A stochastic Petri net model of jamming attacks on remote-controlled switches during service restoration

Mahdi Bahrami
Montefiore Institute, Department of EE&CS
University of Liège
Liège, Belgium
mahdi.bahrami@uliege.be

Louis Wehenkel
Montefiore Institute, Department of EE&CS
University of Liège
Liège, Belgium
l.wehenkel@uliege.be

***Abstract*— Cyber-attackers can take the advantage of accessibility to field devices to disrupt distribution system (DS) operation. Among field devices, remote-controlled switches (RCSs) play a key role in the fault detection, isolation, and restoration (FDIR) process. Jamming attacks do not require intrusion into the cyber-network of DSs. Thus, RCSs can be easily targeted by jammers. To address this concern, this paper proposes a novel model for simulating jamming attacks against RCSs during an FDIR process. To this end, a novel stochastic Petri net model is proposed that includes two sub-models: jamming-strategy model and trip-issuing model. Using this model, the probability of successful jamming attacks on a target RCS is calculated. In the hypothesized scenario, the attackers create man-made faults on some distribution lines, prompting the distribution system operator (DSO) to initiate an FDIR process. At the same time, they start launching jamming attacks on RCSs. This model can be used by the DSO for performing risk assessment analysis. To show how the jamming attacks could impact DSs, a distribution feeder is studied under the jamming attacks during the FDIR process. Then, the probability of successful jamming attacks, load restoration times, and expected energy not served (EENS) are analyzed in different situations.**

***Keywords*— Jamming attacks, cyber-physical reliability assessment, distribution systems, remote-controlled switches (RCSs), restoration process, stochastic Petri net.**

I. INTRODUCTION

A. Motivation

Smart cyber-attacks could adversely affect power grid operation. In the case of faults in distribution systems (DSs), a fault detection, isolation, and restoration (FDIR) process is applied to detect and isolate the faulty area and re-energize affected loads in the shortest time [1]. Thus, it plays a critical role in the reliability of DSs. However, the malicious actors could target this critical process. To attain their goal, cyber-criminal actors might do coordinated attacks against an FDIR process. Therefore, the operation of DSs under such cyber-attacks can be extremely challenging for the distribution system operator (DSO).

DS components are in an open space. Thus, they can be easily accessed by adversaries. In particular, jamming attacks could easily be launched against communication networks of the field devices. Unlike most of the cyber-attacks, jammers do not require any specific knowledge about the physical part of the system under attack. Additionally, they do not need to intrude into the cyber-networks of targets. Furthermore, it is hard to protect such devices against jamming attacks [2]. Thus, it is necessary for the DSO to deal with such situations during the restoration process. Remote-controlled switches (RCSs) are field devices equipped with communication modules that provide a remote-control option through wireless communication [3]. They are of critical importance to the FDIR process. Indeed, they can isolate a faulty area or restore a load remotely [4]. It is difficult to detect such attacks before issuing switch commands to RCSs [5]. Therefore, the cyber-attacks against RCSs can severely disrupt the FDIR process.

B. Practical Need Description

The DSO mainly counts on the availability of sectionalizing switches (SSs), namely RCSs and manual switches (MSs), for implementing the FDIR process in the face of faults in DSs. In contrast, RCSs might be unavailable due to jamming attacks. Thus, the DSO would not be able to remotely change the status of the targeted RCSs during the FDIR process. In this situation, the DSO needs to come up with a new solution for the FDIR process. In accordance, DSOs require a tool to analyze the risk imposed by this type of cyber-attacks. To this end, DSOs need to estimate the probability of successful jamming attacks against RCSs.

C. Background

In the literature, there are many studies that have focused on the cybersecurity of distribution systems. Among these studies, some researchers have addressed the failure modes of RCSs and their impacts on DSs. The existing research works can be categorized into two main groups. The first group concerns the failure caused by normal events [4], [6]. In this group, the authors in [7] propose a framework for incorporating the unsuccessful operation of SSs into the SS placement problem. Three types of malfunctions are considered, including a malfunction in the remote-control capability of RCSs. However, the second group includes the research works on the cyber-security of RCSs. Among these few research works, the authors in [8] incorporate the two communication failures

This work has been prepared with the support of the Belgian Energy Transition Fund, project CYPRESS (https://cypress-project.be/).

(normal or malicious) into the optimal placement of fault indicators (FIs) and switching devices. The objective is to minimize the investment cost and service restoration cost. In [5], the possible impacts of cyber-attacks against switching devices of DSs are discussed and analyzed in a qualitative way. The malicious actions on RCSs can be classified into several groups, the two most important of which are:

- Sending malicious trip (open/close) commands to RCSs in normal conditions.
- Launching denial-of-service (DoS) attacks against RCSs to make their communication unavailable.

Nonetheless, none of the few publications has explicitly simulated jamming attacks against RCSs during an FDIR process. Thus, they have not yet addressed the evaluation of the probability of success of such DoS attacks.

D. Contributions and Organization of the Article

Promoted by the abovementioned considerations, this paper proposes a new stochastic Petri net (SPN) model for simulating jamming attacks against RCSs during an FDIR process. In the first stage of the hybrid attack, man-made faults are created on some distribution lines by attackers, and when the DSO starts the FDIR process, jammers start launching noise signals against target RCSs. In this situation, noise-jamming signals interfere with control signals sent to an RCS, which may cause trip commands to be not detected by target RCSs. To model this process, an SPN model is proposed that simulates the possibility of coincidence of issued trip commands from the control center to RCSs and jamming signals. In doing so, the probability of successful jamming attacks against a targeted RCS may be calculated. The proposed framework is run from the DSO perspective, and it can be used as a tool for measuring the risk posed by such attacks. The focus of this paper is on modeling jamming-attacks against RCSs. However, to show how they could impact load points, a distribution feeder is analyzed under different situations in the simulation section. In particular, the probability of successful jamming attacks, load restoration times, and the expected energy not served (EENS) are given for each situation. On this basis, the main contribution of this paper can be summarized as follows:

- An SPN model is proposed for calculating the probability of successful jamming attacks on RCSs;
- The proposed model is the first one that simulates the jamming-attacks on RCSs during an FDIR process.

The rest of this paper is organized as follows: Section II presents the considered overall cyber-physical attack scenario. In Section III, the proposed SPN model for the jamming attacks is explained. Numerical results are given and discussed in Section IV. Finally, Section V provides conclusions.

II. Proposed Framework Outline

A. Overall Cyber-Physical Attack Scenario against RCSs

In the hypothesized cyber-attack scenario, some man-made faults are created on distribution lines. Subsequently, coordinated cyber-actors initiate jamming attacks against RCS communications shortly after the occurrence of the man-made faults, while the DSO starts to open/close RCSs to restore service. Consequently, the communication network of compromised RCSs becomes unavailable, because control signals are jammed by attackers. Thus, the status of the RCSs with successfully targeted communication networks cannot be remotely changed during the jamming attack. It is assumed that each jammer is equipped with the required devices to transit noise signals against target RCSs. In addition, the jammers have already selected their victims and found proper places to emit jamming signals against the targets. In this regard, the timeline of the overall attack scenario is shown in Fig. 1.

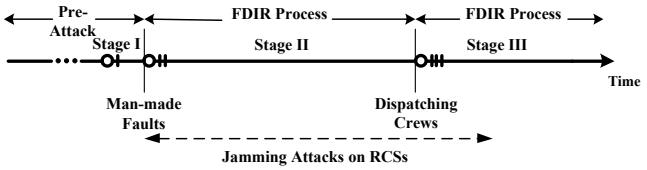

Fig. 1. Timeline for the events of the overall cyber-physical attack scenario.

In Fig. 1, the stages are defined as follows:

Stage I: attackers cause man-made faults on target distribution lines. Thus, the faults are sensed by circuit breakers (CBs), and downstream load points are de-energized.

Stage II: DSO starts to perform the FDIR process, and meanwhile jamming attacks are launched against target RCSs. In the second stage, the DSO tries to perform some remote switching actions to restore as much load as possible. However, due to the jamming-attacks, successfully targeted RCSs cannot be controlled remotely. In other words, the DSO cannot remotely change the status of targeted RCSs.

Stage III: due to the uncontrollability of targeted RCSs, switching actions should be manually done. Thus, crews are dispatched to the locations of targeted RCSs.

Notice that the focus of this paper is on the second stage, namely modeling noise-jamming attacks against an RCS to enable the computation of their probability of success.

III. Proposed Stochastic Petri Net Model for Jamming Attacks against RCSs

In this section, an SPN model is proposed for simulating jamming-attacks on a target RCS during an FDIR process.

A. Petri Net Overview

Petri nets are a type of graphical-based models, by which we can simulate the dynamic behavior of real systems. The dynamic aspect is characterized by firing rules [9]. A Petri net includes four different components [10], as follows:

Places: which are represented by circles and show conditions.

Transitions: which are drawn by bars and model actions in the system. In general, transitions can be divided into *immediate* and *timed* transitions. The former is drawn by a black bar while the latter is graphically represented by an open bar.

Tokens: which are depicted by black dots. Tokens reside within places, and a token models a specific value of conditions. For example, it can indicate the availability of resources.

Arcs: which are used for interconnection between places and transitions.

When a transition is enabled according to the transition enabling rules, it can fire (an event or activity takes place) after

firing time [11]. The firing time of immediate transitions is equal to zero, while that of a timed transition is random and follows an exponential distribution. In the context of Petri nets, the parameter of the exponential distribution is referred to as the transition rate. In this regard, each timed transition has its own transition rate. When a transition fires, a certain number of tokens are removed from input places, and some tokens are generated in output places.

B. Proposed SPN Model for the Jamming Attacks

In the proposed model, the SPNs are used to model a jamming-attack against a target RCS. SPNs can model discrete events as well as stochastic timing. In addition, they are a suitable tool for modeling the dynamic nature of jamming attacks against RCSs. In contrast, other approaches such as the Monte Carlo simulation are not able to show it. Furthermore, Petri nets can model concurrent events as well as state transitions. For a successful jamming attack against RCSs, the events must happen simultaneously: 1- issuing trip commands 2. emitting jamming signals. In this regard, SPNs are deployed in this paper.

The proposed model consists of two sub-models: *Jammer's strategy model* and *control-command-issuing model*. This model integrates three agents, namely a jammer, the control center (DSO), and a target RCS. Fig. 2 shows the proposed SPN model. This model simulates jamming attacks against trip commands during an FDIR process. As man-made faults are created by attackers, the jammers know the timeline for the FDIR process approximately. However, they do not know the exact time of data transmission over the communication channel. Thus, this event (issuing the trip command) is a stochastic process. It should be notified that this model represents the attempts to send a trip command to a targeted RCS. However, some of the attempts are unsuccessful, because they are successfully jammed. The idea is to calculate the probability that legitimate data packets are indeed accompanied by noise signals, in order to evaluate the probability of successful jamming attacks.

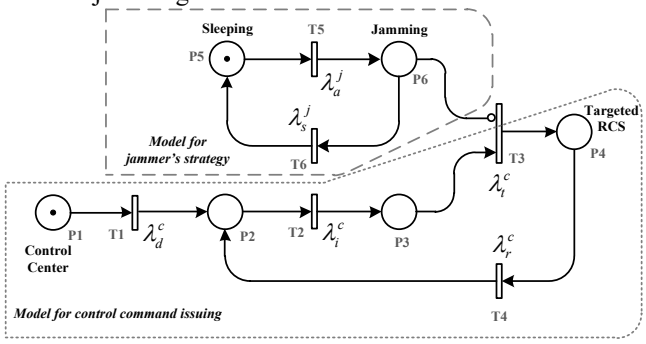

Fig. 2. Proposed SPN model for simulating noise-jamming attacks against a target RCS.

1) Sub-model for Trip Command Issuing: This sub-model models the attempts of an operator to send a trip command to a targeted RCS. When the attacker is in the jamming mode, the trip command issued by the control center cannot be detected by the RCS. If data packets of the trip command are transmitted during this duration, they are accompanied by strong noise. Thus, signal-to-noise ratio (S/N) would be very low, and the RCS has difficulty receiving the legitimate data packets [12].

In this model, transition T1 models the time delay of making a decision about the FDIR process. In other words, it models the time required to find a solution for the FDIR process. In addition, its transition rate, λ_d^c, represents the rate at which the DSO finds a solution for the FDIR process. In the SPN model, place P1 represents the situation in which the decision is made. In place P2, the trip command is ready to be sent to the RCS. The transition rate of transition T2, λ_i^c, shows the rate at which control command is issued from the control center during the FDIR process. The reason for this consideration is that when a trip command is jammed by noise signals, it is still received by the RCS. However, the legitimate data packets have been corrupted, and they cannot be interpreted by the receiver (the targeted RCS). Place P3 models the situation in which the legitimate packets are in transit over the communication channel. Thus, transition T3 models the time delay of the communication channel between the DSO and the RCS. The transition rate of T3, λ_t^c, is reciprocal of the transmission delay of data packets over the communication network. Once the data packets are received by the RCS in place P4, they are proccessed by the RCS. In this situation, there are two possibilities:

- The trip command is detected by the RCS, and its status is changed (unsuccessful jamming attack).
- The trip command is successfully jammed, and it cannot be detected by the RCS (successful jamming attack).

For both possibilities, the DSO monitors the status of the RCS. To show this interaction for remote monitoring, there is a return path from place P4 to place P2. The transition rate of this path, denoted by λ_r^c, represents the rate at which the control center receives a response from the RCS. It is associated with the time delay of receiving response from the RCS. In this regard, when the operator finds out that the status of the RCS could not be remotely changed, he/she repeats the trip command.

2) Sub-model for Jammer's Strategy: This submodel represents the strategy of a jammer to disrupt the communication between the control center and a target RCS. In this submodel, place P5 depicts the sleeping mode of a jammer. In this place, the jammer is ready to launch noise signals. In other words, transition T5 becomes enabled once place P5 is marked with at least one token (i.e. jammer is in sleeping mode). After it fires, the jammer moves to the jamming mode, namely place P6. However, when a jammer emits noise signals, the communication channel is under a jamming attack. This is modeled by connecting place P6 to transition T3 via an inhibitor arc (the circle-headed arc). As can be seen in Fig. 2, when place P6 is marked with a token, the transition T3 cannot become enabled, which is according to one of the enabling rules of Petri nets [10]. If there is also a token in place P3 in this situation, the token cannot move to place P4 and remains in place P3 until

the jammer returns to the sleeping mode. Once the jammer goes back to the sleeping mode, the token can transfer from place P3 to place P4. This models the situation in which the legitimate data packets have been successfully jammed. In this situation, the communication channel has been saturated with noise signals. Thus, the processing or transmission of the data is delayed. Furthermore, once processed, the trip command cannot be detected by the RCS.

In this model, λ_a^j and λ_s^j are so-called jamming rate and sleeping rate, respectively. Jamming rate represents the number of times that an attacker moves into the jamming mode divided by the time spent in the sleeping mode. Similarly, sleeping rate is the rate at which a jammer transits from the jamming mode to the sleeping mode.

C. Analysis of the SPN Model

Quantitative analysis of an SPN can be conducted by analyzing its associated Markov model [9]. To this end, the reachability graph of the SPN under study should be constructed first.

1) Reachability Graph of the SPN

Starting from an initial marking, a reachability graph represents all possible markings that are reachable from it. Each marking depicts a distribution of tokens among the places. The reachability graph of the SPN shown in Fig. 2 is depicted in Fig. 3.

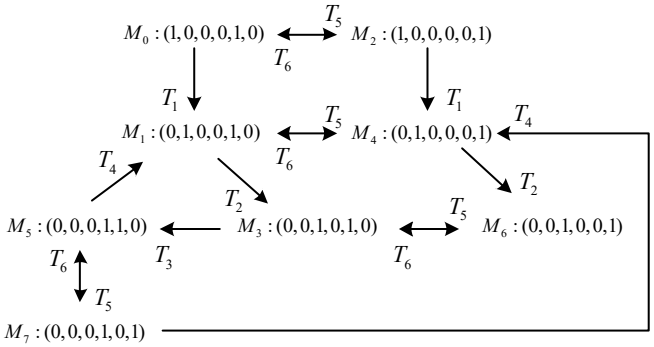

Fig. 3. Reachability graph of the proposed SPN.

As depicted in Fig. 3, there are eight possible markings (labeling M_0 to M_7) for the SPN under study. The initial marking, M_0, corresponds to the starting point of the SPN, (1, 0, 0, 0, 1, 0), also shown in Fig. 2.

2) Calculating Steady-State Probabilities of Different Markings

In the case of SPNs, a reachability graph can be directly transformed to its associated Markov model. To this end, markings and transitions are replaced by states and their corresponding transition rates, respectively. The steady-state probability of being in each state (marking), π_s , can be calculated by solving the following linear equation:

$$\tilde{\pi} Q = \mathbf{0}, \quad \sum_{s=0}^{7} \pi_s = 1 \tag{1}$$

In (1), the transition rate matrix, $\mathbf{Q}$, is constructed as follows:

$$\begin{bmatrix}
-\lambda_d^c-\lambda_a^j & \lambda_d^c & \lambda_a^j & 0 & 0 & 0 & 0 & 0 \\
0 & -\lambda_i^c-\lambda_a^j & 0 & \lambda_i^c & \lambda_a^j & 0 & 0 & 0 \\
\lambda_s^j & 0 & -\lambda_s^j-\lambda_d^c & 0 & \lambda_d^c & 0 & 0 & 0 \\
0 & 0 & 0 & -\lambda_i^c-\lambda_a^j & 0 & \lambda_i^c & \lambda_a^j & 0 \\
0 & \lambda_s^j & 0 & 0 & -\lambda_s^j-\lambda_i^c & 0 & \lambda_i^c & 0 \\
0 & \lambda_r^c & 0 & 0 & 0 & -\lambda_r^c-\lambda_a^j & 0 & \lambda_a^j \\
0 & 0 & 0 & \lambda_s^j & 0 & 0 & -\lambda_s^j & 0 \\
0 & 0 & 0 & 0 & \lambda_r^c & \lambda_s^j & 0 & -\lambda_r^c-\lambda_s^j
\end{bmatrix}$$

Among the obtained markings, M_6 represents the situation in which the trip command is successfully jammed by the jammers. In this marking, there is a token in place P3 and a token in place P6. Thus, the probability of launching successful attacks against an RCS is:

$$P^{jam} = \pi_6 \tag{2}$$

IV. Simulation Results

In this section, the proposed model is applied to a simple network to investigate its performance.

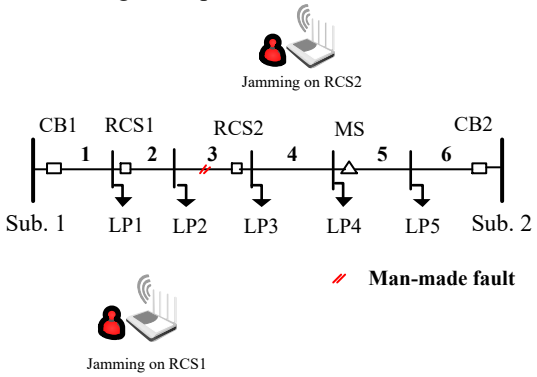

Fig. 4. A simple distribution network under jamming attacks against the RCSs.

A. Assumptions and Simulation Data

A simple network, including two circuit breakers (CBs), two RCSs, and one MS; is shown in Fig. 4. It is assumed that two jammers are positioned to disrupt the communication between the DSO and the RCSs in a coordinated manner. Thus, each jammer targets an RCS.

The jammers are assumed to operate in jamming mode for about 85 percent of the jamming attack duration. In addition, it is assumed that it takes the DSO 10 minutes to start the FIDR process following the man-made fault on distribution line 3. Afterward, the DSO starts to send trip commands to the RCSs. However, as the DSO detects a problem with the communication channel, trip commands are re-sent every 5 minutes. Based on these assumptions, the values of different transition rates of the proposed SPN are calculated, which are given in Table I. For the sake of simplicity, the parameters of the SPN are assumed to be the same for the jamming attacks against the two RCSs.

TABLE I. TRANSITION RATES OF THE SPN MODEL

Transition	Rate (occ/*min*)
λ_a^j	30
λ_s^j	5
λ_t^c	4000
λ_i^c	0.2
λ_r^c	1600
λ_d^c	0.1

B. *Simulation Results for a Single RCS Attack*

In order to investigate the effectiveness of the proposed model, the following three cases are studied, while focusing on a jamming attack on a single RCS (either RCS2, RCS1):

1) Quantitative analysis of the SPN (base case):

By quantitative analysis of the reachability graph illustrated in Fig. 3, the probability of successful jamming attack on the RCS is calculated as 0.033.

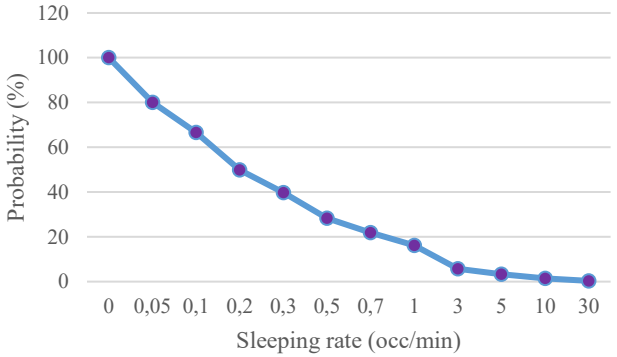

Fig. 5. The probability of successful jamming attack against an RCS under different values of sleeping rate.

2) Sensitivity analysis with respect to sleeping rate (λ_s^j)

In this case, a sensitivity analysis is performed to investigate the effect of sleeping rate on the probability of successful jamming against an RCS. To this end, the value of this parameter is changed in discrete steps from 0 to 30. The results are shown in Fig. 5. As can be traced in this figure, as the value of sleeping rate increases, the probability of successful jamming decreases. This observation can be justified as follows. As the value of this parameter is increased, the time that a jammer spends in jamming mode is reduced. Thus, the probability of coincidence between jamming signals and the legitimate data packets decreases. However, the variations do not follow a linear pattern. In particular, when sleeping rate is zero, the jammer remains in jamming mode and never switches to sleeping mode. In this situation, the probability of successful jamming must be equal to one, which is verified by the results shown in Fig. 5.

3) Implementing the model on a distribution feeder

To show how load points are affected by jamming attacks, the jamming attacks are launched against the two RCSs of the distribution feeder depicted in Fig. 4. Additionally, four different scenarios for the coordinated jamming attacks on the RCSs are considered, which are summarized in Table II.

TABLE II. SCENARIOS FOR THE COORDINATED JAMMING ATTACKS

Scenario #	RCS1	RCS2	Probability
1	Normal	Normal	0.935089
2	Jammed	Normal	0.03191
3	Normal	Jammed	0.03191
4	Jammed	Jammed	0.0011

In addition, the initial status of the switches is given in Table III.

TABLE III. INITIAL STATUS OF THE SWITCHING DEVICES BEFORE THE MAN-MADE FAULT

Switching Devices	CB1	RCS1	RCS2	MS	CB2
Initial Status	Closed	Closed	Closed	Closed	Open

Notice that in this scenario, we assume that the successfulness of the attacks on the two RCSs are probabilistically independent events. The reason for this is that the jamming attacks are carried out by two jammers at two different locations. Although they target the two RCSs in a coordinated manner, the timing of their jamming and sleeping modes may differ. Additionally, the trip commands to the RCSs can be issued sequentially with a short interval by the DSO. Furthermore, the transmission time of a trip command over the communication channel is very short. Therefore, this assumption is reasonable. After the occurrence of the man-made fault on line 3, CB1 operates and de-energizes all the load points. When jammers are unsuccessful in targeting the RCSs, RCS1 and RCS2 are opened remotely by the DSO, and then CB1 is closed. Afterward, CB2 is closed. In this case (scenario 1 in Table II), all the load points except for load point 2 (LP2) are energized after the remote switching time (T_{RS}). Load point 2 will be energized after the repair time (T_R). In scenario 2, RCS1 is under successful jamming attacks. Therefore, the DSO cannot remotely control it. In this situation, the DSO should modify the initial service restoration plan. Therefore, the DSO remotely opens RCS2 and closes CB2, thereby supplying LP3-LP5. In addition, crews are dispatched to the location of RCS1, and it is then opened manually. As a result, LP1 becomes energized after manual switching time (T_{MS}). Once line 3 is repaired, LP2 is supplied. A similar analysis can be carried done for the other two scenarios, namely 3 and 4. The results in terms of the restoration time of each load point are listed in Table IV.

TABLE IV. LOAD POINT RESTORATION TIMES FOR EACH SCENARIO

Scenario#	**LP1**	**LP2**	**LP3**	**LP4**	**LP5**
1	T_{RS}	T_R	T_{RS}	T_{RS}	T_{RS}
2	T_{MS}	T_R	T_{RS}	T_{RS}	T_{RS}
3	T_{RS}	T_R	T_{MS}	T_{MS}	T_{MS}
4	T_{MS}	T_R	T_{MS}	T_{MS}	T_{MS}

It should be notified that in the simulations, only one cyber-event caused by jammers is studied, and the results in terms of probability and restoration times are reported in Tables II and IV, respectively. The restoration times for each load point are reported in numerical values in Table V.

TABLE V. LOAD POINT RESTORATION TIMES FOR EACH SCENARIO

Load point #	LP1	LP2	LP3	LP4	LP5
Demand in kW	800	600	400	480	1000
Scenario #	Restoration time in min				
1	10	360	10	10	10
2	60	360	10	10	10
3	10	360	60	60	60
4	60	360	60	60	60

Using the data provided in Table V as well as the probability of successful jamming attacks (shown in Fig. 5), EENS is calculated for various values of the sleeping rate. The results of this sensitivity analysis are presented in Fig. 6.

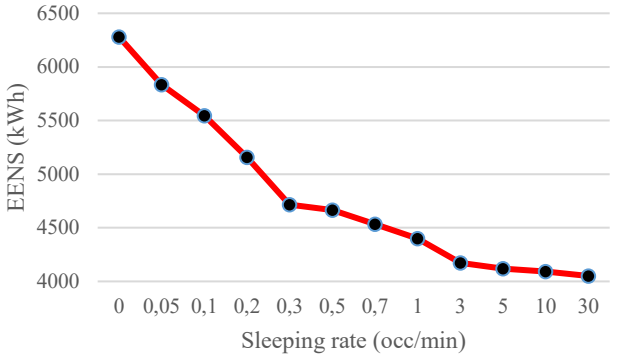

Fig. 6. EENS under different values of sleeping rate.

When there are no jamming attacks or when both jamming attacks are unsuccessful, the value of EENS is 4043 kWh due to the fault on line 3. However, if both attackers remain active and never switch to sleeping mode (a sleeping rate of zero), EENS value increases to 6280 kWh, representing a 55.3% rise from the base value of 4043 kWh. Notice that this is caused by a single jamming attack on the RCSs. Indeed, if the jammers target them multiple times a day, they could be able to disrupt the normal operation of the DS.

V. CONCLUSION AND SUMMARY

This paper proposed a new SPN for simulating noise-jamming attacks against RCSs during an FDIR process. The proposed model considers attackers' strategy as well as the transmission of a trip command between a control center and an RCS. In the model, attackers switch between sleeping and jamming modes. Using the proposed SPN, the probability of successful jamming against a target RCS is calculated. In addition, this model equipes DSOs with a tool for doing risk analysis. To this end, the jamming scenario under study was implemented on a simple distribution network to show how load points are affected by such attacks. To this end, the probability of successful jamming attacks, load restoration times, and EENS were calculated and discussed for different conditions. The results showed that such attacks could severely affect load point restoration times and jeopardize DS reliability. Thus, this attack scenario not only could disrupt the normal operations of DS but also could lead to customer dissatisfaction. DSOs can take some measures to defend or mitigate the impacts of jamming attacks against RCSs. For example, they can use resilient communication, jamming-resistant protocols, or adaptive system design. However, jammers could still successfully launch jamming attacks. In this regard, this paper helps DSOs enhance their situational awareness.

REFERENCES

[1] A. Zidan *et al*., "Fault Detection, Isolation, and Service Restoration in Distribution Systems: State-of-the-Art and Future Trends," in *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2170-2185, Sept. 2017, doi: 10.1109/TSG.2016.2517620.

[2] J. Niu, Z. Ming, M. Qiu, H. Su, Z. Gu, and X. Qin, "Defending jamming attack in wide-area monitoring system for smart grid," *Telecommun. Syst*., vol. 60, no. 1, pp. 159–167, 2015.

[3] ABB. (2024). Outdoor switching points [Online]. Available: https://search.abb.com/library/Download.aspx?DocumentID=3407PL1618-W1-EN&LanguageCode=en&DocumentPartId=&Action=Launch.

[4] M. Farajollahi, M. Fotuhi-Firuzabad and A. Safdarian, "Simultaneous Placement of Fault Indicator and Sectionalizing Switch in Distribution Networks," in *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2278-2287, March 2019, doi: 10.1109/TSG.2018.2794994.

[5] I. -S. Choi, J. Hong and T. -W. Kim, "Multi-Agent Based Cyber Attack Detection and Mitigation for Distribution Automation System," in *IEEE Access*, vol. 8, pp. 183495-183504, 2020.

[6] J. Liu, C. Qin and Y. Yu, "Enhancing Distribution System Resilience with Proactive Islanding and RCS-Based Fast Fault Isolation and Service Restoration," in *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2381-2395, May 2020, doi: 10.1109/TSG.2019.2953716.

[7] M. Farajollahi, M. Fotuhi-Firuzabad and A. Safdarian, "Optimal Placement of Sectionalizing Switch Considering Switch Malfunction Probability," in *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 403-413, Jan. 2019, doi: 10.1109/TSG.2017.2741424.

[8] M. Heidari Kapourchali, M. Sepehry and V. Aravinthan, "Fault Detector and Switch Placement in Cyber-Enabled Power Distribution Network," in *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 980-992, March 2018, doi: 10.1109/TSG.2016.2573261.

[9] M. Bahrami, M. Fotuhi-Firuzabad and H. Farzin, "Reliability Evaluation of Power Grids Considering Integrity Attacks Against Substation Protective IEDs," in *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1035-1044, Feb. 2020, doi: 10.1109/TII.2019.2926557.

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

[11] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis, Modelling with Generalized Stochastic Petri Nets. Hoboken, NJ, USA: Wiley, 1994.

[12] D. Orlando, "A Novel Noise Jamming Detection Algorithm for Radar Applications," in *IEEE Signal Process. Lett.*, vol. 24, no. 2, pp. 206-210, Feb. 2017, doi: 10.1109/LSP.2016.2645793.