Chapter 4

Towards Analyzing the Impact of Intrusion Prevention and Response on Cyber-Physical System Availability: A case study of NPP

Deploying either preventive or responsive measures alone may not be enough to detect and respond to intrusion attempts and subsequent sophisticated attacks. Industrial Control Systems Computer Emergency Response Team (ICS-CERT) and International Society of Automation/ International Electrotechnical Commission Standards (ISA/IEC-62443) recommend defense-in-depth strategies to reduce intrusion and their impact [35, 143]. In this chapter, we present a GSPN based modeling approach [27] to quantitatively analyze the effect of integrating preventive and responsive defense measures. GSPN can model the dynamics of realistic systems by considering the stochastic nature of threats, attackers, and safeguards. Moreover, it tackles the problem of state space explosion. The integration of diverse defense mechanisms reduces the intrusion rate to make the system secure and fault-tolerant.

If one layer turns out to be inadequate, another layer of defense would hopefully prevent a complete breach. The applied preventive measures integrate a series of defense measures including perimeter protection, authentication, and authorization mechanisms to reduce the attack frequency by preventing unauthorized access. The responsive measures are implemented using the Intrusion Detection and Response Layer (IDRL). It periodically monitors the behavior of authenticated users to detect unusual behavior and its impact on the system. Once the attack is detected, remedial actions are taken by blocking the suspicious activity. If IDRL fails to detect and respond to the attack, manual recovery needs to initiate to make the system operational. Thus, 2-stage-layered security model significantly reduces the probability of attack and manual recovery rate. Further, as it is difficult to test cyber-attacks experimentally in NPPs or to simulate them virtually. Hence, the transition rates of stochastic model are difficult to obtain and so is the determining the failure probabilities of preventive and responsive security measures. The proposed work overcomes this problem also by performing a sensitivity analysis to analyze the effect of defense measures strength and to prioritize these measures.

Outline: The rest of this chapter is organized as follows. Section 4.1 presents a roadmap to identified research question RQ.2. Section 4.2 presents a formal specification of preventive and responsive measures. Section 4.3 validates the proposed approach on the NPP case study and section 4.4 summarises the chapter.

4.1 A roadmap to research solution

The section briefly presents the answer to the identified research question RQ.2 in the subsections.

4.1.1 Intrusion-Disruption Model

This section explains the intrusion-attack model for SC-CPS. Each subsystem of SC-CPS is formally a closed-loop process control system and represented as a 3-tuple $< S, C, A >$ where S is a set of sensors, C is a set of controllers, A is a set of actuators. The dynamic behavior of CPS is formally presented as equations (3.1) and (3.2) as mentioned in section 3.1. In SC-CPS, attacks on the networked control system and assets are performed to intrude into the system and exercise the damage or disruptions in the intended system functionalities by exploiting the existing vulnerabilities. These attacks may be generated in-house or by external malicious actors. Formally, an attack atk_i is defined as an 8-tuple

$$atk_i = (as, p_i, ta, s_{ta}, \omega_i(t), \delta_t, av, v_i) \tag{4.1}$$

where, as is attack surface, which may be sensors, digital actuators, control nodes or storage servers, p_i represents frequency of successful attack atk_i, ta is target security attribute including confidentiality, availability or integrity and represented as continuous variable with value $0 \geq ta \leq 1$, s_{ta} is targeted system attribute or functionality to affect the target attribute value, $\omega_i(t)$ is impact per unit time, δ_t is active attack duration defined as difference between time stamps t_e and t_s where t_s is attack start time and t_e is attack end time, av is attack vehicle or vector, v_i is a vulnerability to be exploited. Thus, an attacker may launch an attack atk_i such as with frequency p_i using attack surface as and attack vehicle av such as malware, remote access trojan, malicious botnet or social engineering to target the security attribute ta with impact $\omega_i(t)$ per unit time for attack duration δ_t by exploiting the vulnerability v_i to disturb the system functionality s_{ta} or operational state of system $sm_x(t)$. To damage a control system, an attacker performs attack actions in two phases. In the first phase, a series of attacks are launched to penetrate the target system. In case of intrusion phase, $\omega(t) = \phi$ as the disruption or loss is zero in intrusion attack. In the second phase, an integrity or DoS attack is launched to abuse

and disrupt the critical functions of system, consequently the system availability.

$$ta' = ta - \int_{ts}^{te} \omega(t)dt \tag{4.2}$$

Thus, the weak intrusion detection and prevention policy facilitates the attacker to intrude into the control network. In our intrusion-disrupt model, the attacker intrudes into control network by exploiting open port vulnerability (v_1) to connect to the networked system. He exploits the remote code execution vulnerability v_2 to install and execute the payload (malicious script) on control nodes. He further uses weak encryption (v_3) or stack overflow vulnerabilities (v_4) to perform data or operational parameters tempering, denial of intended services, respectively. The cyber risk impact RI is estimated as

$$RI = p \times L \tag{4.3}$$

where the probability of a successful disruption is a joint probability of exploiting the vulnerabilities to intrude into the system p_i and the probability to disrupt the system p_d

$$p = p_i \times p_d \tag{4.4}$$

To disrupt the CPS, an attacker performs integrity or denial of service attacks on either sensors or control system to disrupt the system functionality or affect the system availability that results in forcing the CPS into an emergency shut down. DoS and integrity attacks on the sensor can be represented as described in equation (3.6) and (3.7). Similarly, DoS attack on controller C_y is represented as loss of the control signal c_y

$$c_y'(t + \delta t - t) = 0 \tag{4.5}$$

and

The integrity attack on the controller C_y is represented as manipulation of control signals c_y

$$c'_y(t + \delta t - t) = c_y(t + \delta t - t) \pm \sigma'(t + \delta t - t) \tag{4.6}$$

The total possible loss in case of successful disruption or abuse is calculated as $L = \omega(\delta_t) = \int_{t1}^{t2} \omega(t)dt$ which reduces the target attribute, the availability Avl to

$$Avl = 1 - \int_{t1}^{t2} \omega(t)dt \tag{4.7}$$

where $\int_{t1}^{t2} \omega(t)dt$ estimates the time system is in failed state.

The following assumptions are taken into consideration in the presented work, (1) the difference between outside and inside attackers is based on their perimeter permission privileges. Unlike insider attackers, the outside attacker needs to defeat perimeter protection to intrude into the target system/node. (2) We assume that the attacker has knowledge of operational and control parameters and whenever he/she has chance, he/she attacks with probability 1. (3) Attacks and component failures are independent.

4.1.2 Security Measures

This subsection briefs the model of the proposed work that applies a sequence of preventive layers in the first stage to harden the attack path for protecting the system against the exploitation of network and host level vulnerabilities. Although, there is still a possibility that the preventive defense measures are failed to prevent intrusion into control nodes. In the second stage, responsive defense aspects are applied for attack detection and response to minimize the attack effects or losses. Section 4.2 and 4.3 present the answer to RQ2 in details. These sections explain the formal specification of each defense layer and its combined effect with proof of concept.

4.2 Formal Specification of Applied Security Measures

This section formally explains arrangement of applied preventive and responsive security measures as shown in FIGURE 4.1 to counter the probable attacks on the ICS control system. The security approach cascades a series of diverse preventive and responsive defense measures to implement defense in-depth strategy that significantly reduces the risk of compromising the intended system functionality and security attributes.

$$D = \{D_P \wedge D_R\} \tag{4.8}$$

where, D_P is a set of preventive defense measures, D_R is a set of responsive defense measures. By the strength of security mechanism S_{Dj} we mean the probability of defense D_j being successful against attack atk_i, which is equivalent to $P(D_j|atk_i)$ as probability of the same as shown in equation (4.9). The strength of defense measure subsumes the notion of strength of the attacker as in cases when the attack can not be countered by the defense mechanism then security failure takes place. Thus, we are only concentrating on frequency of occurrence of attack and correspondingly being successful or failing of the defense mechanism for the chosen attack type. The strength of defense measure is calculated as conditional probability

$$S_{Dj} = P(D_j|atk_i) = \frac{P(D_j \cap atk_i)}{P(atk_i)} = \frac{P(D_j) \times P(atk_i)}{P(atk_i)} = P(D_j) = 1 - f_{Dj} \tag{4.9}$$

where, f_{Dj} represents the failure rate or failure probability of each defense measures D_j acting against attack atk_i.

4.2.1 Preventive Measures

Preventive measures act proactively to reduce the frequency of attacks by preventing unauthorized access. Firewalls deny the unauthorized network connections but unable to defend against the attacks from authorized ports (internal attacks). Hence, it

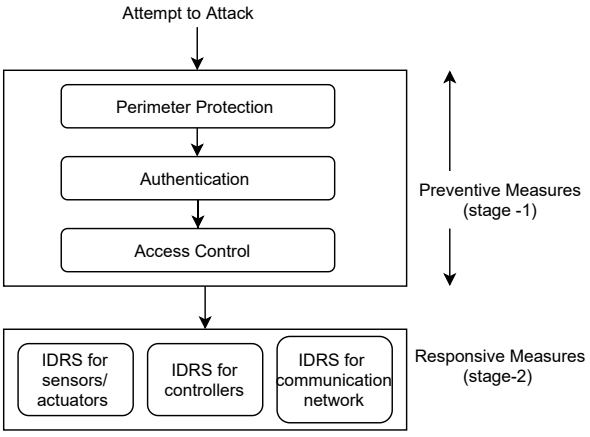

FIGURE 4.1: General underline framework of CPS security

does not cover the critical unpatched vulnerabilities on host. Authentication and access control prevent the host level intrusions. Hence, preventive measures integrate perimeter, authentication and access control model to reduce penetration attempts on control system. D_P is defined as conjunction of defense measures

$$D_p = \{D_{PP} \wedge D_A \wedge D_{AC}\} \tag{4.10}$$

where, D_{PP} is perimeter protection layer, D_A is authentication layer and D_{AC} is access control layer. These integrated layers jointly perform the boundary inspection of malicious packets and intrusion attempt on each controller node.

4.2.1.1 Perimeter Protection Layers

Firewall guards the private network resources against outside Internet. It provides a primary level of protection to the ICS control network [57]. A firewall filters the malicious packets based on different criteria, including interface, source IP, destination IP, protocol type, port, and packet size of a predefined security rule set. Formally, firewall D_f maps each packet $pkt \in \Sigma$, to a decision set dn as [84]

$$< dn >= D_f(pkt) \tag{4.11}$$

where $\Sigma = \{pkt_c\} \cup \{pkt_m\}$ is a finite set of all packets including clean or malicious and $dn = \{accept, discard\}$. D_f and pkt is defined over the d-tuple criteria $(C_1, ..., C_d)$, where $1 \leq i \leq d$, is a set of non-negative integers. D_f consists of a sequence of x non-overlapping rules $< r_1, ..., r_x >$. Each rule r_j, where $1 \leq j \leq x$, is defined as

$$(C_1 \in S_1) \wedge ..... \wedge (C_d \in S_d) \implies < dn >$$

where $S_i \subseteq D(C_i)$. A packet $pkt = (pkt_1, ..., pkt_d)$ satisfies the firewall rule iff the condition $(pkt_1 \in S_1) \wedge ..... \wedge (p_d \in S_d)$ holds.

Thus, the firewall reduces the probability of attack p to resultant attack probability p' by its defense strength.

$$p' = p - (1 - f_{D_f})p \tag{4.12}$$

where f_{D_f} is firewall failure probability, depending on firewall misconfiguration and calculated as

$$f_{D_f} = 1 - (\frac{\text{number of detected malicious packets}}{\text{total malicious packets}}) \tag{4.13}$$

4.2.1.2 Authentication Layer

Authentication maintains host-level security and privacy to prevent the host level vulnerability exploitation by password protection. Password design is governed by a password policy that includes password encryption and authentication methods. Formally, authentication D_a maps each request $ar \in \Sigma'$, to a decision set dn' as

$$< dn' >= D_a(ar) \tag{4.14}$$

where $\Sigma' = \{ar_l\} \cup \{ar_{il}\}$ is a finite set of all requests including legitimate or illegitimate and $dn' = \{success, fail\}$. It reduces the p' to resultant attack probability p'' by its defense strength.

$$p'' = p' - (1 - f_{Da})p' \tag{4.15}$$

where f_{D_a} is authentication failure rate, depending on missing, default or weak password and calculated as

$$f_{D_a} = 1 - (\frac{\text{number of detected illegitimate login attempt}}{\text{total login attempt by attacker}}) \tag{4.16}$$

4.2.1.3 Access Control Layer

The access control layer checks the associated permissions of authenticated user before allowing access and operates on critical resources using user-role assignment matrix UM and role-permission matrix RM. UM is defined as 2-tuple (u, rl), where u is a set of users, rl is a set of user-role. RM is defined as 3-tuple (rl, r, op), where r is a set of resources, op is a set of operations. Thus, $role$ is a mapping defined as $role : u \rightarrow pr$, where $pr = \{r \times op\}$ is a set of permissions. [2]. Formally, access control measure D_{ac} maps each access request $ar \in \Sigma''$ to a decision set dn'' as

$$< dn'' >= D_{ac}(ar) \tag{4.17}$$

where $\Sigma'' \subset \Sigma'$ and $\Sigma'' = \{ar_a\} \cup \{ar_{ua}\}$ is a finite set of all requests including authorized or unauthorized, $dn'' = \{permissiongranted, permissiondenied\}$. Thus, p'' reduces to resultant attack probability p''' as

$$p''' = p'' - (1 - f_{Dac})p'' \tag{4.18}$$

where f_{Dac} is authorization failure rate, depending on unencrypted rules or default root permission etc. and calculated as

$$f_{Dac} = 1 - (\frac{\text{number of detected malicious access requests}}{\text{total malicious access requests}}) \tag{4.19}$$

Hence, RI is proportionally reduced to $\overline{RI}$ after applying the aforementioned preventive measures.

$$\overline{RI} = p''' \times L \tag{4.20}$$

4.2.2 Responsive Measures

Responsive measures detect and respond to attacks that have successfully passed through the applied preventive measures and can abuse the system.

4.2.2.1 Intrusion Detection and Response Layer

This layer works to reduce the attack impact and manual recovery rate using anomaly based intrusion Detection and Response System (IDRS) at the host level including sensor/actuator, controller nodes and communication channel. Host intrusion detector module periodically activates after t_d time to monitor the system state where $t_d < \delta t$. Detection measure based on local monitoring compares if the deviation of compromised system attribute values $C_{s_{ta}}$ from nominal operational values $N_{s_{ta}}$ is greater than the specified threshold Th to detect an active attack

$$|N_{s_{ta}} - C_{s_{ta}}| > Th \tag{4.21}$$

and

$$ta' = \int_{ts}^{td} (ta - \omega(t_d))dt \tag{4.22}$$

The setting of the activation interval parameter t_d affects the attack impact significantly. On attack detection, intrusion response module responds as follows

$$\tilde{\omega}(t_d) = \omega(t_d) \times (1 - (1 - f_{D_r})) \tag{4.23}$$

where $\tilde{\omega}(t_d)$ is resultant impact function and f_{D_r} is failure rate of detection-response estimated as

$$f_{D_r} = \frac{\text{number of undetected and unresponded attacks}}{\text{number of actual attacks}} \tag{4.24}$$

Response action stops when $\tilde{\omega}(t_d) = 0$ and $ta' = ta$. IDRS selects a set of reactive responses according to identified abuse attack type as mentioned in TABLE 4.1. If IDRS fails to detect and respond to the disruptive attack, manual recovery starts. It is worth mentioning that we have selected the firewalls, authentication and authorization mechanism as preventive mechanisms and intrusion detection and response as reactive mechanism and analyzing its joint effect for defending against the network and host level vulnerabilities. To demonstrate the applicability of the proposed idea, the three preventive security measures (perimeter protection, authentication, access control) and one responsive security measure are considered. The same idea can be used for other relevant security measures according to vulnerabilities and threat model of target system as well.

4.3 Proof of Concept

This section models the dynamic behavior of SC-CPS under normal condition and under cyber attack using GSPN. In NPP, control network consists of several subsystems for different critical operations like the Digital feedwater control system (DFWCS), Reactor core isolation cooling system (RCICS), Emergency response system. Here, we have considered the study of DFWCS developed by NUREG/CR-6942

TABLE 4.1: IDRS responses

Abuse attack	**IDRS responses**
Integrity	isolating compromised node, using freeze values, use of redundant nodes.
DoS	blacklisting/ blocking the IP of suspicious, limiting the incoming packet rates, switch to alternate source to provide service, restating firewalls with updated rules.

[5] discussed in section 3.3 to analyze the impact of applying preventive defense measures on the attack probability. Because both preventive and responsive measures are applied, we are demonstrating the combined effect on control node disturbance and manual recovery probability in the proof of concept.

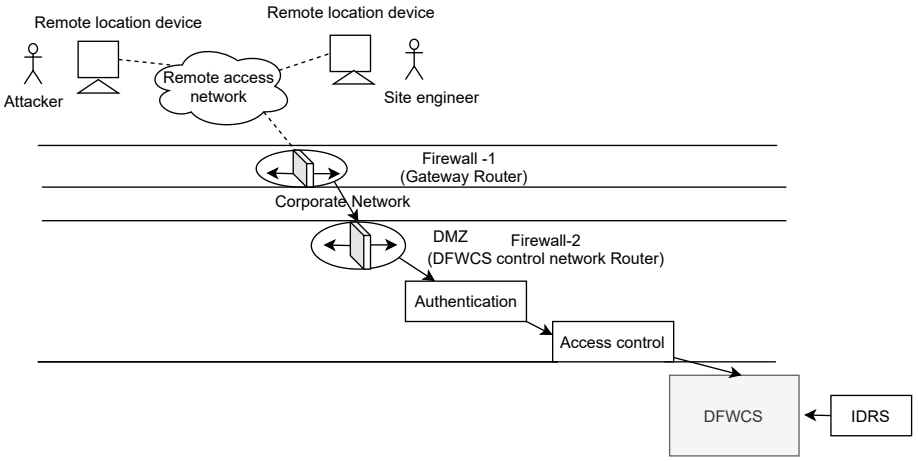

FIGURE 4.2: Applied preventive and responsive defense measures on DFWCS

TABLE 4.2: Place Description of Figure 4.3

Place	**Description**
P0	SG Feed water in normal range
P1	Water level out of range
P2	Comparative diagnosis completed
P3	MC signal interpreted by MFV controller
P4	MC signal interpreted by FP controller
P5	MFV Position adjusted
P6	FP speed increased

TABLE 4.3: Transition Description of Figure 4.3

Transition	**Description**
T0	Feed water level starts decreasing
T1	Level sensors sending the observed value to MC
T2	MC sending control directives to MFV and FP controllers
T3	MFV controller signals MFV to adjust position
T4	FP controller signals FP to increase speed
T5	Increasing feed water flow to maintain feed water level

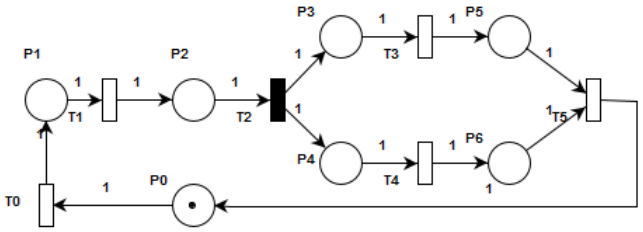

FIGURE 4.3: GSPN model of DFWCS functionality

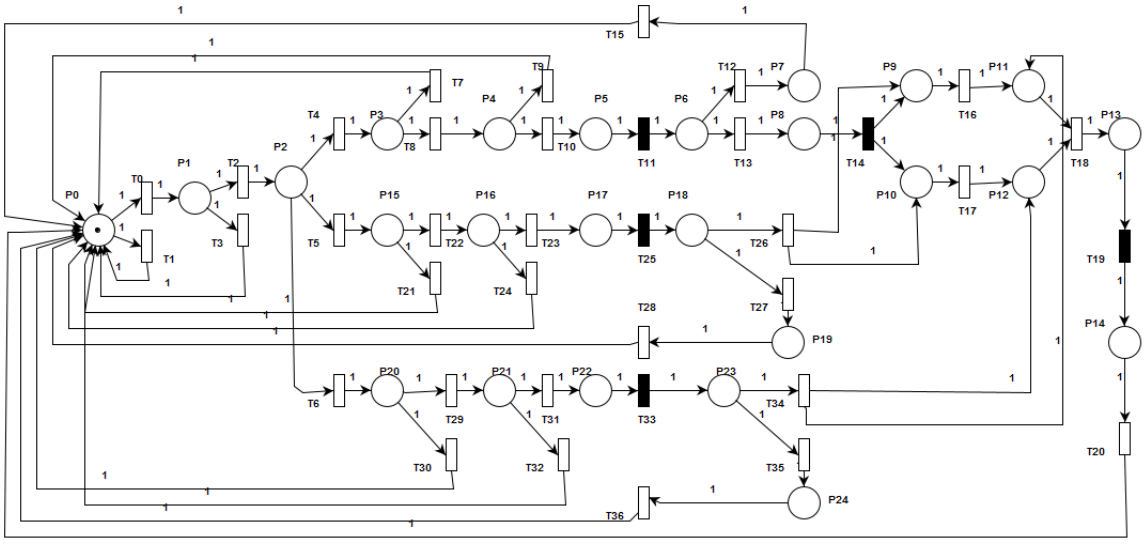

FIGURE 4.4: GSPN model of DFWCS under attack and defense

4.3.1 DFWCS Security Modeling

We have modelled the corresponding functionality using GSPN in FIGURE 4.3 as a functional model. Here, for the sake of simplicity, only the level sensor values are modeled as environment input parameter for MC to carry out comparative diagnostic. The description of places and transitions of FIGURE 4.3 is given in TABLE 4.2 and TABLE 4.3 respectively. The token at place P_0 represents that initially SG feed water is in a normal range. When feed water level starts decreasing, transition T_0 fires and the system transit from normal state P_0 to water level out of range state P_1. Firing of T_1 shows that level sensors send the value to MC, as a result token at P_2 shows that MC performs comparative diagnostic of received value with setpoints. Firing of transition T_2 reflects that MC sends control directives to MFV

and FP controllers to adjust their position and speed respectively. These signals are interpreted by MFV and FP controller and represented by deposit of tokens at P_3 and P_4. The MFV position is adjusted and FP speed is increased which is represented by token at P_5 and P_6 after firing of transitions T_3 and T_4 respectively. Firing of transition T_5 shows the increase in flow of feedwater supply that results in maintaining its initial state P_0.

We analyze the dynamic behavior of DFWCS in presence of attack and applied security measures as shown in FIGURE 4.2. The attacker may try to abuse the system and force it to transit into undesired states such as feed water outage or reactor trip using different ways including compromising sensors, compromising MC/BC, or compromising field controllers like FPC, MFVC. For instance, in FIGURE 4.7 and FIGURE 4.8 demonstrates the impact on level sensor values under integrity attack and DoS attack respectively which affect the level sensors reading $x(t)$ as defined in equations 3.6 and 3.7. The X-axis denotes time and Y-axis denotes water level (x).

TABLE 4.4: Place Description of Figure 4.4

Place	**Description**
P0	Intrusion attempt starts on enterprise LAN
P1	Enterprise LAN intruded
P2	DFWCN intruded
P3	Level sensor identified as attack surface or target
P4	Successful login to sensor node
P5	Permission granted to execute malicious payload
P6	Level sensor abused
P7	Attack detected and alert generated
P8	MC processed manipulated data
P9	Incorrect MC signals interpreted by MFV controller
P10	Incorrect MC signals interpreted by FP controller
P11	MFV position not adjusted
P12	FP speed not increased
P13	Water level decreased
P14	Reactor trip
P15	MC identified as attack surface
P16	Successful login to MC
P17	Permission granted to execute malicious payload
P18	MC abused
P19	Attack detected and alert generated
P20	Field controllers identified as attack surface
P21	Successful login on field controllers
P22	Permission granted to execute malicious payload
P23	FP and MFV controllers abused
P24	Attack detected and alert generated

TABLE 4.5: Transition Description of Figure 4.4

Transition	**Description**
T0	Enterprise firewall fails to prevent intrusion attack
T1	Enterprise firewall detects intrusion attempt and redirecting to enterprise firewall interface
T2	DFWCN firewall fails to prevent intrusion attack
T3	DFWCN firewall detects intrusion attempt and redirecting to enterprise firewall interface
T4	Listing the sensor nodes as attack target
T5	Identify MC node as attack target Attacker fails to intrude the authentication layer
T6	Listing the controller nodes as attack target
T7	Fails to intrude the authentication layer at sensor node
T8	Cracking the sensor node authentication successfully
T9	Fails to escalate privileges
T10	Escalating privileges to administrative level to install and execute payload fail to abuse level sensor
T11	Performing integrity/ DoS attack successfully to abuse level sensor
T12	IDRS detects the attack on sensor
T13	level sensor sending incorrect value to MC as IDRS fails to detect the attack
T14	MC sending control directives to MFV and FP controllers based on manipulated sensor data
T15	Responding the attack accordingly
T16	MFV controller do not signal MFV to adjust position
T17	FP controller do not signal FP to increase speed
T18	feed water flow not increasing to maintain water level
T19	Responding the attack
T20	Manual recovery starts
T21	Responding the attack
T22	Cracking the MC node authentication successfully
T23	Escalating privileges to install and execute payload at MC
T24	Fails to escalate privileges
T25	Performing integrity/ DoS attack successfully to abuse MC
T26	Fail to detect the attack on MC
T27	IDRS detects the MC attack
T28	responding attack by transferring computational responsibilities to BC
T29	Cracking the controller nodes authentication successfully
T30	Responding the attack
T31	Escalating privileges to install and execute payload at FP and MFV controllers
T32	Fails to escalate privileges
T33	Performing integrity/ DoS attack successfully to abuse level sensor
T34	Fail to detect the attack on MFV and FP
T35	IDRS detects attack on MFV and FP
T36	Responding the attack accordingly

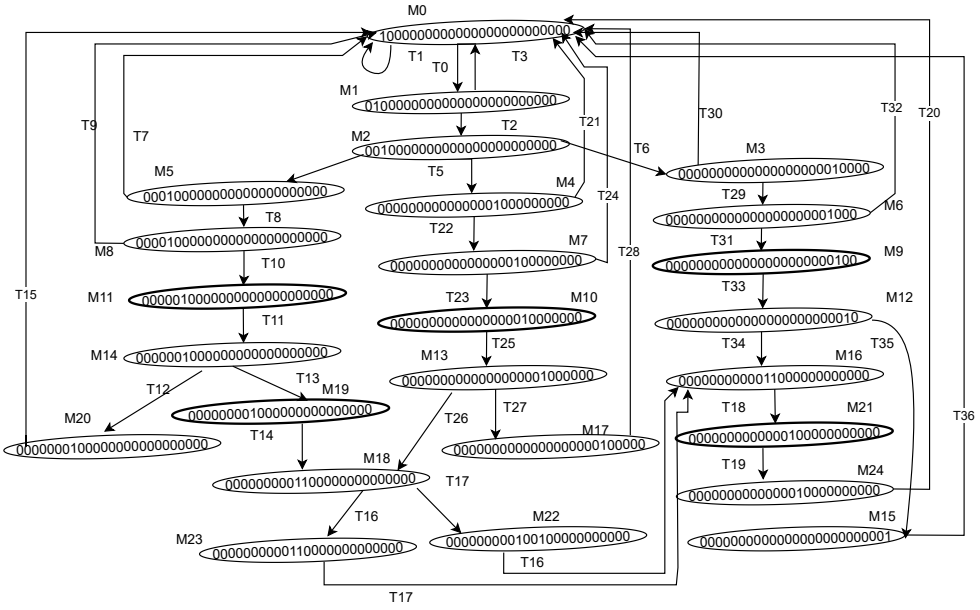

FIGURE 4.5: Reachability graph of FIGURE 4.4

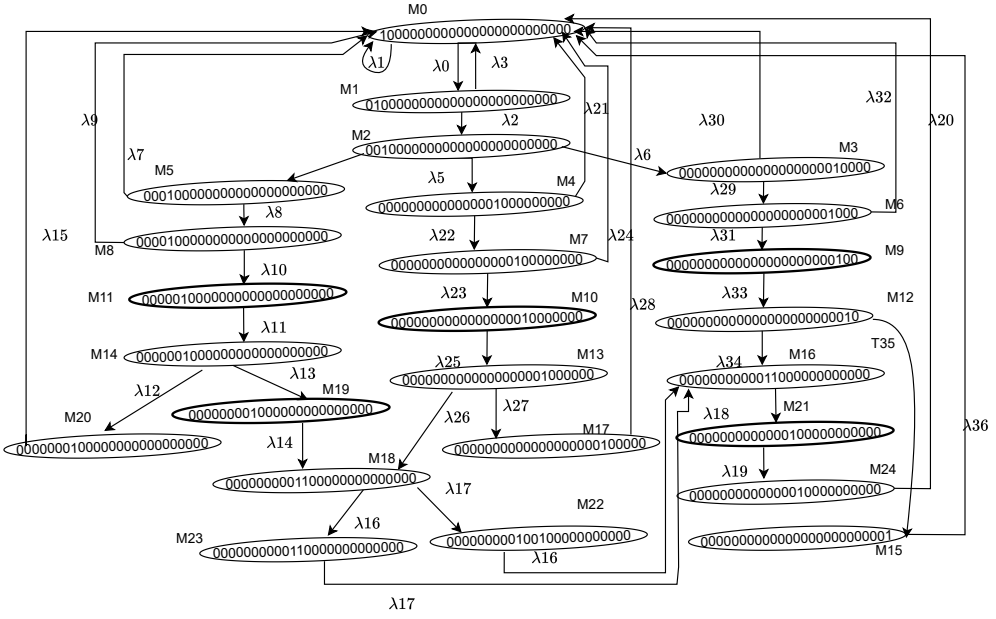

FIGURE 4.6: EMC generated from reachability graph of FIGURE 4.4

For additive integrity attack, we assume the random values for disturbance factor $\sigma'(\delta t) = 0.5$ and the attack start time as $t = 3.2$ time unit, which alter the values of x to x' from $t = 3.2$ onwards. In FIGURE 4.8 DoS attack starts at $t = 4.2$ time unit and results in loss of sensor signal value x. Although, the presence of different protection measures at network and host-level reduces the probability of successful

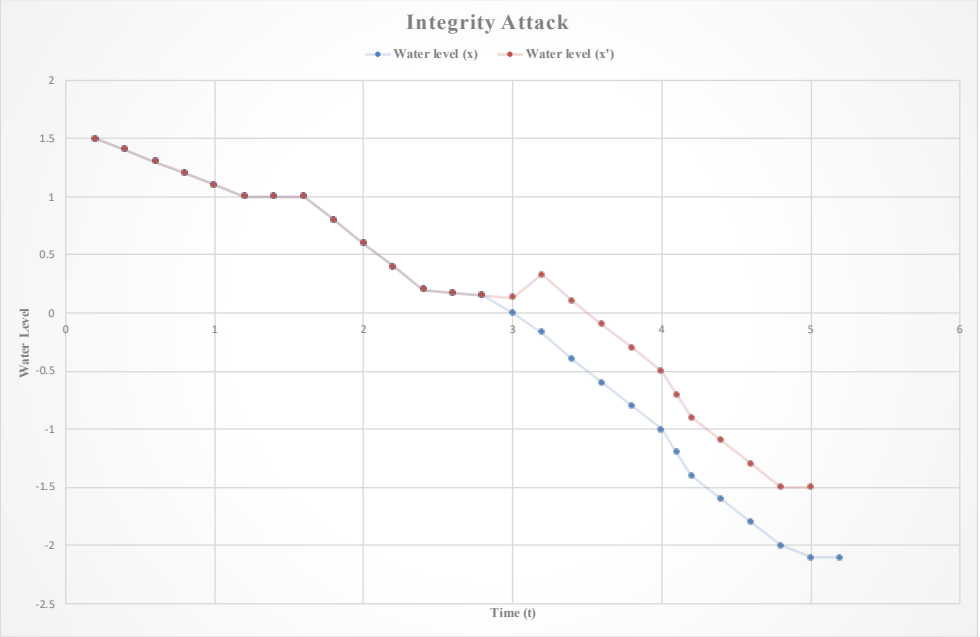

FIGURE 4.7: Integrity Attack (IA) on level sensor

intrusion and its impact or atleast they delay the disruption attacks (depending on defense layer strength). The perimeter protection layer consists of two firewalls, one at the enterprise level and the other at the DFW Control Network (DFWCN), each enriched with list of network accessing rules to create a Demilitarized Zone (DMZ).

TABLE 4.6: Impact of attack

Time(t)	0.2	0.4	0.6	0.8	1	1.2	1.4	1.6	1.8
x	1.5	1.4	1.3	1.2	1.1	1	1	1	0.8
x'_{IA}	1.5	1.4	1.3	1.2	1.1	1	1	1	0.8
x'_{DoS}	1.5	1.4	1.3	1.2	1.1	1	1	1	0.8
Time(t)	2	2.2	2.4	2.6	3	3.2	3.4	3.6	3.8
(x)	0.6	0.4	0.2	.17	.15	0	-.17	-.4	-.6
x'_{IA}	0.6	0.4	0.2	.17	.15	0	.33	.1	-.1
x'_{DoS}	0.6	0.4	0.2	.17	.15	0	-.17	-.4	-.6
Time(t)	4.0	4.1	4.2	4.4	4.6	4.8	5.0	5.2	
(x)	-.8	-1	-1.2	-1.4	-1.6	-1.8	-2	-2.1	
x'_{IA}	-.3	-.5	-.7	-.9	-1.1	-1.3	-1.5	-1.5	
x'_{DoS}	-.8	-1	-1.2						

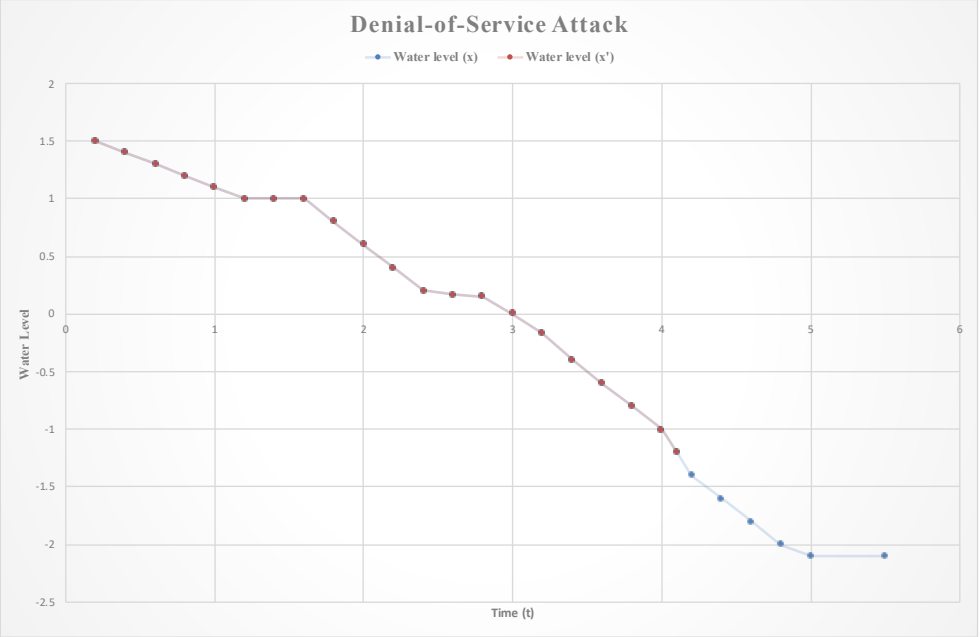

FIGURE 4.8: DoS Attack on level sensor

Authentication and access control layers provide a host-level defense. The IDRS periodically analyses the behavior of computing and monitoring nodes in the control network and responses according to the type of abuse attacks.

4.3.2 Quantitative Evaluation

To quantitatively evaluate the impact of security measures on attack probability of networked DFWCS functional workflow, GSPN is constructed (referring to FIGURE 4.2 and FIGURE 4.3) and shown in FIGURE 4.4. As this is a safety-critical system with high-level security requirements, access failure at any defense layer demands user verification from the initial state to access the functional workflow of DFWCS. The places and transitions of the GSPN model are mentioned in TABLE 4.4 and TABLE 4.5. Token at place P_0 models the attacker starts intrusion attempt by sending access request to enterprise firewall, when system in normal state and all

nodes are working as per specification . This enables timed transitions T_0 and T_1, out of which anyone transition may fire depending upon the transition rates. Transition T_0 fires when the enterprise firewall allows the malicious packets (requests) to connect the enterprise network. T_1 fires when it identifies the intrusion attempt and rejects the request. Token at place P_1 denotes that after intruding enterprise firewall, the attacker tries to penetrate the DFWCN firewall to access the control network. This enables timed transition T_2 and T_3. T_2 fires when the attacker successfully exploits the vulnerabilities of DFWCN firewall rules and intrude it and T_3 fires to deny the access request. The firing of T_2 deposits the token at place P_2, which represents the control network firewall intruded. The attacker tries to scan and list the sensors or main and backup computers or field controllers to identify the host-level vulnerabilities by firing any of the timed transition T_4, T_5, T_6. Hence, they use them as attack surfaces to disturb the functional workflow of DFWCS . The token at place P_3 denotes the level sensor node is identified as target, which leads to two possibilities i.e. enabling T_7 or T_8. The firing of T_8 denotes the attacker deceives the authentication mechanism of level sensor node, and the token deposited into place P_4 to represent the authentication is compromised, while the firing of T_7 denotes the attacker fails to bypass the authentication process and redirect to the enterprise firewall interface to restart the intrusion process again. After compromising the authentication measure, the attacker attempts to authorize its malicious actions. Once the token is deposited at P_4, either timed transition T_{10} fires to denote either the attacker successfully escalates the privileges to execute payload and deposits the token at place P_5 which shows the privilege escalated or transition T_9 fires to represent attacker fails to compromise authorization measures at level sensor node. After defeating all the preventive level, the firing of immediate transition T_{11} represents the immediate installation to perform either integrity or DoS attack to disrupt the control center or sensors. Token at P_6 models the level sensor is abused. Firing of T_{12} represents IDRS detects the attack and deposits token at P_7 to show alert generated state which requires firing of transition T_{15} for starting recovery process to avoid any unwanted state and bring back the system in normal state. The firing of T_{13} represents sending incorrect values to MC as IDRS fails

to detect the level sensor node is compromised and results in deposit of token at P_8 which shows MC processed the manipulated data received from compromised sensor. As a result it could not detect the actual status that feed water is low. It sends the control directives to MFV and FP controllers remain in their current position by firing transition T_{14}. As a result, token deposits at P_9 and P_{10} that represents incorrect MC signals interpreted by MFV and FP controller respectively. As a result firing of T_{16} and T_{17} shows MFV and FP controllers do not signal the MFV and FP to adjust the position and speed respectively. Token at P_{11} and P_{12} shows MFV position is not adjusted and FP speed is not increased. Hence, T_{18} fires and token deposited at P_{13} represents the feed water is decreased at critical level. As NPP is safety-critical system where safety measures are applied to handle the unexpected safety conditions, hence system transit into state P_{14} where reactor is tripped to be in fail-secure mode. The token at place P_{15} denotes the MC/BC node is identified as target while token at P_{20} denotes field controllers (MFVC, and FPC) are selected as targets to compromise. The token at P_{16} and P_{17} represents host level security measures are bypassed at MC including authentication and authorization level security failure by firing T_{22} and T_{23}. As a result token is deposited at P_{18} which shows MC is compromised and it sends incorrect control directives to MFV and FP controllers by firing T_{26}. While firing of T_{27} shows IDRS detects the attack and move token at place P_{19} to represent alert is generated which enables the transition T_{28} to respond attack by transferring computational responsibilities to BC and recover MC to take the system in at P_0. Similarly, the token at P_{21} and P_{22} represents host level security at MFVC and FPC is bypassed including authentication and authorization level security failure by firing T_{29} and T_{31}. As a result token is deposited at P_{23} which shows MFVC and FPC are compromised. firing T_{34} represents the MFVC and FPC send incorrect control directives to MFV and FP by depositing token at P_{11} and P_{12}. Firing of T_{35} shows IDRS at field controllers detects the attack and deposit token at place P_{24} to represent alert is generated which enables the transition T_{36} to respond attack by starting recovery process to take the system in at P_0.

To evaluate the impact of security measures, we carry out the sensitivity analysis. For this, the reachability graph and EMC of the constructed GSPN in FIGURE 4.4 is generated and shown in FIGURE 4.5 and FIGURE 4.6 with the set of 20 tangible states $\{ M_0, M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8, M_{12}, M_{13}, M_{14}, M_{15}, M_{16}, M_{17}, M_{18}, M_{20}, M_{22}, M_{23}, M_{24}\}$ and 5 vanishing state $\{ M_9, M_{10}, M_{11}, M_{19}, M_{21}\}$. The transition rates are the parameters assigned to each directed edge among the states generated through corresponding transition in FIGURE 4.6. The strength of respective defense measures S_{Dj} is represented as firing rate of timed transitions of FIGURE 4.4. The firing delay of respective transitions of FIGURE 4.4 at each run is calculated as $(MST_{Ti} = 1/\lambda_{Ti})$

Firing weight is assigned to show the priority among timed transitions. The firing probability of transitions shows the probability of transiting from one state to another. These transition probabilities are embedded in transition probability matrix **P** as

$$\mathbf{P} = \mathbf{A} + \mathbf{B} = \begin{pmatrix} C & D \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ E & F \end{pmatrix}$$

where,

$C = (c_{jk}) = P[M_j \rightarrow M_k; M_j, M_j \in \tilde{V}]$

$D = (d_{jk}) = P[M_j \rightarrow M_k; M_j \in \tilde{V}, M_j \in \tilde{T}]$

$E = (e_{jk}) = P[M_j \rightarrow M_k; M_j \in \tilde{T}, M_j \in \tilde{V}]$

$F = (f_{jk}) = P[M_j \rightarrow M_k; M_j \in \tilde{T}, M_j \in \tilde{T}]$

In our model, matrix **P** of dimensions 25×25 is obtained where, the dimension of C is 5×5, D is 5×20 , E is 20×5, F is 20×20. The columns and rows are sorted as marking $M_9, M_{10}, M_{11}, M_{19}, M_{21}, M_0, M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8, M_{12}, M_{13}, M_{14}, M_{15}, M_{16},$

$$\mathbf{P} = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T25} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T14} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T19} \\
0 & 0 & 0 & 0 & 0 & p_{T1} & p_{T0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T3} & 0 & p_{T2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T5} & p_{T6} & p_{T4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T30} & 0 & 0 & 0 & 0 & 0 & p_{T29} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T21} & 0 & 0 & 0 & 0 & 0 & 0 & p_{T22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T7} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T31} & 0 & 0 & 0 & 0 & p_{T32} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & p_{T23} & 0 & 0 & 0 & p_{T24} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & p_{T10} & 0 & 0 & p_{T9} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T35} & p_{T34} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T27} & p_{T26} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & p_{T13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T12} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T36} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & p_{T18} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T28} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T17} & p_{T16} & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T15} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T16} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T17} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & p_{T20} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

$$\tilde{\mathbf{P}} = \begin{pmatrix}
p_{T1} & p_{T0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T3} & 0 & p_{T2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & p_{T5} & p_{T6} & p_{T4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T30} & 0 & 0 & 0 & 0 & 0 & p_{T29} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T21} & 0 & 0 & 0 & 0 & 0 & 0 & p_{T22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T7} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T32} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T31} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T24} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T23} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T9} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T35} & p_{T34} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T27} & p_{T26} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T13} & p_{T12} & 0 & 0 & 0 \\
p_{T36} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T18} \\
p_{T28} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T17} & p_{T16} & 0 \\
p_{T15} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T16} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{T17} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p_{T20} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

$M_{17}, M_{18}, M_{20}, M_{22}, M_{23}, M_{24}$. First row of P denotes the transition probability from M_9 to $M_9, M_{10}, M_{11}, M_{19}, M_{21}, M_0, M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8, M_{12}, M_{13}, M_{14}, M_{15}$,$M_{16}, M_{17}, M_{18}, M_{20}, M_{22}, M_{23}, M_{24}$. Similarly, for other rows it can be understood.

To evaluate the performance of proposed model, the steady state probabilities $\tilde{\pi}$ of EMC is given as [9]

$$\pi_j = \begin{cases} \tilde{\pi} P = \tilde{\pi}, \\ \sum_{M_i \in \tilde{T} \cup \tilde{V}} \tilde{\pi}_s = 1 \end{cases} \tag{4.25}$$

The transition probability matrix P of EMC is further reduced to $\tilde{P}$ by removing vanishing marking $\tilde{V}$ and considering the tangible marking $\tilde{T}$ only as [9]

$$\tilde{P} = F + E \times (I - C)^{-1} \times D \tag{4.26}$$

where I is identity matrix. The dimension of $\tilde{P}$ is reduced into 20×20 by removing vanishing marking $\{M_9, M_{10}, M_{11}, M_{19}\}$ corresponding to immediate transitions $\{T11, T25, T33, T14, T19\}$ and considering the tangible marking set $\{M_0, M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8, M_{12}, M_{13}, M_{14}, M_{15}, M_{16}, M_{17}, M_{18}, M_{20}, M_{22}, M_{23}, M_{24}\}$. The steady state probability distribution $\tilde{\pi}$ of REMC is obtained using [9]

$$\tilde{\pi} = \begin{cases} \tilde{\pi}\tilde{P} = \tilde{\pi}, \\ \sum_{M_i \in \tilde{T} \cup \tilde{V}} \tilde{\pi}_s = 1 \end{cases} \tag{4.27}$$

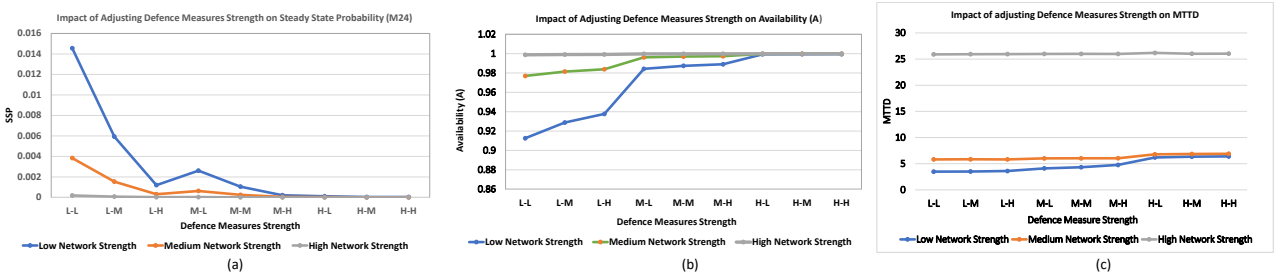

FIGURE 4.9: Impact of adjusting defense strength on security evaluation metrics

The steady-state probabilities π of GSPN is calculated, which is a fraction of time a process spends in marking M_j by weighting $\tilde{\pi}$ with the sojourn time of its respective marking. Each π_j is computed as a ratio of mean sojourn time of M_j and mean cycle time [9]

$$\pi_j = \begin{cases} \frac{\tilde{\pi}_j \times 1/(\sum_{k:t_k \in EN(M_j)} \lambda_k)}{\sum_{M_s \in \tilde{T}} \tilde{\pi}_s \times 1/(\sum_{k:t_k \in EN(M_s)} \lambda_k)} & if M_j \in \tilde{T} \\ 0, & if M_j \in \tilde{V} \end{cases} \tag{4.28}$$

To perform sensitivity analysis for evaluating and comparing steady state probabilities, we vary the strength of preventive measures and responsive measures (at network and host level) and analyze its effect on model evaluation metrics including steady state probability, MTTD and system availability. In each run, while calculating steady state probabilities $\tilde{\pi}$, the firing rates of the transitions that models the attack propagation is kept constant. Hence, for these transitions the corresponding firing rates $\lambda_4 = \lambda_5 = \lambda_6 = 1$, $\lambda_{15} = \lambda_{16} = \lambda_{17} = \lambda_{18} = \lambda_{20} = \lambda_{28} = \lambda_{36} = 1$. However,

TABLE 4.7: Effect of readjustment of mitigation strength on performance metrics

S_{Df}	S_{Dh}	S_{Dr}	π_0	π_1	π_2	π_3	π_4	π_5	π_6	π_7	π_8	π_9	π_{10}	π_{11}	π_{12}	π_{13}
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	.4660	.2330	.0388	.0388	.0388	.0388	.0194	.0194	.0194	0	0	0	.0097	.0097
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .8$	.4743	.2371	.0395	.0395	.0395	.0395	.0197	.0197	.0197	0	0	0	.0098	.0098
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .96$	.4788	.2394	.039	.0399	.0399	.0399	.0199	.0199	.0199	0	0	0	.0099	.0099
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	.5226	.2613	.0435	.0435	.0435	.0435	.0087	.0087	.0087	0	0	0	.0017	.0017
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .8$	.5243	.2621	.0437	.0437	.0437	.0437	.0087	.0087	.0087	0	0	0	.0017	.0017
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .96$	.5251	.2626	.0437	.0437	.0437	.0437	.0087	.0087	.0087	0	0	0	.0017	.0017
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	.5421	.2710	.0452	.0452	.0452	.0452	.0018	.0018	.0018	0	0	0	7×10^{-5}	7×10^{-5}
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .8$	.5422	.2711	.0452	.0452	.0452	.0452	.0018	.0018	.0018	0	0	0	7×10^{-5}	7×10^{-5}
$\lambda_1 = \lambda_3 = .8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	.7672	.1534	.0102	.0102	.0102	.0102	.0051	.0051	.0051	0	0	0	.0025	.0025
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.77081	.15416	.01028	.01028	.01028	.01028	.00514	.00514	.00514	0	0	0	.00257	.00257
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .96$	.77272	.15454	.0103	.0103	.0103	.0103	.00515	.00515	.00515	0	0	0	.00258	.00258
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.78981	.15796	.01053	.01053	.01053	.01053	.00211	.00211	.00211	0	0	0	.00042	.00042
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.79041	.15808	.01054	.01054	.01054	.01054	.00211	.00211	.00211	0	0	0	.00042	.00042
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	.79073	.15815	.01054	.01054	.01054	.01054	.00211	.00211	.00211	0	0	0	.00042	.00042
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.79673	.15935	.01062	.01062	.01062	.01062	.00042	.00042	.00042	0	0	0	.00002	.00002
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.79676	.15935	.01062	.01062	.01062	.01062	.00042	.00042	.00042	0	0	0	.00002	.00002
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.95773	.03831	.00051	.00051	.00051	.00051	.00026	.00026	.00026	0	0	0	.00013	.00013
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.95795	.03832	.00051	.00051	.00051	.00051	.00026	.00026	.00026	0	0	0	.00013	.00013
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	.95807	.03832	.00051	.00051	.00051	.00051	.00026	.00026	.00026	0	0	0	.00013	.00013
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.9591	.03836	.00051	.00051	.00051	.00051	.0001	.0001	.0001	0	0	0	.00002	.00002
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.95913	.03837	.00051	.00051	.00051	.00051	.0001	.0001	.0001	0	0	0	.00002	.00002
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	.95915	.03837	.00051	.00051	.00051	.00051	.0001	.0001	.0001	0	0	0	.00002	.00002
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.9595	.03838	.00050	.00050	.00050	.00050	.00002	.00002	.00002	0	0	0	1.0×10^{-6}	1.0×10^{-6}
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.95951	.03838	.00051	.00051	.00051	.00051	.00002	.00002	.00002	0	0	0	1.0×10^{-6}	1.0×10^{-6}
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	.95951	.03838	.00064	.00051	.00051	.00051	.00002	.00002	.00002	0	0	0	1.0×10^{-6}	1.0×10^{-6}

TABLE 4.8: Effect of readjustment of mitigation strength on performance metrics

S_{Df}	S_{Dh}	S_{Dr}	π_{14}	π_{15}	π_{16}	π_{17}	π_{18}	π_{19}	π_{20}	π_{21}	π_{22}	π_{23}	π_{24}	Avl	$MTTD$
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	.0097	.0048	.0145	.0048	.0048	0	.0048	0	.0048	.0048	.0145	.9126	3.49
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .8$	.0098	.0079	.0059	.0079	.00198	0	.0079	0	.0019	.0019	.0059	.9288	3.51
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .96$	.0099	.0095	.0012	.0095	.0004	0	.0095	0	.0004	.0004	.0012	.9377	3.60
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	.0017	.0008	.0026	.0008	.0008	0	.0008	0	.0008	.0008	.0026	.9843	4.11
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .8$	.0017	.0014	.0010	.0014	.0003	0	.0014	0	.0003	.0003	.0010	.9874	4.33
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .96$	.0017	0.0017	.0002	.0017	.00007	0	.0016	0	.00007	.00007	.0002	.9890	4.77
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	7×10^{-5}	4×10^{-5}	.0001	4×10^{-5}	4×10^{-5}	0	4×10^{-5}	0	4×10^{-5}	4×10^{-5}	.0001	.99936	6.2
$\lambda_1 = \lambda_3 = .5$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .8$	7×10^{-5}	6×10^{-5}	4×10^{-5}	6×10^{-5}	1×10^{-5}	0	6×10^{-5}	0	1×10^{-5}	1×10^{-5}	4×10^{-5}	.9994	6.35
$\lambda_1 = \lambda_3 = .8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .5$	.0025	.0012	.0038	.0012	.0012	0	.0012	0	.0012	.0012	.0038	.9769	5.83
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.00257	.00206	.00154	.00206	.00051	0	.00206	0	.00051	.00051	.00154	.98151	5.853
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = .96$	.00258	.00247	.00031	.00247	.0001	0	.00247	0	.0001	.0001	.00031	.98391	5.824
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.00042	.00021	.00063	.00021	.00021	0	.00021	0	.00021	.00021	.00063	.99622	6.02
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.00042	.00034	.00025	.00034	.00008	0	.00034	0	.00008	.00008	.00025	.99698	6.04
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	.00042	.0004	.00005	.0004	.00002	0	.0004	0	.00002	.00002	.00005	.99737	6.05
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.00002	.00001	.00003	.00001	.00001	0	.00001	0	.00001	.00001	.00003	.99982	6.8
$\lambda_1 = \lambda_3 = 0.8$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.00002	.00001	.00001	.00001	.000001	0	.00001	0	.000001	.000001	.00001	.99985	6.86
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	0.00013	0.00006	0.00019	0.00006	0.00006	0	0.00006	0	0.00006	0.00006	0.00019	0.99886	25.90
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.00013	.0001	.00008	.0001	.00003	0	.0001	0	.00003	.00003	.00008	.99909	25.93
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.5$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	.00013	.00012	.00002	.00012	.00001	0	.00012	0	.00001	.00001	.00002	.99921	25.94
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	.00002	.00001	.00003	.00001	.00001	0	.00001	0	.00001	.00001	.00003	.9998	25.97
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	.00002	.00002	.00001	.00002	.000001	0	.00002	0	.000001	.000001	.00001	.99984	25.98
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = 0.8$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	.00002	.00002	.000001	.00002	.000001	0	.00002	0	.000001	.0000015	.000001	.99986	25.98
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.5$	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	0	1.0×10^{-7}	0	1.0×10^{-6}	1.0×10^{-6}	1.3×10^{-6}	.9999	26.026
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.8$	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	0	1.0×10^{-7}	0	1.0×10^{-6}	1.0×10^{-6}	1.2×10^{-6}	.99996	26.026
$\lambda_1 = \lambda_3 = 0.96$	$\lambda_7 = \lambda_9 = \lambda_{21} = \lambda_{24} = \lambda_{30} = \lambda_{32} = .96$	$\lambda_{12} = \lambda_{27} = \lambda_{35} = 0.96$	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	0	1.0×10^{-7}	0	1.0×10^{-6}	1.0×10^{-6}	1.0×10^{-6}	.99996	26.03

the transition rates of corresponding malicious transitions that represents the failure rate of different defense measures $\lambda_0, \lambda_2, \lambda_8, \lambda_{10}, \lambda_{13}, \lambda_{22}, \lambda_{23}, \lambda_{26}, \lambda_{29}, \lambda_{31}, \lambda_{34}$ are varied systematically. The corresponding transition rates that represents the success rate (strength) of different defense measures $\lambda_1, \lambda_3, \lambda_7, \lambda_9, \lambda_{12}, \lambda_{21}, \lambda_{24}, \lambda_{27}, \lambda_{30}, \lambda_{32}, \lambda_{35}$ also varies accordingly to analyze its impact on security metrics (steady state probabilities, MTTD and availability). It is assumed that the strength of defense measures {L, M, H} is represented with value range {0.1-0.5, 0.51-0.8, 0.81-1.0} respectively in the interval [0.1, 1]. As an exhaustive analysis is performed and due to limited page length, the results can not be shown in a single table. We split the table into two parts and show the analysis in TABLE 4.7 and TABLE 4.8. TABLE 4.7 lists the steady state values from π_0 to π_{13}; In the continuation, TABLE 4.8 lists the remaining the steady state values from π_{14} to π_{24}, availability (A) and MTTD corresponding to different values of defense measures. For instance, when the strength of network level defenses is kept fix, the strength of host level preventive defense (authentication & authorization) and reactive defense (IDRS) are varied *i.e.* when the enterprise and control network level firewalls are fixed at high strength represented as $S_{Df1} = \lambda_1 = .96, S_{Df2} = \lambda_3 = .96$ then the strength of host level defense and IDRS at each nodes are varied as {low (L), medium (M), high (H)} to analyze the effect of high strength network level defenses.

TABLE 4.9: Comparative study

Research work	**Vulnerabilities handled**
[133]	Presented firewall and password model, although access control vulnerabilities are not considered. Moreover, no responsive actions are taken that affect the system availability by limiting the impact of successful disruption.
[28]	Proposed firewall and password model, although access control vulnerabilities are not considered which are critical for SC-CPS. Moreover, repair actions are taken after disruption but no provisions made for responsive actions.
[96]	Presented intrusion detection model to detect and respond to the attack that has already damaged the system nodes. However, no provisions are discussed to prevent the intrusion attempts.
[138]	Presented anomaly based intrusion detection model to detect and respond to the attack on NPP. However, no provisions are applied to hardening the protection and resist the intrusion attacks.
Proposed approach	models and analyzes the impact of preventive and responsive measures both.

For comparative analysis, we have fixed the strength of defense measures {L, M, H} as value {0.5, 0.8, .96} respectively, for the purpose of illustration for all cases. Here, we compute and analyze the impact on security metrics when the strength of defense measures is considered [H, H, H] at network layer S_{Df}, at host layer S_{Dh} and responsive measures S_{Dr} respectively, as listed in TABLE 4.7 and TABLE 4.8. S_{Df} considers S_{Df1} and S_{Df2}, S_{Dh} includes S_{Da_s}, S_{Dac_s}, S_{Da_mc}, S_{Dac_mc}, S_{Da_fc}, S_{Dac_fc} and S_{Dr} including $S_{Dr\_s}, S_{Dr\_mc}, S_{Dr\_fc}$. The transition probabilities corresponding to concerned transitions for matrix $\tilde{P}$ are calculated using equation (4.9) and (2.14) as

$p_{T0} = f_{Df1} = \lambda_0/(\lambda_0 + \lambda_1) = 0.04$ $p_{T1} = S_{Df1} = 1 - f_{Df1} = \lambda_1/(\lambda_0 + \lambda_1) = 0.96$, $p_{T2} = f_{Df2} = \lambda_2/(\lambda_2 + \lambda_3) = 0.04$, $p_{T3} = S_{Df2} = 1 - f_{Df2} = \lambda_3/(\lambda_2 + \lambda_3) = 0.96$, $p_{T4} = \lambda_4/(\lambda_4 + \lambda_5 + \lambda_6) = 1/3$, $p_{T5} = \lambda_5/(\lambda_4 + \lambda_5 + \lambda_6) = 1/3$, $P_{T6} = \lambda_6/(\lambda_4 + \lambda_5 + \lambda_6) = 1/3$, $p_{T7} = S_{Da\_s} = 1 - f_{Da\_s} = \lambda_7/(\lambda_7 + \lambda_8) = 0.96$, $p_{T8} = f_{Da\_s} = \lambda_8/(\lambda_7+\lambda_8) = 0.04$, $p_{T9} = S_{Dac\_s} = 1-f_{Dac\_s} = \lambda_9/(\lambda_9+\lambda_{10}) = 0.96$, $p_{T10} = f_{Da\_s} = \lambda_{10}/(\lambda_9 + \lambda_{10}) = 0.04$, $p_{T12} = S_{Dr\_s} = 1 - f_{Dr\_s} = \lambda_{12}/(\lambda_{12} + \lambda_{13}) = 0.96$, $p_{T13} = f_{Dr\_s} = \lambda_{13}/(\lambda_{12}+\lambda_{13}) = 0.04$, $p_{T21} = S_{Da\_mc} = 1-f_{Da\_mc} = \lambda_{21}/(\lambda_{21}+\lambda_{22}) = 0.96$, $p_{T22} = f_{Da\_mc} = \lambda_{22}/(\lambda_{21} + \lambda_{22}) = 0.04$, $p_{T23} = f_{Dac\_mc} = \lambda_{23}/(\lambda_{23} + \lambda_{24}) = 0.04$, $p_{T24} = S_{Dac\_mc} = 1-f_{Dac\_mc} = \lambda_{24}/(\lambda_{23}+\lambda_{24}) = 0.96$, $p_{T27} = S_{Dr\_mc} = 1-f_{Dr\_mc} = \lambda_{27}/(\lambda_{26} + \lambda_{27}) = 0.96$, $p_{T29} = f_{Da\_fc} = \lambda_{29}/(\lambda_{29} + \lambda_{30}) = 0.04$, $p_{T30} = S_{Da\_fc} = 1 - f_{Da\_fc} = \lambda_{30}/(\lambda_{29} + \lambda_{30}) = 0.96$, $p_{T31} = f_{Dac\_fc} = \lambda_{31}/(\lambda_{31} + \lambda_{32}) = 0.04$, $p_{T32} = S_{Dac\_fc} = 1-f_{Dac\_fc} = \lambda_{32}/(\lambda_{31}+\lambda_{32}) = 0.96$, $p_{T34} = f_{Dr\_fc} = \lambda_{34}/(\lambda_{34}+\lambda_{35}) = 0.04$ $p_{T35} = S_{Dr\_fc} = 1 - f_{Dr\_fc} = \lambda_{35}/(\lambda_{34} + \lambda_{35}) = 0.96$. and by using equation (4.27), we obtain the vector $\tilde{\pi} = [0.95951, 0.03838, 0.00051, 0.00051, 0.00051, 0.00051, 0.00002, 0.00002, 0.00002, 1.0\times10^{-6}, 1.0\times10^{-6}, 1.0\times10^{-6}, 1.0\times10^{-6}, 1.0\times10^{-6}, 1.0\times10^{-6}, 1.0\times10^{-6}, 1.0\times10^{-6}, 1.0\times10^{-7}, 1.0\times10^{-6}, 1.0\times10^{-6}]$. Using equation (4.28), the mean cycle time and steady-state probabilities (SSP) are calculated. The mean cycle time $= 0.95951\times(1.04+25)+0.03838\times(1.04+25)+0.00051\times(.33)+.00051\times(1.04+25)+.00051\times(1.04+25)+.00051\times(1.04+25)+.00002\times(1.04+25)+.00002\times(1.04+25)+.00002\times(1.04+25)+1.0\times10^{-6}\times(1.04+25)+1.0\times10^{-6}\times(1.04+25)+1.0\times10^{-6}\times(1.04+25)+1.0\times10^{-6}\times(1)+1.0\times10^{-6}\times(1)+1.0\times10^{-6}\times(1)+1.0\times10^{-6}\times(1)+1.0\times10^{-6}\times(1)+1.0\times10^{-7}\times(1)+1.0\times10^{-6}\times(1)+1.0\times10^{-6}\times(1) = 26.03$.

The SSP are obtained as
$\pi_0 = (0.9595\times(1.04+25))/26.03 = 0.9595$, $\pi_1 = (0.03838\times(26.04))/26.03 = 0.03838$, $\pi_2 = (0.00051 \times (.33))/26.03 = 0.00064$, $\pi_3 = (0.00051 \times (26.04))/26.03 = 0.00051$, $\pi_4 = (0.00051\times(26.04))/26.03 = 0.00051$, $\pi_5 = (0.00051\times(26.04))/26.03 = 0.00051$, $\pi_6 = (.00002 \times (26.04))/26.03 = 0.00002$, $\pi_7 = (.00002 \times (26.04))/26.03 = 0.00002$, $\pi_8 = (.00002 \times (26.04))/26.03 = 0.00002, \pi_9 = 0, \pi_{10} = 0, \pi_{11} = 0, \pi_{12} = (1.0 \times 10^{-6} \times (26.04))/26.03 = 1.0 \times 10^{-6}$, $\pi_{13} = (1.0 \times 10^{-6} \times (26.04))/26.03 = 1.0 \times 10^{-6}$, $\pi_{14} = (1.0\times10^{-6}\times(26.04))/26.03 = 1.0\times10^{-6}$, $\pi_{15} = (1.0\times10^{-6}\times(26.04))/26.03 = 1.0 \times 10^{-6}$, $\pi_{17} = (1.0 \times 10^{-6} \times (26.04))/26.03 = 1.0 \times 10^{-6}$, $\pi_{18} = (1.0 \times 10^{-6} \times (26.04))/26.03 = 1.0\times10^{-6}$, $\pi_{19} = 0$, $\pi_{20} = (1.0\times10^{-7}\times(26.04))/26.03 = 1.0\times10^{-7}$ $\pi_{21} = 0$, $\pi_{22} = (1.0 \times 10^{-6} \times (26.04))/26.03 = 1.0 \times 10^{-6}$ $\pi_{23} = (1.0 \times 10^{-6} \times (26.04))/26.03 = 1.0 \times 10^{-6}$ $\pi_{24} = (1.0 \times 10^{-6} \times (26.04))/26.03 = 1.0 \times 10^{-6}$;

which shows the intrusion-attack probability at M_0, M_1, $M_3 = M_4 = M_5$, $M_6 = M_7 = M_8$, $M_{12} = M_{13} = M_{14}$ and M_{18} is reducing after applying each preventive defense layer respectively. Whereas π_{24} shows that out of 10^6 intrusion-abuse attack attempts, only 1 attack can penetrate all the defensive measures and force the system to get in undesired state (or reactor trip condition) which is very less.

Using the steady-state probabilities, we calculate Mean time to disrupt as
$MTTD = \sum_{i=0}^{8} \pi_i \times MST_i = 26.03$
which shows the time to abuse increases on applying intrusion preventive measures. The steady-state availability is obtained by reducing the disrupted states probabilities

$Avl = 1 - \sum_{i=12}^{24} \pi_i$

$= 1 - .00004 = .99996.$
which shows that the effect of successful disruption on system availability is significantly less when the strength of the preventive measures is kept high. Similarly, the values of security metrics are calculated for all the defense strength combinations. The indicative graph is plotted and shown in FIGURE 4.9 corresponding to TABLE 4.7 and 4.8. The graph in FIGURE 4.9 (a) represents the impact of

defense strength S_{Df}, S_{Dh} and S_{Dr} on steady state probability of being in undesired state (or reactor trip condition) π_{24}, (b) impact of defense strength on Avl and (c) impact of defense strength on $MTTD$. For each graph, three cases are compared, (1) when the strength of network level defenses is fixed as low (L) *i.e* $S_{Df1} = \lambda_1 = .5, S_{Df2} = \lambda_3 = .5$, the strength of host level preventive defense and reactive defense (IDRS) are varied {L, M, H} to analyze the effect of adjusting the defense measures strength , (2) when the strength of network level defenses is fixed as medium (M) *i.e* $S_{Df1} = \lambda_1 = .8, S_{Df2} = \lambda_3 = .8$, the strength of host level preventive defense and reactive defense (IDRS) are varied {L, M, H} to analyze the effect of adjusting the defense measures strength (3) when the strength of network level defenses is fixed as high (H) *i.e* $S_{Df1} = \lambda_1 = .96, S_{Df2} = \lambda_3 = .96$, the strength of host level preventive defense and reactive defense (IDRS) are varied {L, M, H} to analyze the effect of adjusting the defense measures strength. In FIGURE 4.9 (a), Y-axis represents SSP(M_{24}) or π_{24} and X-axis represents different combinations of host level and responsive level defense strength. We observe that when defense measures strength combination is [L, L, L] or [.5,.5,.5], SSP is highest and when the strength combination is [H,H,H] or [.96,.96,.96], SSP is the lowest. Hence, when the network level defense strength increases, SSP reduces significantly, as shown. Moreover, SSP significantly depends on responsive measures strength. As if the attack is detected and responded with high strength, but the network and host level are low *i.e.*[L, L, H] as compared to when the responsive level is low but the network level is low and host level is medium *i.e.* [L, M, L], the SSP is comparatively lesser for [L, L, H]. Similarly, it can be observed when the defense strength is set [M, L, H] and [M, M,L]. In FIGURE 4.9 (b), Y-axis represents Availability (A) and X-axis represents different combinations of host level and responsive level defense strength. It can be observed that as the strength of preventive and responsive security measures increases, the system availability also improves. Availability is highest when defense measures strength is [H,H,H] or [.96,.96,.96] and is lowest when the strength combination is [L,L,L] or [.5,.5,.5]. It should be noted that if it is not possible to place high strength defense measures at network, host level and responsive level due to any reasons, at least either of the network level defense or host-level defense

measures should be strong, as shown in the graph where the availability is comparable for combinations [L, H, M], [L, H, H] and [M, M, L], [M, M, M] and [H, M, L] [H, M, M]. However, for defending against external attackers, the optimal results can be obtained if the network level defense is high that does not allow them to intrude in the network itself. In FIGURE 4.9 (c), Y-axis represents $MTTD$ and X-axis represents different combinations of host level and responsive level defense strength. It can be observed that as the strength of preventive and responsive security measures increases, the system MTTD also increases. $MTTD$ is highest when defense measures strength is [H,H,H] or [.96,.96,.96] and is lowest when the strength combination is [L,L,L] or [.5,.5,.5].

Hence, the proposed methodology is helpful to analyze the system behavior in the presence of attack and defenses and quantify the security attributes. Thus, the method can also compare the alternate security designs to estimate and reduce the overall cyber risk. It is worth noticing that the defense measures strength can be divided into closer ranges for deeper analysis.

4.3.3 Comparative Evaluation

A comparison with previous works is presented in TABLE 4.9 that shows the proposed security model analyses more system level vulnerabilities to guard against exploitations.

4.4 Summary

To disrupt a CPS successfully, the attacker first intrudes into the system and then disrupts the physical process by abusing the process and control parameters. We have presented a GSPN based modeling approach to analyze the dynamic behavior of the cyber-physical system in the presence of attack and sequence of defenses. Specifically, it analyzes the effect of integrating multilevel preventive and responsive measures on security metrics, including steady state probability of system being in

an undesired state, mean time to disrupt, and system availability. As a case study, security of an NPP subsystem is investigated. The quantitative result shows that the number of security measures, their strength and attack detection interval play a significant role in reducing the probability of disruption and increasing system availability. The quantitative models presented in the previous chapter and this chapter model the cyber attacks and analyses the impacts of security measures for CPSs. However, some interesting research questions arise, such as how to organize the security with functionality? What can be the possible architectural arrangement for this? In this scenario, who will take the responsibility of managing functionality and security needs. Chapter 5 deals with these research questions. After considering the system model and understanding developed at the modeling level, we will consider how to model security at the architectural level in the next chapter.