Providing a Model for a Cyber-Attack to a Special Protection Scheme Based on Timed Petri Net

Mohammad Amin Hojjati Kermani[1,*], Masoud Aliakbar Golkar[1] and Sadaan Zokaei[2]

[1] Faculty of electrical engineering, K.N.Toosi university of technology, Tehran, Iran
[2] Faculty of computer engineering, K.N.Toosi university of technology, Tehran, Iran
**Corresponding author: mhojjati@mail.kntu.ac.ir*

Manuscript received 11 October, 2018; Revised 13 January, 2019; accepted 25 January, 2019. Paper no. JEMT-1801-1131.

In order to enhance the reliability of the power transmission grid, planning and employing regional protection along with traditional local protection is necessary. Both regional and wide area protection is contingent upon communication and data networking infrastructure and hence prone to cyber-attacks. Moreover, since this kind of protection maintains network integrity while taking into account the specified combinatorial parameters; its output is not necessarily consistent with the output of local protection mechanisms. In other words, applying regional protection alters the arrangement of the whole network for maintaining the interests of all consumers. On the contrary, the local manager of transmission or distribution network may find this in conflict with his/her interests and may even take actions against it via cyber-attacks. The primary step to analyze these 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 the present study, a multi-stage attack has been extracted and modeled with a timed Petri net, and then the results are compared with those of similar articles.

Keywords: *Cyber Attack, Special Protection Scheme, Timed Petri net.*

http://dx.doi.org/10.22109/jemt.2019.151970.1131

Nomenclature

SPS	Special Protection Scheme.
PMU	Phasor Measurement Unit
NERC	North American Electric Reliability Corporation
CCA	Command Cloning Attack
DoS	Denial of Service
FDI	False data injection
SPS	Special Protection Scheme.
PMU	Phasor Measurement Unit
NERC	North American Electric Reliability Corporation
CCA	Command Cloning Attack
DoS	Denial of Service
FDI	False data injection
SPS	Special Protection Scheme.
PMU	Phasor Measurement Unit
NERC	North American Electric Reliability Corporation
CCA	Command Cloning Attack
DoS	Denial of Service

1. Introduction

Over the past decade, power systems have encountered numerous disturbances causing widespread outages. For instance, in August 2003 a blackout in the northwest of the United States caused a loss of 50 GW of electricity. This outage caused 50 million consumers to suffer from the lack of power. Moreover, another major disturbance disrupted the electricity service of millions of consumers in July and August 1996. Such events typically occur when the system is loaded heavily, and several components of the system go out of service within a short period. This may cause the voltage drop and the rotor angle instability [1]. Similar events have occurred in Iran which, the most important of them occurred in May 20, 2001 at 12 pm; based on the references [2] and [3], this outage was instigated with a fault on the 400 KV lines of the Neka power plant to Tehran which was out of service due to scheduled inspections and tests at that time. Prior to the initiation of the fault, 550 MW of power was dispatched from Neka to Ahuwan. After this line tripping, because of protection relay commands, power flow share of this tripped transmission line fell on to other lines. For instance, the power transmission of the “Hassan Kif” line increased from 390 to 750 MW and the subsequent increase in the loading limit of the “Qaem” to “Kalan” line, caused separation of the northern region and Tehran region. Following the operation of the protection relays, two islands formed in the grid. Imbalance in generation and consumption resulted in generation surplus and overload on the northern and southern island, respectively (Figure 1-1). Followed by this event, the failure of several switches resulted in the outage of a large part of the grid. Another event causing a major outage in Iran took place on February 20, 2004, due to a single-phase-to-ground fault at the 230 KV transmission line between the “Anjirak” and “Arak” substations. The distance protection relay at Anijark -the adjacent substation to the fault- was unable to detect and remove the fault, and eventually, the switch exploded after 56 cycles. After this incident, it was observed that the 230 KV busbar did not have proper protection and the fault removal was delegated to other areas. In this event, since the local protection failed to clear the fault, backup protection in neighboring substations came into action, which finally caused widespread outages [3].

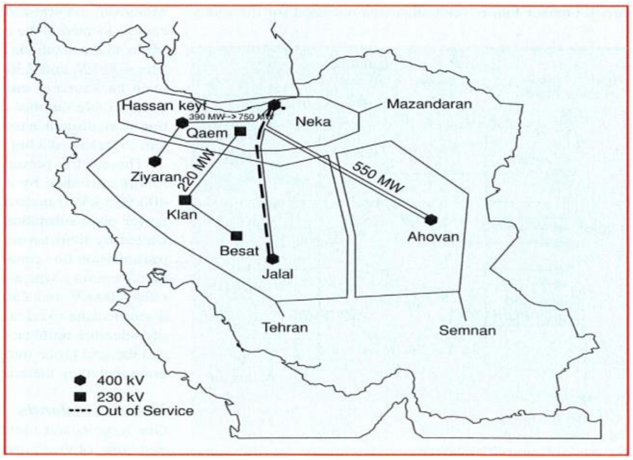


Fig. 1. Boundary between uncontrolled islands in power system of Iran [2]

Putting scrutiny on such events clarifies the significance of applying regional protection in power systems. Damages caused by simultaneous events or inadequacy of the local protection could be minimized through employing multi-parameter wide area protection. Dependency of wide area protection to data communication links makes it prone to cyber-attacks. Acquiring more revenue through power continuity or malicious intentions can be considered as motivations to a cyber-attack on a particular protection system in the power transmission network. Special measures should be carried out to cope with such attacks. These attacks usually take place by manipulating the data in the protection system or by creating a delay in the path of system commands. Making corrupt commands under such attacks not only does not increase the integrity in power grid but also makes more extensive outages and lowers the resilience in the power grid. Therefore, the security of this kind of protection scheme is of great importance.

This paper presented a new:

- Adjustable multistage cyber-physical attack to the power transmission network
- Model of an SPS considering determined cyber attacks

The remaining of the paper is organized as follows: In Section 2, a survey on similar topics in the literature has been made. Section 3 introduces the special protection scheme (SPS). The impact of the cyber-attacks against SPS is examined in this Section. To quantify this impact, Petri net is introduced and used as a means of modeling cyber-attacks in section 3. In addition, a special protection model for generation rejection is also defined for the standard 9-bus network. In Section 4, the simulation results are presented on the basis of the proposed model by making changes in attack parameters and comparison of impacts of the different attack types. In the final section, the paper is concluded by a summary of the achievements.

2. Related works

In advance, a quick review of what researchers have done under similar topics is made. Several articles have included cyber-attacks in their model. For example, in [4], a relatively large power network and its related cyber-infrastructure have been considered for attack analysis. Therefore, the details of the attack parameters have been neglected and only the ultimate probability of success based on the attack tree structure (Figure 2) and the ICS-CIRT statistical reports have been considered as discrete numbers.

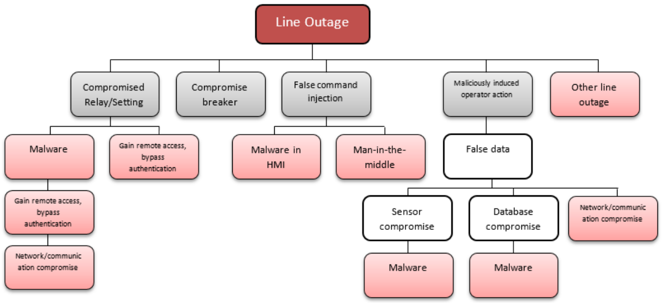

Line Outage
Compromised Relay/Setting
Compromise breaker
False command injection
Maliciously induced operator action
Other line outage
Malware
Gain remote access, bypass authentication
Malware in HMI
Man-in-the-middle
False data
Gain remote access, bypass authentication
Network/communication compromise
Sensor compromise
Database compromise
Network/communication compromise
Malware
Malware

Fig. 2. Attack tree to calculate the probability of line exit [4]

Additionally, in reference [5] the Petri net is also used to model the attack to the supervisory control and data acquisition (SCADA) system infrastructure. The difference between modeling in this reference and the modeling presented in our study is that the modeled attack in [5] is related to the behavior of an attacker inside the system -like the operator of the control center coping with the alarms received from the system. On the other hand, the behavior of an external attacker has also been modeled in the presented study.

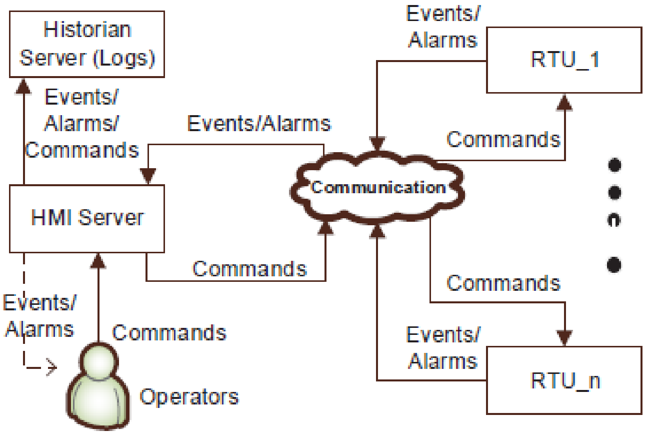


Fig. 3. Internal attacker model in the supervisory control and data acquisition (SCADA) system [5]

In [6], the authors devised a dynamic model of a generation station and attempted to apply a False Data Injection (FDI) attack to sensor readings in that system. Since separated detailed modeling of each power system component and combining them together in a unified platform needs a wide range of cumbersome activities, this method has limited applicability. By using the attack tree model in [7], vulnerability indices have been introduced to evaluate cyber-security state of the power system control, which needs an enumeration of all possible vulnerabilities by using experts' knowledge in each part. In [8] a model-based approach has been introduced for power system with attacks on it. As in [5], detailed system model is needed to reach valid results. Attack scenarios on multiple line outages has been studied in [9]. In the analysis, the worst case attack has been identified with respect to the time of occurrence: sequential or simultaneous. This analysis is useful to form an SPS protection scheme in our model. In [10] a different approach has been used in Petri net modeling by proposing a two-layer modeling. High level and low-level Petri nets have been introduced without a clear way to implement it. A Markov decision process method has been applied in [17] to evaluate possible attacks resulting in opening a circuit breaker in a sample substation. Combination of the attack tree graph and probability model brings about benefits but validating with realistic data rises major problems. In [12] DoS/DDoS cyber-attack is simulated on advanced metering infrastructure (AMI). Under the TCP, UDP and ICMP protocols, multiple traffic flows have been generated and attack scenarios have been applied. A number of packets, which can be delivered to the destination, are counted for a specified smart grid service and the impacts of the applied attacks are evaluated. This analysis is for defined protocols and cannot be generalized in broader applications. As in [7] attack tree model is used in [13] but in an AMI system. One can use this model to propose an attack prevention mechanism, but it is not applicable in analyzing the consequences.

Our proposed method has been extended in both cyber and physical aspect of a power system to model the transition of the system from one state to another after applying a cyber-attack. Multiple attacks with adjustable parameters have been introduced which is a vital feature in analyzing attack consequences. Also, it is extendable in other scenarios with changing the graph-like architecture of places, transitions, and arc parameters.

3. SPS in power grid

After the widespread use of PMUs along with the development of telecommunication network equipment, protection operations have been developed beyond local measurements to wide-area operations in order to cope with disturbances in the large-scale power grids. For implementing regional protection, the information of a vast geographic area is used to deal with large disturbances, which may cause extensive instability and power outage in the power system. The SPS is the most common type of wide-area protection scheme.

NERC defines a special protection model as an automatic protection system designed to detect abnormal predetermined system conditions and enforce necessary actions. The pure separation of disrupted components of the power grid is not included in this definition [14]. Figure 4 demonstrates a general schematic of the SPS function.

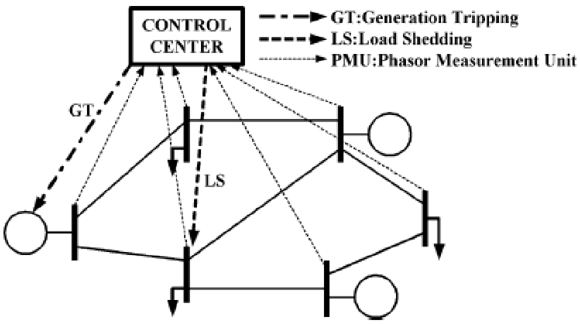


Fig. 4. General function of SPS based on PMUs [14]

Special protection operations may include variation in demand, adjustments in generation (MW and MVAR), or system configuration to maintain the frequency or power flow within a predefined range through voltage control. Generation rejection, under-frequency load shedding, under voltage load shedding, out of synchronism protection, and targeted islanding are among primary applications of the SPS.

Figure 5 depicts a sample SPS implementation to eliminate generation. The operator of the control center considering the conditions of the transmission network and the observed alarms provides the arming signal in this Figure.

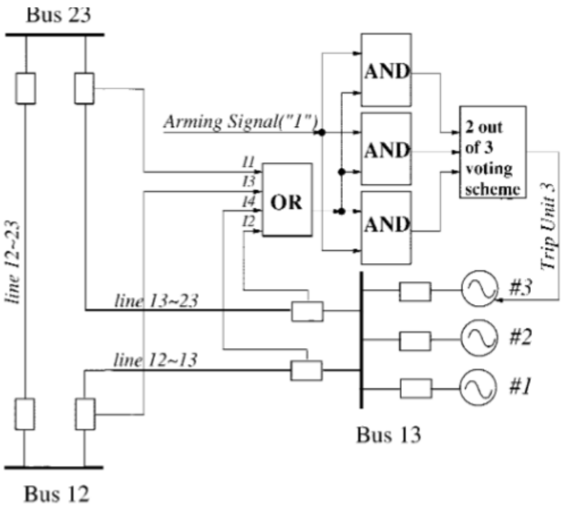


Fig. 5. Implementation of SPS in generation rejection [15]

3.1. Sensitivity of SPS to cyber-attacks

The decision-making outcomes in regional protection have to ensure the accuracy in the process of receiving data, processing them, and sending the control system decisions to the desired devices in the power grid. Since this protection covers a wider range compared to the local protection, validating its accurate performance is of great importance. Therefore, it is necessary to examine this type of protection in the modeling and simulation phases in different scenarios under cyber-attacks before the widespread exploitation of this technique in smart power grids.

Moreover, it is necessary to determine the interaction of cyber and physical parts in the power grid along with taking measures for including the cyber-attack to this model. In the following, the approach intended to connect these two regions and modeling different testing scenarios have been described.

3.2. Use of colored Petri net model

The colored Petri net is a developed Petri net designed to model concurrent systems with synchronous and asynchronous communications. This method is formulated based on bag theory and has a simple graphical interface. Implementation of the model can be observed with a graphical and simple appearance and is based on the algebraic rules of the colored Petri net. Colored Petri net uses the artificial intelligence language ML, which is an official language based on the Lambda calculus [16]. The ML language is utilized for modeling and analyzing the state space of the system. Adding this language to the Petri net, while maintaining its formality, has drastically increased the modeling power of this kind of network. Hierarchical modeling allows for model abstraction in different semantic levels and simplifies the modeling process of the system. A hierarchical CPN tool[1] is a suitable tool for modeling and analyzing the state space of the system.

[1] http://cpntools.org/

3.2.1. Petri net structure

Petri net structure is defined by places, transitions, and input-output functions. A Petri network consists of four components C = (P, I, T, O):

- Set of places P = {P1, P2, ..., Pn}, n≥0
- Set of transitions T = {t1, t2, ..., tm} m≥0
- Input function I: I = T → P is a mapping of transitions to the set of places
- Output function O: O = P → T is a mapping from the set of places to the transitions

The I/O functions are the communication bridges between the transitions (T) and places (P). $P \cap T = \phi$ is the set of separate places and transitions. Each Petri net acts using four elements of transition, arcs, places, and tokens.

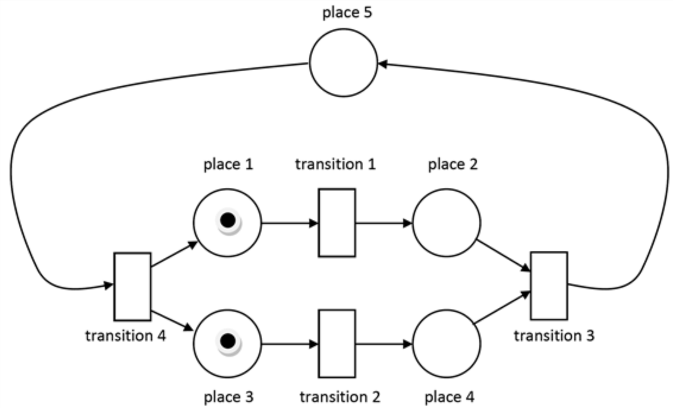


Fig. 6. Petri net components [17]

A CPN model is defined by a nine-element set CPN = (P, T, A, Σ, V, C, G, E, I0), where P = {p1, p2, p3, ..., pm} is a finite set of network places displayed with circles in Figure 6, T is the finite set of network transitions T = {t1, t2, t3, ..., tn}. A is a set of arcs defined from places to transitions, or vice versa $A \subseteq (T \rightarrow P)$ U $(P \rightarrow T)$, Σ is a nonempty set with a set of variables called color-set. V is a set of variables with the type defined in Σ. C is a function specifying color-set to each place as $C : \Sigma \rightarrow P$. G is a guard function on transition determining a condition for each transition t, $Type\ (G\ (t\ )) = Boolean$. E is related to the arc, which finally attributes a color-set to each arc with the color-set set type corresponding to the place attached to that arc: $Type\ (E\ (a)) = C\ (p)$; and finally, I0 is the function of the initial values for the places $Type\ (I_0(p)) = C(p)$.

Transitions and transfer arcs can take advantage of conditional expressions to control the progress of tokens. A token is the fundamental element of a Petri Net's marking. A transition is activated only when there are sufficient tokens for all input places, which satisfy the expressions of the input transmission arcs and the expression of the transition itself. There are two kinds of transitions: real-time transition and timed transition, the former shown with a solid bar and the latter with a hollow bar.

3.3. Definition of an SPS model under cyber-attack

A Western System Coordinating Council (WSCC) 9-bus model is considered for modeling the cyber-attack in the SPS infrastructure. Figure 7 illustrates this system, and the desired attacks are defined on it. Definition of the SPS and enforcing the attacks are discussed in the upcoming sections.

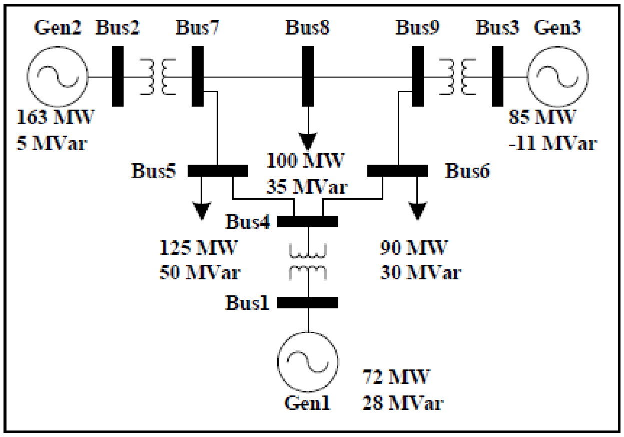


Fig. 7. WSCC 9-bus model [18]

3.3.1. Definition of the special protection model

A production reduction SPS has been designed to eliminate one of the two power plant units in bus No.2 of the system in the event of a fault occurring on one of the two transmission connected to it (lines-line 7-8 and line 7-5). This scheme will be enabled only when the power generation in bus 2 exceeds a specified limit. The power generation is reduced in order to prevent overload of the transmission line and stabilize the power plant units.

3.3.2. Threat model and attack Synthesis

The attacker is assumed as an external malicious entity. He/she could intercept packets that are exchanged through the network. At the first stage, as a passive intruder, he/she eavesdrops data packets and tries to distinguish the patterns. At the suitable time, he clones previously used patterns in data exchanged and pretends to perform a legitimate operation. This type of attack can be categorized as a Man-in-the-Middle Attack.

At the data communication infrastructure, the attacker can flood the network with junk data and fake requests, which could waste network resources and eventually cause drop or delay in corresponding data packets.

At the control process, the attacker could break the authentication control by cracking the password. After intruding the configuration management, the attacker makes changes in the level of acting threshold of inputs and/or the logic of initiating commands.

Here, an attack is considered preventing the implementation of the SPS to reduce and prevent the overload of transmission line 7-8 and eventually the elimination of the transmission line. It is assumed that the power generation in bus 2 is more than the defined threshold and the SPS is activated. Thus, the attack steps are as follows:

1. Command Cloning Attack (CCA) to the protection relay of the transmission line 7-5 to activate SPS. In this infiltration, the attacker uses a legitimate format of previously sent commands to cause damage to the system;

2. Denial of service (DoS) attack to impede sending protection commands to the power plant unit in bus 2 to reach the thermal overloading target of the transmission line 7-8 and eliminating this transmission line.

3. False Data Injection (FDI) attack for the false operation of SPS by manipulating the allowed generation threshold in bus 2 and hence lack of correct command at the right time in the output. In this attack, the attacker uses cyber-security holes in configuration management of the smart digital relay and set fabricated thresholds, which would lead to false SPS commands.

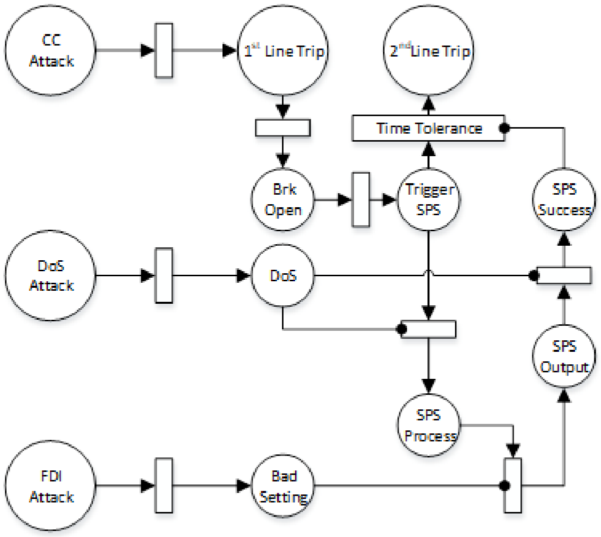
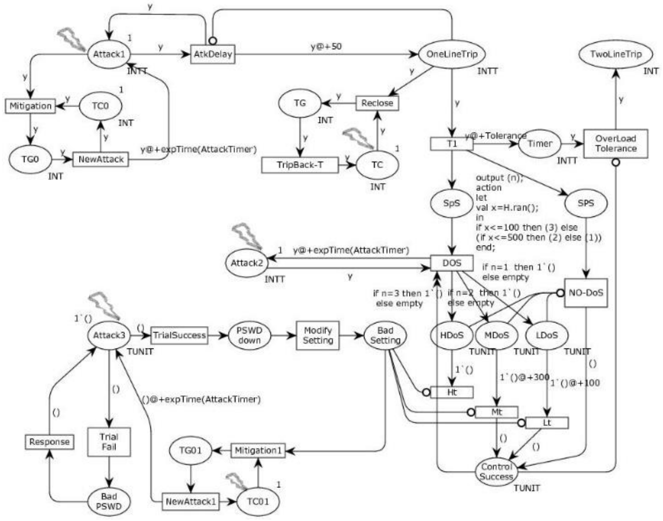


Fig. 8. High level model of attack in Petri net

3.3.3. Timed Petri net (TPN) model

The Petri net model consists of two classes of attack:

First: a two-stage coordinated CCA false command attack to the protection relay of the transmission line 7-5 and a DoS attack to hinder sending the protection command to the generation unit in bus 2. Second: FDI attack.



```
output (n);
action
let
val x=H.ran();
in
if x<=100 then (3) else
(if x<=500 then (2) else (1))
end;
```

Fig. 9. Petri net model for attack using CPN Tools

Three types of mild, moderate, and severe intensity modes have been considered for the DoS attack (Attack2), the probability of each incident is determined in the expression related to the DoS transition and output arcs.

The return time for the attacker is considered as an exponential distribution. In the false trip caused by Attack1, it is assumed that the recloser brings back the transmission line to operate for half of the wrong commands.

In the third attack, the VPN connection created to apply the adjustments of the allowable power for bus 2 is attacked by searching and breaking the password. Through this procedure, the system administrator detects a portion of these attacks by gaining knowledge on the destructive activities using the intrusion detection system (IDS).

The initial places for tokens in this model have been determined in marked locations.

4. Simulation results

In order to evaluate the success rate of the attack defined in two points of the monitor, the number of the desired fault occurrences are defined in the following manner:

- The number of passes through the "Timer" transition: this specifies the number of first transmission line trips, which activates the special protection scheme.
- The number of the second transmission line trip occurrences: this number is achieved by counting the number of accumulated tokens in the "TwoLineTrip" place, indicating the arrival of the attacker to its desired destination of attack.

Table 1. Statistics for single-line and two-line trips

Timed statistics					
Name	Count	Avrg	Min	Max	
Marking-size-Attack'TwoLineTrip_1	248	108.286702	0	237	
Untimed statistics					
Name	Count	Sum	Avrg	Min	max
Count_trans_occur_Attack'T1_1	614	614	1	1	1

Simulation steps executed: 10000
Model Time: 46550

Figure 10 demonstrates the number of single-line and dual trips separately after 10000 execution steps for 46550-time units.

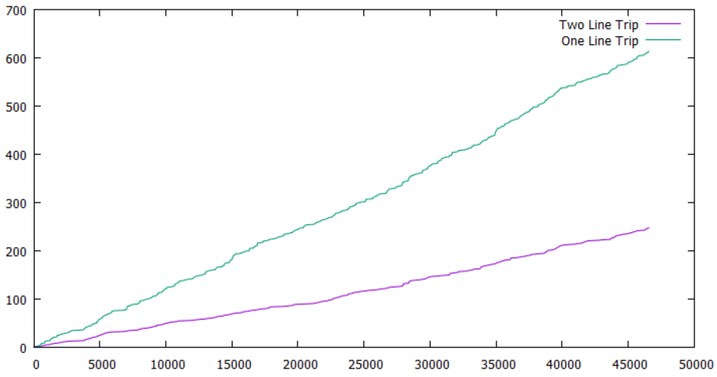


Fig. 10. Number of single-line and dual trips vs. step number

To ensure the output stability, the simulation has been repeated ten times with the same settings, but no significant changes have been observed in the initial trend of the results, indicating the suitable probability patterns for the utilized variables (Table 2).

The results were re-evaluated by changing the parameters of the cyber-attack as follows:

a. Changes in the Return-on-Attack (RoA) time for repeating the attacks.

b. Changes in the probability of intensity in DoS attacks.

Table 2. Statistics for 10 iterations of the simulation

Statistics							
Name	Avrg	90%Half Length	95%alf Length	99%Half Length	StD	Min	Max
count_iid	578.8000	6.4477	7.9567	11.4321	11.1235	550	591
max_iid	1.0000	0.0000	0.0000	0.0000	0.0000	1	1
min_iid	1.0000	0.0000	0.0000	0.0000	0.0000	1	1
sum_iid	578.80	6.4477	7.9567	11.4321	11.1235	550	591
avrg_iid	1.0000	0.0000	0.0000	0.0000	0.0000	1.0000	1.0000
Marking_size_Attack'TwoLineTrip_1							
count_iid	235.3000	6.5182	8.043805	11.5571	11.2452	226	258
max_iid	233.3000	6.5182	8.043805	11.5571	11.2452	224	256
min_iid	0.0000	0.0000	0.0000	0.0000	0.0000	0	0
avrg_iid	115.4896	3.1917	3.9387	5.6591	5.5063	109.7404	129.3526

Number of Replications: 10

4.1. Changes in RoA time to repeat the attacks

By reducing the average RoA time from 30 units to 5 units, it can be observed that with the same number of execution steps, no changes appear in the ratio of the dual trip occurrences to the single-line trip. However, the number of single-line trips increases (Table 3, Figure 11).

Table 3. Statistics for reducing the average RoA time simulation

Name	Count	Avrg	Min	Max
Marking-size-Attack'TwoLineTrip_1	266	125.7657	0	264
Untimed statistics				
Name	Count	Sum	Avrg	Min
Count_trans_occur_Attack'T1_1	699	699	1	1

Simulation steps executed: 10000
Model Time: 11255

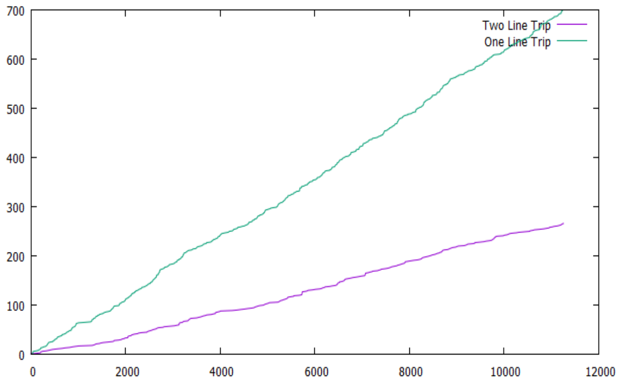


Fig. 11. Simulation result for reducing the average RoA time

4.2. Changes in intensity of DoS attacks

With an increase from 10% to 40% in the high-intensity DoS attack blocking the command line for the SPS, it can be observed that the ratio of the number of trips in both lines to the number of single-line trips increases from about one third to more than half (Table 4, Figure 12).

The intensity of the DoS attack is divided into three levels. Impact of each level is described by adding a delay on the path of SPS commands. The probability of having an attacker with high, medium or low DoS attack ability is tuned in our model.

Table 4. Statistics for increasing the probability of a high-intensity DoS attack

Name	Count	Avrg	Min	Max
Marking-size-Attack'TwoLineTrip_1	329	165.8867	0	327
Untimed statistics				
Name	Count	Sum	Avrg	Min
Count_trans_occur_Attack'T1_1	560	560	1.0000	1

Simulation steps executed: 10000
Model Time: 50352

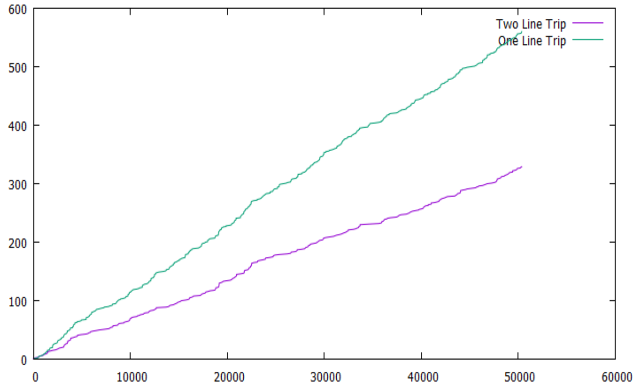


Fig. 12. Simulation result for increasing the probability of a high-intensity DoS attack

4.3. Comparison of the results

The parameters in the reference [19] are considered in order to compare the examples of the cyber-attack model to the proposed SPS (Table 5). Six degrees are taken into account for the DoS attack in this reference. In table 5 x1, x2 and x3 represent the three levels of DoS attack and y1, y2 and y3 are password-breaking parameters. The probability of password breaking by the attacker is P= y1(1-y2) (1-y3).

Table 5. Attack scenarios introduced in [19]

Scenario No.	Low level probability(x1)	Middle level probability (x2)	High level probability (x3)	Foothold obtain rate(y1)	Foothold clear rate(y2)	Password reset rate(y3)
1	0.9	0.05	0.05	1/30	1/5	1/100
2	0.8	0.1	0.1	1/25	1/10	1/200
3	0.6	0.2	0.2	1/20	1/15	1/400

4	0.2	0.4	0.4	1/15	1/20	1/600
5	0.2	0.2	0.6	1/10	1/25	1/800
6	0.1	0.1	0.8	1/5	1/30	1/1000

It is noteworthy that in this study, the parameters involved in changing the probability of the single line trip have not been expressed, hence changes in the settings of the DoS attack in the six defined scenarios does not affect this curve (Table 6, Figure 13). Therefore, the probability of the double-line trip is 0 the reference article with increasing intensity of the DoS attack from scenario number one to six.

Table 6. Statistics for different DoS attack scenarios introduced in [9]

Scenario No.	1	2	3	4	5	6
Number of One-line Attacks	942	946	929	928	909	917
Number of One-line Trips	477	478	466	469	447	464
Number of Two-line Trips	266	285	302	348	352	380
Probability of One-line Trips	0.452	0.446	0.482	0.478	0.498	0.502
Probability of Two-line Trips	0.24	0.268	0.276	0.306	0.361	0.423

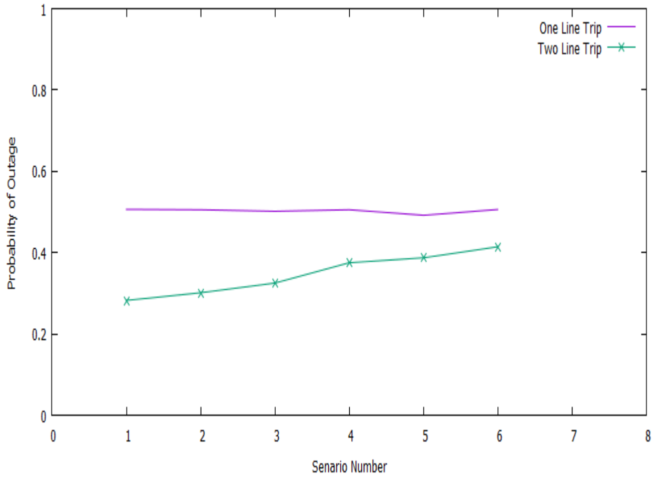


Fig. 13. Comparison of the impact of intensity of DoS attack on double-line and single-line trips in the proposed Petri net model

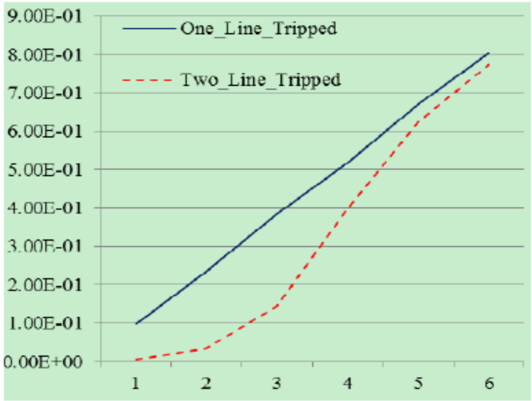


Fig. 14. Impact of intensity of DoS attack on double-line and single-line exits [9]

In both results, it is shown that parametric simulation on the attacker side is working as expected. Although this model is not complete, it is an essential step towards this attempt.

5. Results and future work

In the proposed model, various attacks by means of a unified model in Petri net have been combined. Using this model, it is possible to apply the attack impact on the physical layer, i.e., power transmission network. Also, intermediate and final goal of the attack are separated. The effects of the cyber-attacks are considered here to a specified SPS, which tends to 1. An untimed initiation of a circuit breaker, 2. Delay or block SPS operation and 3. Fake SPS operation. Although this model is used for this specific protective operation, it is also extendable to more general multistage attacks on cyber-physical systems. The authors would like to complete this work on this aspect in the future.

6. Conclusions

Modern power sytems are suseptive to different cyber-attacks, such as multi-stage coordinated attacks to the special protection scheme in power grids. Therefore, these attacks are required to be modeled in an adjustable way. In this study, a timed Petri net was used to model a two-stage attack on the special protection service of the generation rejection. By changing the parameters of the attacker's behavior, including the attacker's average return time and increasing the risk of a high-intensity DoS attack, the simulation results were analyzed. This analysis was done with the goal of examining the effects of these parameters on the attacker's objective for the simultaneous trip of both transmission lines of a system. Finally, a comparison was investigated with the result of a previously presented simulation, and it was revealed that the output of the proposed attack model was suitably consistent. Since other modeling presented in similar studies have not considered the details of the attack model, or only a partial model for the system is examined, the proposed method is ensured to be a completer and more realistic step in the analysis of the cyber-attack to the SPS as a critical service in modern power grids.

References

[1] "Power Swing and Out-of-Step in Transmission Lines - pes-psrc.org." [Online]. Available: http://www.pes-psrc.org/kb/published/reports/Power Swing and OOS Considerations on Transmission Lines F..pdf. [Accessed: 05-Oct-2018].

[2] Parnyan, F., "Black Out Analysis in Iran Power Grid," Niroo Research Institute (NRI) Report, Iran, 2004.

[3] M. Sanaye-Pasand, "Scrutiny of the Iranian National Grid," *IEEE Power and Energy Magazine*, vol. 5, no. 1, pp. 31–39, 2007.

[4] Davis, K. R., C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[5] Nasr, P. M. and A. Y. Varjani, "Petri net model of insider attacks in SCADA system," *2014 11th International ISC Conference on Information Security and Cryptology*, 2014.

[6] Kundur, D., X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a Framework for Cyber-attack Impact Analysis of the Electric Smart Grid," *2010 First IEEE International Conference on Smart Grid Communications*, 2010.

[7] Ten, C., G. Manimaran and C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling", *IEEE Transactions on Systems, Man, and Cybernetics* - Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, 2010.

[8] Mo, Y., T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–Physical Security of a Smart Grid

Infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[9] Zhu, Y., J. Yan, Y. Tang, Y. Sun, and H. He, "The sequential attack against power grid networks," *2014 IEEE International Conference on Communications (ICC), 2014*

[10] Chen, T. M., J. C. Sanchez-Aarnoutse, and J. Buford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp. 741–749, 2011.

[11] Chen, Y., J. Hong, and C.-C. Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations," *IEEE Transactions on Smart Grid,* vol. 9, no. 4, pp. 2541–2552, 2018.

[12] Sgouras, K. I., A. D. Birda, and D. P. Labridis, "Cyber-attack impact on critical Smart Grid infrastructures," *ISGT 2014,* 2014.

[13] Chakraborty, N. and E. Kalaimannan, "Minimum cost security measurements for attack tree-based threat models in smart grid," *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON),* 2017.

[14] Wang, Y.-J., C.-W. Liu, and Y.-H. Liu, "A PMU based special protection scheme: a case study of Taiwan power system," *International Journal of Electrical Power & Energy Systems*, vol. 27, no. 3, pp. 215–223, 2005.

[15] McCalley, J., "System protection schemes: limitations, risks, and management," *Final Report to the Power Systems Engineering Research Center (PSERC),* 2010.

[16] Pashazadeh, S., "Automatic Analysis of Computer Games using Colored Petri net," *Elecrical Engineering Magazine of Tabriz University*, vol. 46, No. 2, 2016.

[17] Wang, J., "Petri Nets for Dynamic Event-Driven System Modeling," *Chapman & Hall/CRC Computer & Information Science Series Handbook of Dynamic System Modeling*, 2007.

[18] Hahn, A., A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[19] Wang, P., A. Ashok, and M. Govindarasu, "Cyber-physical risk assessment for smart grid System Protection Scheme," 2015 *IEEE Power & Energy Society General Meeting,* 2015.