Optimization of Cybersecurity Investment Strategies in the Smart Grid Using Game-Theory

Burhan Hyder, *Student Member, IEEE*, and Manimaran Govindarasu, *Fellow, IEEE*

***Abstract*—With the increasing penetration of cyber systems in the power grid, it is becoming increasingly imperative to deploy adequate security measures all across the grid to secure it against any kind of cyber threat. Since financial resources for investment in security are limited, optimal allocation of these cybersecurity resources in the grid is extremely important. At the same time, optimization of these investments proves to be challenging due to the uncertain behavior of attackers and the dynamically changing threat landscape. Existing solutions for this problem either do not address the dynamic behavior of adversaries or lack in the practical feasibility of the defense models. This paper addresses the problem of optimizing investment strategies in the cybersecurity infrastructure of a smart grid using a game-theoretic approach. The attacker is modeled using various attacker profiles which represent the possible types of adversaries in the context of CPS. Each profile has certain characteristics to bring out the aspect of uncertain behavior of the adversaries. The defender is modeled with various pragmatic characteristics that can be easily translated to the real-world grid scenarios for implementation. These characteristics include the standards laid down by the North American Electric Reliability Corporation (NERC) for Critical Infrastructure Protection (CIP) commonly known as the NERC-CIP standards. The game-theoretic framework allows us to obtain optimal strategies that the defender of the grid can adopt to minimize its losses against the possible attack threats on the grid. The concept is illustrated by a simplistic 3-bus power system model case study which depicts how the solution can be translated to practical implementation in the actual grid.**

***Index Terms*—CPS, Smart Grid, Cybersecurity, Game Theory, Attacker model, Defender model, NERC-CIP**

I. Introduction

The Smart Grid is fast becoming one of the largest Cyber-Physical Systems (CPS) ever built. Rapid growth of this CPS is accompanied by increased vulnerability of the system due to the threats from the cyberspace. Any successful breach of security by the adversaries into the system can cause blackouts in the power grid which in turn can lead to human as well as monetary losses as was witnessed in the Ukrainian 2015 and 2016 Attacks [1]. This creates an obligatory need for securing the power grid against any possible cyber attacks. One of the biggest challenges in securing the grid under an evolving threat landscape is the uncertain behavior of the adversaries when the resources of the stakeholders in the grid (or the defender of the grid) are limited. Cybersecurity solutions that use deterministic models [2] cannot ensure immunity against the dynamic and uncertain adversary behavior. In other words, quantification of the cyber-threat landscape proves to be a bottle-neck while assessing the risk associated with the different elements of the smart grid. This calls for the development of stochastic and heuristic models which can capture this aspect of the smart grid cyberspace to allow for optimal deployment of the available resources. Existing works that try to solve the problem of protecting the grid against cyber attacks using various techniques like optimization theory and Markov Decision Processes do not consider the dynamics of the threat landscape [3], [4]. One of the approaches to model human behavior in a dynamic environment is game theory [5]. Game-theoretic modeling involves two or more entities competing over a common platform to maximize their profits or minimize their losses. In the case of a smart grid, the adversary and the defender can be considered as two entities that are competing against each other where the former entity is trying to maximize its profits from the system and the latter one is trying to minimize its losses. Although there has been a lot of work on the application of game theory to cybersecurity [6], [7], it is mostly limited to just cyber systems and does not deal with CPSs. The works that propose attacker models for CPS [8], [9] and apply game theory for cybersecurity in smart grids [2], [10] lack in the practical feasibility of their models in the current grid scenario.

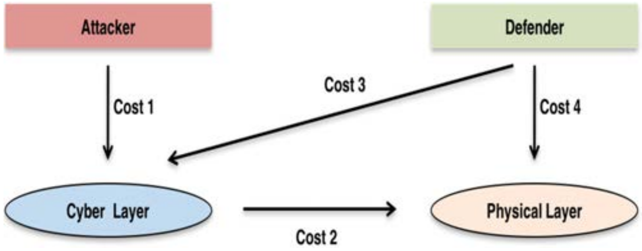


Fig. 1. Attacker and Defender Interactions in the Smart Grid

In this paper, we have proposed an approach to model the attacker and defender of the smart grid that takes into account the uncertain behavior of the attacker and the practical feasibility of the defender model. In addition to these two entities, the smart grid CPS is also modeled under the game-theoretic framework using NERC-CIP standards [11] and the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [12] in order to allow us for practical implementation of the proposed solution in the real-world grid. The solution provides us with the best strategy for the defender to invest the available resources optimally in the grid.

The paper is organized as follows: Section II depicts the problem formulation; Section III shows the methodology used and delineates the different models developed in the game-theoretic framework; Section IV provides a case study to validate the models; and Section V concludes the paper.

II. Problem Formulation

Fig. 1 depicts how the attacker and the defender interact over the cyber and physical layers of the smart grid. The attacker tries to penetrate the cyber layer and incurs a cost represented by $Cost$ 1. A successful attack on the cyber layer has impacts on the physical layer and is associated with a cost represented by $Cost$ 2. This cost is incurred by the defender

978-1-7281-3103-0/20/$31.00 ©2020 IEEE

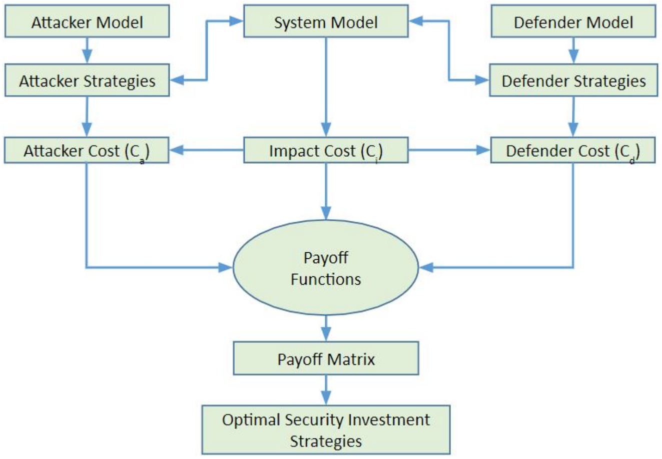


Fig. 2. Proposed Methodology Flowchart

and is called the impact cost on the system due to an attack. The defender, in order to make the grid more secure, invests in the cyber and the physical layers and incurs the costs $Cost\ 3$ and $Cost\ 4$, respectively. The total costs incurred by the Attacker and Defender are given by: $Attacker's\ Cost = Cost\ 1$ and $Defender's\ Cost = Cost\ 2 + Cost\ 3 + Cost\ 4$.

The attacker is trying to minimize its cost while maximizing defender's cost. The objective function for the attacker can be formulated as the following multi-objective optimization problem:

$$\begin{aligned} & min\ Cost\ 1 \\ & max\ Cost\ 2 \\ & subject\ to: \ Attacker's\ resources\ and\ characteristics \\ & \qquad\qquad\quad System\ properties \end{aligned}$$

Similarly, the defender's objective function can be stated as follows:

$$\begin{aligned} & min\ Cost\ 2 + Cost\ 3 + Cost\ 4 \\ & max\ Cost\ 1 \\ & subject\ to: \ Defender's\ resources\ and\ characteristics \\ & \qquad\qquad\quad System\ properties \end{aligned}$$

III. Game Theory-based Modeling

This section discusses in detail the proposed framework, the System model, the Defender model, the Attacker model, and the functions used for game formulation and solution.

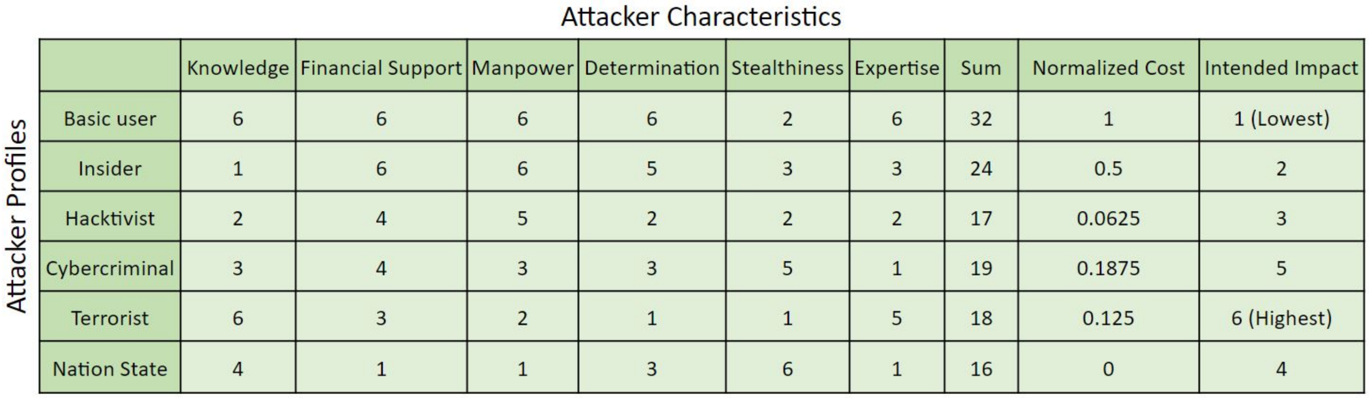
A. *Proposed Framework*

Fig. 2 shows the proposed methodology wherein three types of models have been developed, namely, the Attacker Model, the Defender Model, and the System Model under a game-theoretic framework. The Attacker and Defender Models define various strategies that the attacker and the defender can adopt in an environment defined by the System Model. Depending upon the strategy adopted by the attacker and the defender, each of them incurs a cost which is also dependent on the cost of impact that the attacker's strategy has on the system. These costs define the payoff that each of the players will be receiving by playing the respective strategies. A comprehensive list of payoffs of each of the players for various possible strategies generates a payoff matrix which is solved using game-theoretic tools to culminate into the best strategy to be used by the defender. Although this framework has been developed for the smart grid environment, it can be adopted in any CPS environment wherein the system model, the attacker model and defender model can be changed to fit the given environment.

B. *System and Defender Model*

The Smart Grid CPS at the transmission level can be represented as a network of substations which are connected at both the physical and the cyber layers. The cyber layer of the substations makes them vulnerable to cyber attacks and in this work the substations are considered as the target nodes that the attacker intends to attack. We have defined a model for the substations which is derived from the NERC-CIP standards and the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) introduced by the United States' Department of Energy. The ES-C2M2 proposes a model for organizations related to the electricity subsector wherein they can assign scores to various predefined domains in accordance with the organization's cybersecurity practices. In our work, we have modified this model and changed the domains to various characteristics based on some of the NERC-CIP standards in which each characteristic is scored according to the maturity level of the cybersecurity resources, equipment, and practices of each substation. The domains that were selected from the various NERC-CIP standards to represent the substations are as follows: *Personnel and Training* - Level of training and awareness of personnel about Cybersecurity; *Electronic Security Perimeter* - Maturity of Security at the Software Level including firewalls, Password Protection, Operating Systems, IDS, etc.; *Physical Security* - Maturity of Security at the Physical Level including Physical access to substations, redundant hardware, etc.; *Systems Security Management* - Implementation and management of Firmware Updates, IPS, System Access Control, etc.; *Recovery Plans for Cyber Systems* - Maturity level of recovery plans including their implementation and testing for recovery of BES Cyber Systems to ensure stability, operability, and reliability of the BES; and *Information Protection* - Methods involving storage, transit and use of Information. The summation of all the scores of each characteristic in a substation gives the Maturity Indicator Level (MIL) of the substation. Higher the MIL of a substation, higher will be the cost incurred by the attacker to carry out a successful attack on that substation.

In this work, we have considered that the defense mechanism adopted by the defender to reduce the chances of a successful attack is to increase the cost of attack on a target node, that is, increasing *Cost 1*. The Defender Model lays out the investment strategies that the defender can execute in order to increase this cost. The defender's strategies are to increase the MIL of the substations by investing monetary resources in the substations. As was mentioned previously, increasing of the MIL of a substation increases the cost of attack on that substation. The end result of this work gives the best strategy out of the possible defense strategies such that the cost incurred by the defender is minimized.



Attacker Characteristics

Attacker Profiles	Knowledge	Financial Support	Manpower	Determination	Stealthiness	Expertise	Sum	Normalized Cost	Intended Impact
Basic user	6	6	6	6	2	6	32	1	1 (Lowest)
Insider	1	6	6	5	3	3	24	0.5	2
Hacktivist	2	4	5	2	2	2	17	0.0625	3
Cybercriminal	3	4	3	3	5	1	19	0.1875	5
Terrorist	6	3	2	1	1	5	18	0.125	6 (Highest)
Nation State	4	1	1	3	6	1	16	0	4

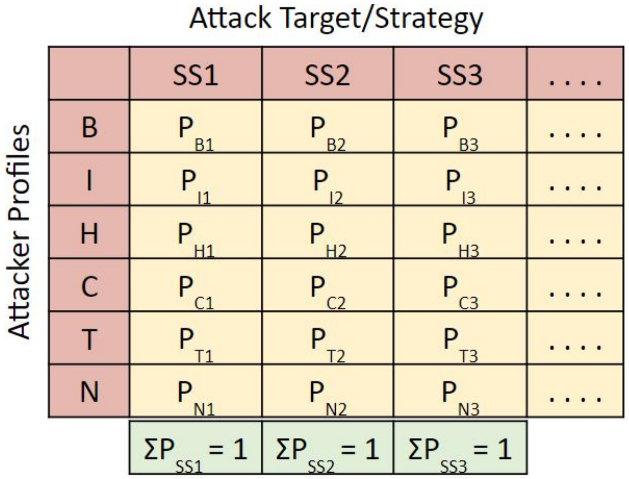
Fig. 3. Attacker Profiles and Characteristics

C. Attacker Model

Modeling of an attacker in the CPS smart grid environment proves to be a challenge due to the fact that the motives and, thus, the characteristics of the attacker are hard to predict. In order to solve this issue, we have considered various possible profiles of an attacker and assigned specific characteristics to the profiles. This is illustrated in Fig. 3 which shows six profiles of the attacker in the left-most column and the the characteristics in the top-most row. The profiles and characteristics are defined below:

Basic user - Unstructured hacker or hobbyist; *Insider* - Disgruntled employee or a social engineering victim; *Hacktivist* - A hacker activist; *Terrorist* - Cyber-terrorist; *Cybercriminal* - Black hat hacker or structured hacker; and *Nation-State* - An attacker sponsored by a nation.

The various characteristics are - *Knowledge*: Cost incurred to gain knowledge of the system; *Financial Support*: Cost incurred to arrange finances for the attack; *Manpower*: Cost incurred to arrange manpower for the attack; *Determination*: Cost incurred to get determination for carrying out the attack; *Stealthiness*: Cost incurred for efforts put in to stay undetected; and *Expertise*: Cost incurred to gain attacking proficiency. Each profile is given a relative score under each column based on heuristics for the particular characteristic of each profile. The *Sum* column adds all the scores of each row. The *Sum* represents the overall relative cost incurred by each type of attacker to carry out an attack on any component in the system. This relative cost is normalized to a different range in the *Normalized Costs* column for better visualization of the relative costs. For the purpose of bringing in the stochastic nature of the threats, each attack target in the system is assigned a probability of attack based on the intention of each type of attacker profile and the impact that the target node will have on the system if taken out. The intention of an attacker defines the level of impact that the attacker wants to have on the system and its value is obtained from heuristic evaluation as is represented in the column *Intended Impact* in Fig. 3. Fig. 4 shows how different attacker profiles can have varying probabilities of attack over different substations. The sum of the probabilities of all profiles for a particular substation is one as is represented in the last row. This is because we have distributed the attack probabilities across different attacker profiles according to their *Intended Impact* after considering that an attack on a substation has occurred.



Attack Target/Strategy

Attacker Profiles	SS1	SS2	SS3	. . . .
B	P_{B1}	P_{B2}	P_{B3}	. . . .
I	P_{I1}	P_{I2}	P_{I3}	. . . .
H	P_{H1}	P_{H2}	P_{H3}	. . . .
C	P_{C1}	P_{C2}	P_{C3}	. . . .
T	P_{T1}	P_{T2}	P_{T3}	. . . .
N	P_{N1}	P_{N2}	P_{N3}	. . . .
	$\Sigma P_{SS1} = 1$	$\Sigma P_{SS2} = 1$	$\Sigma P_{SS3} = 1$	

Fig. 4. Attack Probability Matrix

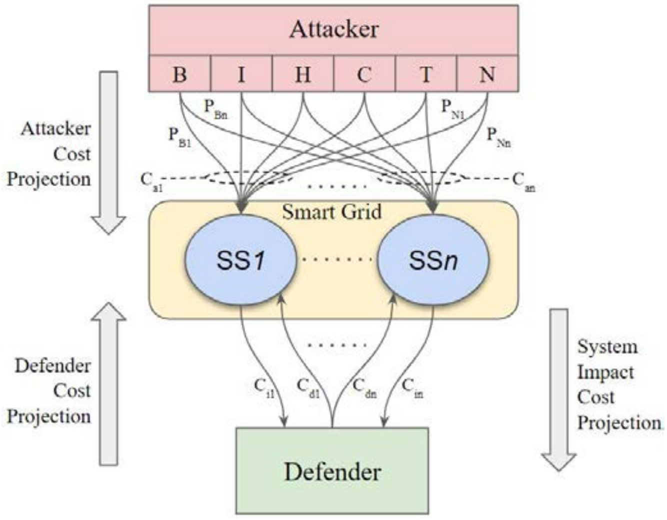


Fig. 5. Attacker and Defender Cost Projections and System Impacts

Fig. 5 shows how the Attacker and the Defender project their respective costs on the system, that is, the Smart Grid and how the system responds to those cost projections. Each attacker profile incurs some cost to attack a substation SS_n with some probability $P_{pr,n}$, where pr is the attacker profile. A weighted sum of these costs based on the probabilities gives the total attacker's cost to attack the substation SS_n and is represented in the figure as C_{an}. The defender in turn invests C_{dn} in SS_n and also incurs an impact cost C_{in} due to the attack on SS_n.

To obtain the actual cost incurred by the attacker to attack a target node (substation) in the system, four factors are taken into consideration: The relative cost of attack for each profile of attacker; the probability of attack by each type of attacker for the target node; the impact due to the loss of the target node; and the MIL of the target substation node. The actual cost of attack on a target node is calculated by taking a weighted sum of the relative costs of each attacker profile and multiplying this weighted sum with the impact cost metric. The impact cost metric is based on the load lost due to the attack and the MIL of the target node. As was mentioned previously, higher the MIL of the target node, higher will be the cost of attack. The weights given to the relative cost incurred by each attacker profile are equal to their respective probabilities of attack on the target node. This cost of attack for any target node, thus, takes into account the threat from various sources of attack that are represented by the different attacker profiles. The following equation is used to calculate the actual cost incurred by the attacker to attack a substation:

$$C_{a,SSn} = \sum_{pr} (P_{pr,SSn} * N_{c,pr} * I_{c,n}) \tag{1}$$

where $C_{a,SSn}$ represents the actual cost of attack on substation SSn, pr represents the attacker profile, n represents the substation number, $P_{pr,SSn}$ represents the probability by which the attacker profile pr will attack substation SSn whose value is taken from the attack probability matrix. $N_{c,pr}$ represents the relative normalized cost for attacker profile pr given in the *Normalized Cost* column of Fig. 3 and $I_{c,n}$ represents the impact cost metric for substation SSn.

For the sake of simplicity at the stage of proof of concept, we have not considered coordinated attacks on substations. The strategies for the attacker taken into account in this work are single-stage attacks on a substation.

D. Payoff Functions and Nash Equilibrium

We have considered a zero-sum game formulation wherein the payoff of the attacker and the defender add up to zero. The payoff that the attacker gets from the game is the sum of the costs incurred by the defender minus the cost incurred by the attacker and is represented by the following equation:

$$U_a = \alpha_0(\alpha_1 C_d + \alpha_2 C_i - \alpha_3 C_a) \tag{2}$$

where C_d = *Cost 3* + *Cost 4*, C_i = *Cost 2*, and C_a = *Cost 1*. α_1, α_2, and α_3 are normalizing factors to get different costs on the same scale and are dependent on C_d, C_i, and C_a, respectively. α_0 is a scaling up factor to bring the normalized costs on to a larger scale in order to allow for differentiation between closely valued data and is dependent on $(\alpha_1 C_d + \alpha_2 C_i - \alpha_3 C_a)$.

For a zero-sum game, the defender's payoff is the negative of the attacker's payoff and is given by the following equation:

$$U_d = -U_a \tag{3}$$

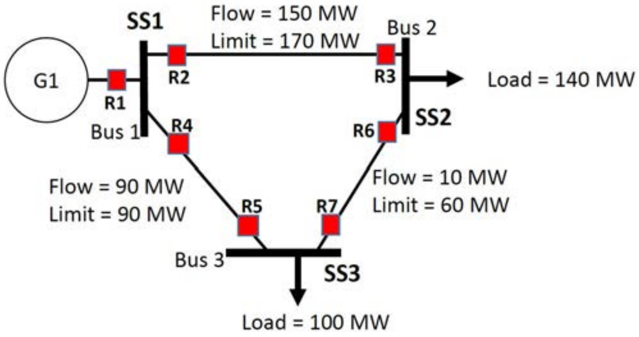


Fig. 6. Three bus power system model used for the case study

After the payoffs for each player are calculated, we can obtain the payoff matrix in which all possible strategies of the defender are represented by the rows and the attacker's strategies are represented by the columns. The Nash Equilibrium or the optimal strategy to be adopted by each player is obtained by using the following set of equations:

$$v_{dp} = \max_i \min_j U_{ij} \tag{4}$$

$$v_{ap} = \min_j \max_i U_{ij} \tag{5}$$

Equations 4 and 5 give the minimum payoff that the defender and attacker can get from the game represented by v_{dp} and v_{ap}, respectively. U_{ij} represents the payoff for defender's ith strategy when the attacker plays the jth strategy. For a zero sum game, $v_{dp} = v_{ap}$ represents the Pure Strategy Nash Equilibrium (PSNE) wherein a single strategy is dominant over all other strategies for each player.

In case of a game where a single strategy is not dominant, a Mixed Strategy Nash Equilibrium (MSNE) is obtained. Equation 6 represents the expected payoff in such a case with p and q being the probability distributions over different strategies for the defender and the attacker, respectively. v_{dm} and v_{am} in equation 7 and 8 represent the optimal payoffs for the defender and attacker, respectively, in case of a mixed strategy solution and $v_{dm} = v_{am}$ is the MSNE.

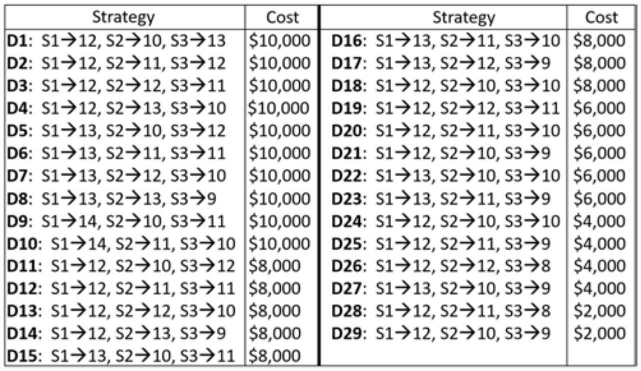
$$E(p, q) = \sum_{j=1}^{n} \sum_{i=1}^{m} p_i q_j U_{ij} \tag{6}$$

$$v_{dm} = \max_p \min_q E(p, q) \tag{7}$$

$$v_{am} = \min_q \max_p E(p, q) \tag{8}$$

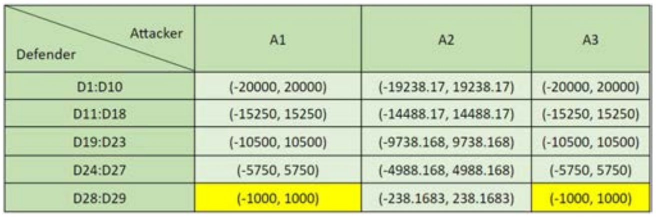
IV. Case Study

For the proof of concept of this work, we have considered a simplistic case study of a three bus transmission system with each bus acting as a substation, namely, SS1, SS2, and SS3 as shown in Fig. 6. It shows relays from R1 to R7 each monitoring different transmission lines in their respective substations. R1, R2, and R4 are controlled by SS1; R3 and R6 are controlled by SS2; and R5 and R7 are controlled by SS3. In this case study, we have assumed that an attacker after attacking a substation manipulates all the relays associated



Strategy	Cost	Strategy	Cost
D1: S1→12, S2→10, S3→13	$10,000	**D16**: S1→13, S2→11, S3→10	$8,000
D2: S1→12, S2→11, S3→12	$10,000	**D17**: S1→13, S2→12, S3→9	$8,000
D3: S1→12, S2→12, S3→11	$10,000	**D18**: S1→12, S2→10, S3→10	$8,000
D4: S1→12, S2→13, S3→10	$10,000	**D19**: S1→12, S2→12, S3→11	$6,000
D5: S1→13, S2→10, S3→12	$10,000	**D20**: S1→12, S2→11, S3→10	$6,000
D6: S1→13, S2→11, S3→11	$10,000	**D21**: S1→12, S2→10, S3→9	$6,000
D7: S1→13, S2→12, S3→10	$10,000	**D22**: S1→13, S2→10, S3→10	$6,000
D8: S1→13, S2→13, S3→9	$10,000	**D23**: S1→13, S2→11, S3→9	$6,000
D9: S1→14, S2→10, S3→11	$10,000	**D24**: S1→12, S2→10, S3→10	$4,000
D10: S1→14, S2→11, S3→10	$10,000	**D25**: S1→12, S2→11, S3→9	$4,000
D11: S1→12, S2→10, S3→12	$8,000	**D26**: S1→12, S2→12, S3→8	$4,000
D12: S1→12, S2→11, S3→11	$8,000	**D27**: S1→13, S2→10, S3→9	$4,000
D13: S1→12, S2→12, S3→10	$8,000	**D28**: S1→12, S2→11, S3→8	$2,000
D14: S1→12, S2→13, S3→9	$8,000	**D29**: S1→12, S2→10, S3→9	$2,000
D15: S1→13, S2→10, S3→11	$8,000		

Fig. 7. Defender Strategies



Attacker Defender	A1	A2	A3
D1:D10	(-20000, 20000)	(-19238.17, 19238.17)	(-20000, 20000)
D11:D18	(-15250, 15250)	(-14488.17, 14488.17)	(-15250, 15250)
D19:D23	(-10500, 10500)	(-9738.168, 9738.168)	(-10500, 10500)
D24:D27	(-5750, 5750)	(-4988.168, 4988.168)	(-5750, 5750)
D28:D29	(-1000, 1000)	(-238.1683, 238.1683)	(-1000, 1000)

Fig. 8. Payoff Matrix

with that substation, that is, the substation and the transmission lines associated with it are isolated from the grid.

The MIL of each substation is assumed according to the critical level of the substation. Each substation has six characteristics or domains with each domain having a maturity value ranging from 0 to 3, where 0 is lowest maturity level and 3 is the highest maturity level. Thus, any substation can have an MIL ranging from 0 to 18. The defender's and attacker's strategies and costs are obtained after taking few assumptions as follows: 1) The MIL for SS1, SS2, and SS3 are 12, 10, and 8, respectively. 2) The defender has a budget of $10,000. 3) Increase in MIL of each domain costs the same across all substations which is equal to $2,000. 4) The maximum allowed difference in MIL of any two substations is 4. 5) The cost of loss of load is $100/MW. 6) The attacker will attack only one substation in a single attack. The possible defender's strategies under these assumptions are listed down in Fig. 7 along with the costs associated with each strategy. These costs mentioned in the figure represent C_d, that is, the investment cost of the defender. The cost due to loss of each substation or the impact cost gives the value of C_i. The attacker's cost for carrying out the attack, C_a, is calculated after substituting appropriate values in eq. 1. Using these costs, α_1, α_2, α_3, and α_0 are calculated. For each strategy, the payoff for the defender and the attacker is computed using their respective payoff functions given in eq. 2 and eq. 3 to form the payoff matrix as shown in Fig. 8. The defender's strategies having the same value of C_d are clubbed together as one row for easy visualization as all the strategies with the same C_d result in the same payoff values. The game is then solved using equations 4 to 8 to obtain the Nash Equilibrium which is highlighted as the yellow cells in the payoff matrix in Fig. 8.

The Nash Equilibrium gives us the best strategy that the defender needs to adopt in order to minimize losses from a cyber attack on the given system. In this system, the Nash Equilibrium suggests that the defender should either increase the MIL of SS2 to 11 from the initial value of 10 or increase the MIL of SS3 to 9 from the initial value of 8. This can be done by investing in the substation's cybersecurity resources according to NERC-CIP standards, that is, by having a more mature level of compliance to the standards.

V. Conclusion and Future Work

We have proposed a novel method for modeling of the Cyber-Physical Smart Grid System and the various stakeholders involved in it including the defender and the attacker of the system based on a game-theoretic framework. We have introduced an approach to incorporate the uncertain and dynamic behaviour of the attack landscape in a CPS smart grid. The results provide us with optimal strategies to be adopted by the defender of the smart grid in order to optimally use their available resources against potential cyber attacks. We have demonstrated the practical feasibility of the results in the current real-world grid scenario by considering the NERC-CIP standards and ES-C2M2 model that are being implemented in the United States' power grid. We have also presented a case study on a simplistic three-bus power transmission system represented as a three-substation system in order to illustrate the concept of the work. For our future work, we plan to carry out risk assessment studies under the same framework and also consider larger systems for our case studies. Additionally, apart from implementing this methodology for offline risk assessment studies, we plan to modify the models for its application in online dynamic cyber contingency studies.

References

[1] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid" March 18, 2016.

[2] A. Ashok and M. Govindarasu, "Cyber-physical risk modeling and mitigation for the smart grid using a game-theoretic approach," 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, 2015, pp. 1-5.

[3] C. Y. T. Ma, D. K. Y. Yau and N. S. V. Rao, "Scalable Solutions of Markov Games for Smart-Grid Infrastructure Protection," in IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 47-55, March 2013.

[4] P. Chen, S. Cheng and K. Chen, "Smart attacks in smart grid communication networks," in IEEE Communications Magazine, vol. 50, no. 8, pp. 24-29, August 2012.

[5] T. Basar and G. J. Olsder, Dynamic Noncooperative Game Theory: SIAM Series in Classics in Applied Mathematics,Jan. 1999.

[6] Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, and Sundaraja Sitharama Iyengar, "Game Theory for Cyber Security and Privacy" ACM Comput. Surv. 50, 2, Article 30 (May 2017).

[7] Y. Wang, Y. Wang, J. Liu, Z. Huang and P. Xie, "A Survey of Game Theoretic Methods for Cyber Security," IEEE First International Conf. on Data Science in Cyberspace (DSC), Changsha, 2016, pp. 631-636.

[8] Rocchetto M., Tippenhauer N.O. "On Attacker Models and Profiles for Cyber-Physical Systems," ESORICS 2016.

[9] S. Adepu and A. Mathur, "Generalized Attacker and Attack Models for Cyber Physical Systems," IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, 2016, pp. 283-292.

[10] Saad, Walid & Han, Zhu & Poor, H. Vincent & Baar, Tamer. (2012). Game Theoretic Methods for the Smart Grid. IEEE Signal Processing Magazine, Special Issue on Signal Processing for the Smart Grid. 29.

[11] North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP) Standards [ONLINE] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[12] Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [ONLINE] https://www.energy.gov/ceser/ activities/ cybersecurity -critical-energy- infrastructure/ energy-sector-cybersecurity