 13–16 May 2014; pp. 730–736.

[2] Al Ghazo, Alaa, "A framework for Cybersecurity of Supervisory Control and Data Acquisition (SCADA) Systems and Industrial Control Systems (ICS)" (2020). Graduate Theses and Dissertations. 17834.

[3] Davis, K. R., Davis, C. M., Zonouz, S. A., Bobba, R. B., Berthier, R., Garcia, L., et al. (2015). A cyber-physical modeling and assessment framework for power grid infrastructures. IEEE Trans. Smart Grid 6, 2464–2475. doi:10.1109/tsg.2015.2424155.

[4] Handa, A., Sharma, A., and Shukla, S. K. (2019). Machine learning in cybersecurity: a review. WIREs Data Mining Knowl Discov. 9, e1306. doi:10.1002/widm.1306.

[5] Johnson, J., Onunkwo, I., Cordeiro, P., Wright, B.J., Jacobs, N. and Lai, C. (2020), Assessing DER network cybersecurity defenses in a power-communication co-simulation environment. IET Cyber-Physical Systems: Theory & Applications, 5: 274-282. https://doi.org/10.1049/iet-cps.2019.0084.

[6] Li, Beibei & Xiao, Gaoxi & Lu, Rongxing & Deng, Ruilong & Bao, Haiyong. (2019). On Feasibility and Limitations of Detecting False Data Injection Attacks on Power Grid State Estimation Using D-FACTS Devices. IEEE Transactions on Industrial Informatics. PP. 10.1109/TII.2019.2922215.

[7] Hans de Bruijn, Marijn Janssen. Building Cybersecurity Awareness: The need for evidence-based framing strategies, Government Information Quarterly, Volume 34, Issue 1, 2017, Pages 1-7.

[8] Coffey K. et al. (2018) Vulnerability Assessment of Cyber Security for SCADA Systems. In: Parkinson S., Crampton A., Hill R. (eds) Guide to Vulnerability Analysis for Computer Networks and Systems. Computer Communications and Networks. Springer, Cham. https://doi.org/10.1007/978-3-319-92624-7_3.

[9] Hong, Jin & Enoch, Simon & Kim, Dan & Nhlabatsi, Armstrong & Fetais, Noora & Khan, Khaled. (2018). Dynamic Security Metrics for Measuring the Effectiveness of Moving Target Defense Techniques. Computers & Security. 79. 10.1016/j.cose.2018.08.003.

[10] Häckel, Björn & Niesel, Oliver & Bogenreuther, Maximilian & Berger, Stephan. (2019). Modeling Availability Risks of IT Threats in Smart Factory Networks - A Modular Petri Net Approach.

[11] Razzaq M, Ahmad J (2015) Petri Net and Probabilistic Model Checking Based Approach for the Modelling, Simulation, and Verification of Internet Worm Propagation. PLoS ONE 10(12): e0145690. https://doi.org/10.1371/journal.pone.0145690.

[12] T. M. Chen, J. C. Sanchez-Aarnoutse and J. Buford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid," in IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 741-749, Dec. 2011, doi: 10.1109/TSG.2011.2160000.

[13] K. Labadi, A.-M. Darcherif, I. El Abbassi and S. Hamaci (2020) Petri Net-Based Approach for “Cyber” Risks Modelling and Analysis for Industrial Systems E3S Web Conf., 170 02001 DOI: https://doi.org/10.1051/e3sconf/202017002001.

[14] Beibei Li, Rongxing Lu, Kim-Kwang Raymond Choo, WeiWang, and Sheng Luo (2018) On Reliability Analysis of Smart Grids under Topology Attacks: A Stochastic Petri Net Approach.

[15] Mahmoudi-Nasr, Payam. (2018). Petri Net Model of Insider Attacks in SCADA System.

[16] Markiewicz, Michał & Gniewek, Lesław. (2017). A Program Model of Fuzzy Interpreted Petri Net to Control Discrete Event Systems. Applied Sciences (Switzerland). 7. 10.3390/app7040422.

[17] Radoglou Grammatikis, Panagiotis & Sarigiannidis, Panagiotis & Giannoulakis, Ioannis & Kafetzakis, Emmanouil & Panaousis, Emmanouil. (2019). Attacking IEC-60870-5-104 SCADA Systems. 10.1109/SERVICES.2019.00022.

[18] Jasiul, B.; Szpyrka, M.; Śliwa, J. Detection and Modeling of Cyber Attacks with Petri Nets. Entropy 2014, 16, 6602-6623. https://doi.org/10.3390/e16126602.

[19] K. Yamashita, C.-W. Ten, Y. Rho, L. Wang, W. Wei, and A. F. Ginter, (2020) Measuring systemic risk of switching attacks based on cybersecurity technologies in substations,” IEEE Trans. Power Syst., vol. 35, no. 6, pp. 4206–4219, Nov. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9078877.

[20] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, Cyber-physical security and dependability analysis of digital control systems in nuclear power plants,” IEEE Trans. Syst., Man, Cybern., vol. 46, no. 3, pp. 356–369, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7192645.

[21] Henry, M.H., Layer, R.M., Snow, K.Z., & Zaret, D.R. (2009). Evaluating the risk of cyber attacks on SCADA systems via Petri net analysis with application to hazardous liquid loading operations. 2009 IEEE Conference on Technologies for Homeland Security, 607-614.

[22] Zeng, R., Jiang, Y., Lin, C., & Shen, X. (2012). Dependability Analysis of Control Center Networks in Smart Grid Using Stochastic Petri Nets. IEEE Transactions on Parallel and Distributed Systems, 23, 1721-1730.

[23] Kundur, Deepa & Feng, Xianyong & Liu, Shan & Zourntos, Takis & Butler-Purry, K.L.. (2010). Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. 244 - 249. 10.1109/SMARTGRID.2010.5622049.

[24] Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., & Butler-Purry, K.L. (2012). A smart grid vulnerability analysis framework for coordinated variable structure switching attacks. 2012 IEEE Power and Energy Society General Meeting, 1-6.,

[25] E. E. Miciolino, G. Bernieri, F. Pascucci, and R. Setola, "Communications network analysis in a SCADA system testbed under cyber-attacks," 2015 23rd Telecommunications Forum Telfor (TELFOR), 2015, pp. 341-344, doi: 10.1109/TELFOR.2015.7377479.

[26] Liberati, Francesco, Emanuele Garone, and Alessandro Di Giorgio. 2021. "Review of Cyber-Physical Attacks in Smart Grids: A System-Theoretic Perspective" Electronics 10, no. 10: 1153. https://doi.org/10.3390/electronics10101153

[27] Geeta Yadav, Kolin Paul, Architecture and security of SCADA systems: A review, International Journal of Critical Infrastructure Protection, Volume 34, 2021, 100433, ISSN 1874 5482, https://doi.org/10.1016/j.ijcip.2021.100433. (https://www.sciencedirect.com/science/article/pii/S1874548221000251).

[28] Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. Energies 2021, 14, 5894. https://doi.org/10.3390/en14185894.

[29] Pillitteri, V.; Brewer, T. Guidelines for Smart Grid Cybersecurity, 2014-09-25; NIST Interagency/Internal Report (NISTIR); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.

[30] Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Li, J. A denial of service attack in advanced metering infrastructure network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 1029–1034.

[31] Bari, A.; Jiang, J.; Saad,W.; Arunita, J. Challenges in the Smart Grid Applications: An Overview. Int. J. Distrib. Sens. Netw. 2014, 1–11.

[32] Gauci, A.; Michelin, S.; Salles, M. Addressing the challenge of cyber security maintenance through patch management. CIREDOpen Access Proc. J. 2017, 2017, 2599–2601.

[33] Khalid, A.; Sundararajan, A.; Hernandez, A.; Sarwat, A. FACTS Approach to Address Cybersecurity Issues in Electric Vehicle Battery Systems. In Proceedings of the 2019 IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA, 12–14 June 2019.

[34] Agarkar, A.; Agrawal, H. A review and vision on authentication and privacy preservation schemes in the smart grid network. Secur. Priv. 2019, 2, e62. [CrossRef]

[35] Zhang, F.; Mahler, M.; Li, Q. Flooding attacks against secure time-critical communications in the power grid. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 449–454. [CrossRef]

[36] Huseinovic, A.; Mrdovic, S.; Bicakci, K.; Uludag, S. A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; pp. 1–4.

[37] Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.

[38] Huseinovi´c, A.; Mrdovi´c, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. IEEE Access 2020, 8, 177447–177470.

[39] Cameron, C.; Patsios, C.; Taylor, P.C.; Pourmirza, Z. Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of- Service Attacks on Voltage Control Schemes. IEEE Trans. Smart Grid 2019, 10, 3010–3019.

[40] Kurt, M.N.; Yilmaz, Y.; Wang, X. Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. IEEE Trans. Inf. Forensics Secur. 2019, 14, 498–513.

[41] Chatfield, B.; Haddad, R.J.; Chen, L. Low-Computational Complexity Intrusion Detection System for Jamming Attacks in Smart Grids. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 367–371.

[42] Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. IEEE Trans. Smart Grid 2017, 8, 2431–2439.

[43] Ying, H.; Zhang, Y.; Han, L.; Cheng, Y.; Li, J.; Ji, X.; Xu, W. Detecting Buffer-Overflow Vulnerabilities in Smart Grid Devices via Automatic Static Analysis. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 813–817.

[44] He, Y.; Mendis, G.J.; Wei, J. Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. IEEE Trans. Smart Grid 2017, 8, 2505–2516.

[45] Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. J. Netw. Comput. Appl. 2020, 170, 102808.

[46] Deng, R.; Liang, H. False Data Injection Attacks With Limited Susceptance Information and New Countermeasures in Smart Grid. IEEE Trans. Ind. Inform. 2019, 15, 1619–1628.

[47] Riggs, H.; Tufail, S.; Khan, M.; Parvez, I.; Sarwat, A.I. Detection of False Data Injection of PV Production. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 7–9 April 2021; pp. 7–12.

[48] Singh, V.K.; Ebrahem, H.; Govindarasu, M. Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment. In Proceedings of the 2018 North American Power Symposium (NAPS), Fargo, ND, USA, 9–11 September 2018; pp. 1–6.

[49] Green, B.; Prince, D.; Busby, J.; Hutchison, D. The Impact of Social Engineering on Industrial Control System Security. In Proceedings of the First ACMWorkshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC ’15, Denver, CO, USA, 16 October 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 23–29.

[50] Mrabet, Z.E.; Kaabouch, N.; Ghazi, H.E.; Ghazi, H.E. Cyber-security in smart grid: Survey and challenges. Comput. Electr. Eng. 2018, 67, 469–482.

[51] Pour, M.M.; Anzalchi, A.; Sarwat, A. A review on cyber security issues and mitigation methods in smart grid systems. In Proceedings of the SoutheastCon 2017, Concord, NC, USA, 30 March–2 April 2017; pp. 1–4.

[52] Rajendran, G.; Sathyabalu, H.V.; Sachi, M.; Devarajan, V. Cyber Security in Smart Grid: Challenges and Solutions. In Proceedings of the 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 21–23 August 2019; pp. 546–551.

[53] Shitharth, S.; Winston, D.P. A novel IDS technique to detect DDoS and sniffers in smart grid. In Proceedings of the 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016; pp. 1–6.

[54] Pandey, R.K.; Misra, M. Cyber security threats—Smart grid infrastructure. In Proceedings of the 2016 National Power Systems Conference (NPSC), Bhubaneswar, India, 19–21 December 2016; pp. 1–6.

[55] Wang, X.; Shi, D.; Wang, J.; Yu, Z.; Wang, Z. Online Identification and Data Recovery for PMU Data Manipulation Attack. IEEE Trans. Smart Grid 2019, 10, 5889–5898.

[56] Wang, J.; Shi, D.; Li, Y.; Chen, J.; Ding, H.; Duan, X. Distributed Framework for Detecting PMU Data Manipulation Attacks With Deep Autoencoders. IEEE Trans.

Smart Grid 2019, 10, 4401–4410.

[57] Irita, T.; Namerikawa, T. Detection of replay attack on smart grid with code signal and bargaining game. In Proceedings of the 2017 American Control Conference (ACC), Seattle, WA, USA, 24–26 May 2017; pp. 2112–2117.

[58] Alohali, B.; Kifayat, K.; Shi, Q.; Hurst, W. Replay Attack Impact on Advanced Metering Infrastructure (AMI). In Smart Grid Inspired Future Technologies; Hu, J., Leung, V.C.M., Yang, K., Zhang, Y., Gao, J., Yang, S., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 52–59.

[59] The Essential Role of Cyber Security in the Smart Grid. Available online: https://electricenergyonline.com/energy/magazine/312/article/The-Essential-Role-of-Cyber-Security-in-the-Smart-Grid-.htm (accessed on 30 July 2021).

[60] Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. J. Inf. Secur. Appl. 2020, 50, 102419.

[61] https://github.com/sarahtattersall/PIPE

[62] http://www.di.unito.it/~greatspn/index.html

[63] F. Bause and P. S. Kritzinger, Stochastic Petri Nets: An Introduction to the Theory, 2nd ed. Braunschweig, Germany: Vieweg, 2002.

[64] K. Yamashita, C.-W. Ten, Y. Rho, L. Wang, W. Wei, and A. F. Ginter, "Measuring systemic risk of switching attacks based on cybersecurity technologies in substations," IEEE Trans. Power Syst., vol. 35, no. 6, pp. 4206–4219, Nov. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9078877.

Copyright © 2022 The Author(s). Published by Scientific & Academic Publishing
This work is licensed under the Creative Commons Attribution International License (CC BY). http://creativecommons.org/licenses/by/4.0/