A Novel Methodology for Cybersecurity Investment Optimization in Smart Grids using Attack-Defense Trees and Game Theory

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

***Abstract*—Securing cyber-physical systems (CPS) like the Smart Grid against cyber attacks is making it imperative for the system defenders to plan for investing in the cybersecurity resources of cyber-physical critical infrastructure. Given the constraint of limited resources that can be invested in the cyber layer of the cyber-physical smart grid, optimal allocation of these resources has become a priority for the defenders of the grid. This paper proposes a methdology for optimizing the allocation of resources for the cybersecurity infrastructure in a smart grid using attack-defense trees and game theory. The proposed methodology uses attack-defense trees (ADTs) for analysing the cyber-attack paths (attacker strategies) within the grid and possible defense strategies to prevent those attacks. The attack-defense strategy space (ADSS) provides a comprehensive list of interactions between the attacker and the defender of the grid. The proposed methodology uses the ADSS from the ADT analysis for a game-theoretic formulation (GTF) of attacker-defender interaction. The GTF allows us to obtain strategies for the defender in order to optimize cybersecurity resource allocation in the smart grid. The implementation of the proposed methodology is validated using a synthetic smart grid model equipped with cyber and physical components depicting the feasibility of the methodology for real-world implementation.**

***Index Terms*—CPS, Smart Grid, Cybersecurity, Game Theory, Attack-Defense Tree**

I. Introduction

With the increasing number of cyber incidents in the critical infrastructure, there is a growing need to secure critical cyber-physical systems (CPSs) like the smart grid against cyber threats as is recommended by federal agencies like The President's National Infrastructure Advisory Council (NIAC) [1]. One of the recommendations from the NIAC report to achieve cybersecurity in CPSs is to optimally align resources for cyber defense of these infrastructures. This makes it necessary for the stakeholders of the critical infrastructure to find novel methods that allows them to adopt ways for securing these assets against the dynamically changing cyber threat landscape. Given the vast and complex design of the grid and the increasing sophistication of targeted cyber attacks, risk assessment along with security resource allocation in the grid to prevent cyber intrusions proves to be challenging [2].

There has been a lot of research using various methods for solving this issue of cybersecurity resource optimization in the smart grid over the past decade. Some of these methods include use of Markov Decision Processes (MDP) approach [3], multiarmed bandits (MAB) approach [4], cognitive radio networks for cognitive smart grids [5], petri-net modeling [6], attack trees and graphs [7], attack-defense trees [8]–[11], and game theory [12]–[14]. While the methods used in the existing research have shown various capabilities for CPS security like assessing vulnerabilities in the system for attack surface detection (Attack Trees and ADT), adoption of defense mechanisms for securing the attack surfaces (MDP, MAB, PetriNet, and ADT), risk assessment (Attack Trees, ADT, and Game-Theory), and cybersecurity resource optimization (MDP, MAB, and Game Theory), none of the methods address all of these issues for CPS security.

In this paper, we propose a novel methodology with a combination of attack-defense trees (ADT) and game theoretic approach for identification of attack surfaces in the smart grid followed by optimization of defender's resources for securing the attack surfaces in the grid. A comparison of various features of combining the advantages of ADT and game theory over other commonly used methods in the context of cyber-physical security of the smart grid is shown in Table I. The table shows that by integrating ADT and game-theory, the advantages of both the methods are combined to provide a holistic approach for CPS security in the smart grid. The methodology used in this work is outlined in Section II and evaluated using a case study in Section III.

II. Proposed Methodology

Fig. 1 shows the overview of the proposed methodology with four modules, namely, *Cyber-Physical Smart Grid Model*, *Attack-Defense Tree* (ADT), *Attack-Defense Strategy Space* (ADSS), and *Game-Theoretic Formulation* (GTF). The final stage is the output of the GTF which provides the *Optimal Strategy* (S'_d) to be used by the defender for investment in the cybersecurity infrastructure of the smart grid. The ADT modeling assists in identifying the vulnerabilities and attack-access points in the grid (attack surface) as well as providing avenues for suggesting defense mechanisms against the possible attacks.The game-theoretic formulation allows for optimization of the defender's resources to be allocated for securing the components of the grid that the attacker can exploit to achieve its objectives. Both of these methods can be used for risk assessment of the system as well which is not discussed in this work but will be pursued in a follow-up work as mentioned in Section IV.

A. Cyber-Physical Smart Grid Model and Attack Surface

The smart grid is modeled as a network of substations representing the bulk power system with cyber-layer communication capabilities. Each substation has two types of components, namely, *Physical Components* and *Cyber Components*, that

This work is funded by the NSF CPS grant ECCS 1739969

TABLE I
COMPARISON OF VARIOUS METHODS FOR SMART GRID CYBERSECURITY AND THEIR FEATURES

Feature↓ /Method →	MDP	MAB	Attack Tree	PetriNet	ADT	Game Theory	ADT + Game Theory
Vulnerability Assessment	x	x	✓	✓	✓	x	✓
Security Mechanisms	✓	✓	x	✓	✓	x	✓
Risk Assessment	x	x	✓	x	✓	✓	✓
Resource Optimization	✓	✓	x	x	x	✓	✓

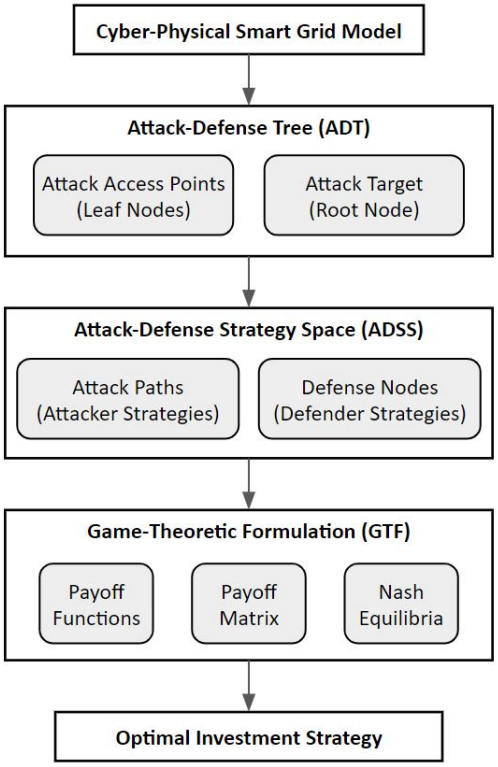

Fig. 1. Overview of the Proposed Methodology

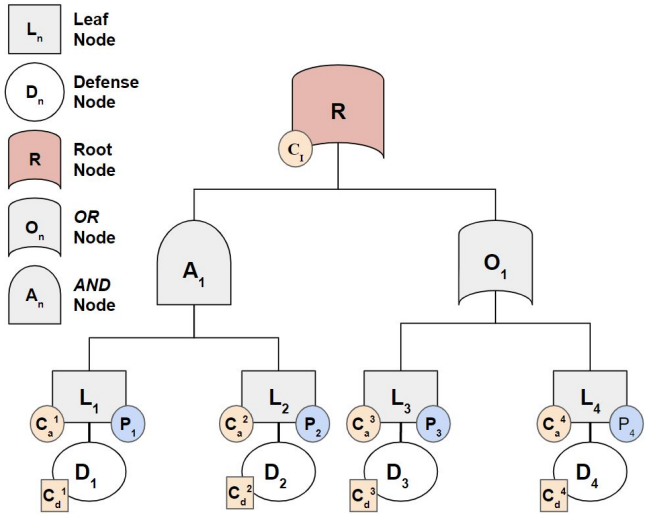

Fig. 2. Attack-Defense Tree Example

allow the bulk power system operations and wide-area network (WAN) communication for wide-area monitoring, protection, and control (WAMPAC), respectively. The physical-layer connectivity represents the topology of the grid at the transmission level while the cyber layer-connectivity represents the cyber-topology, connecting the substations to the WAN. This implies that each substation is susceptible to cyber-attacks through the WAN, acting as the system's attack surface.

B. Attack Defense Trees (ADT)

An Attack-Defense Tree is a connected hierarchical tree that depicts pathways that an attacker can take within a system in order to achieve their target along with the countermeasures that a defender can take to prevent the attacks. The entry points (or access points) for the attacker in the system are represented by leaf nodes that are connected through logical operator nodes like *AND* and *OR* nodes that eventually lead to the root node which represents the attacker target. Each leaf node is associated with a defense node representing the defense measure for securing the associated leaf node. A simplistic example of an ADT is shown in Fig. 2. The figure shows four access points (leaf nodes) for the attacker to breach the system L_1, L_2, L_3, and L_4. Each leaf node is associated with a defense node D_1, D_2, D_3, and D_4, respectively. The attacker target (root node) R can be reached through three attack paths:

Attack Path-1: L_1 and L_2
Attack Path-2: L_3
Attack Path-3: L_4

Note that both L_1 and L_2 nodes need to be breached to reach R as these are conjointed by an *AND* node, while either one of the L_3 or L_4 nodes can be breached to reach R as these are conjointed by an *OR* node.

Furthermore, each leaf node (j) is associated with a cost, C^j_{aL}, that the attacker incurs to breach that access point. The leaf nodes also have an associated probability of attack, P_j. Similarly, each defense node (k) is associated with a cost, C^k_{dL}, that the defender incurs to secure that node against an attack. The root node has an impact cost, C_I, associated with it which represents the additional cost incurred by the defender if the attacker achieves its target. The costs, C^j_{aL} and C^k_{dL}, and the probabilities, P_j, are obtained using models and methods described in our previous work [12]. In this work, the impact cost, C_I, is calculated as a measure of the load loss in the smart grid due to attacker actions based on a rate (r_L) defined in terms of dollars lost per Megawatt load loss ($\$/MW_{LL}$).

C. Attack-Defense Strategy Space (ADSS)

The ADSS is derived by evaluating the ADT. The ADSS includes all the strategies for the attacker to attack the system and the strategies for the defender to prevent the attacker from achieving its target. The strategies for the attacker are defined by the set of attack paths that lead to the root node of the tree starting from the leaf nodes. The strategies for the defender are defined by the set of defender nodes that secure each attack path against possible cyber attacks.

The Attack Strategy Space (set of attacker strategies), S_a (shown in (1)), is a set of all attack paths (AP_i) that the attacker can take to achieve its target, that is, reach R.

$$S_a : \{AP_1, AP_2, ..., AP_n\} \tag{1}$$

where n is the number of attacker strategies.

For the example shown in Fig. 2, S_a is the set $\{AP_1, AP_2, AP_3\}$ with subsets: (a) AP_1: $\{L_1, L_2\}$; (b) AP_2: $\{L_3\}$; and (c) AP_3: $\{L_4\}$

The Defense Strategy Space, which is the set of defender strategies (DS_i), denoted as S_d (shown in (2)), is a set of combinations of all defense nodes that the defender needs to invest in for securing all the attack paths in S_a.

$$S_d : \{DS_1, DS_2, ..., DS_m\} \tag{2}$$

where m is the number of defense strategies.

Again, for the example shown in Fig. 2, S_d is the set $\{DS_1, DS_2\}$ where: (a) DS_1: $\{D_1, D_3, D_4\}$; and (b) DS_2: $\{D_2, D_3, D_4\}$

In order to secure all the attack paths in S_a, the defender needs to invest in one of the defense nodes that precede the *AND* nodes and all the defense nodes that precede the *OR* nodes.

D. Game Theoretic Formulation (GTF)

The GTF uses a zero-sum game formulation wherein the payoff of the attacker and the defender add up to zero. The strategy space for the GTF module is provided by the ADSS module ($\{S_a, S_d\}$). The output of the GTF module is the optimal strategy for the defender, denoted by S'_d, for investing in the defense nodes contained in the set S'_d.

1) Payoff Functions: The payoff of the attacker, U_a^{jk}, for strategy j when the defender chooses strategy k is given by (3).

$$U_a^{jk} = C_d^k + C_I - C_a^j \tag{3}$$

where C_d^k is the cost of defense for defense strategy k and C_a^j is the cost of attack for attack strategy j. C_d^k and C_a^j are calculated as shown in (4).

$$\begin{aligned} C_d^k &= \sum_{i=1}^{v} C_{dL}^i \\ C_a^j &= \sum_{i=1}^{w} P_i * C_{aL}^i \end{aligned} \tag{4}$$

where v and w are the number of elements in strategy sets k and j, respectively, and P_i is the probability of attack of the leaf node i.

For a zero-sum game, the defender's payoff is the negative of the attacker's payoff. The payoff for the defender, U_d^{jk}, when the defender chooses strategy k and the attacker chooses strategy j is shown in (5).

$$U_d^{jk} = -U_a^{jk} \tag{5}$$

2) Payoff Matrix and Nash Equilibrium: The payoff matrix, which is a matrix of all the elements of the set S_a as columns and all the elements of S_d as rows, is obtained using the payoffs generated from the equations (3) and (5) for all the strategies in the sets S_a and S_d.

To obtain S'_d, Nash Equilibrium of the payoff matrix is calculated using (6) and (7) if the game has a Pure Strategy Nash Equilibrium (PSNE) wherein a single strategy is dominant over all other strategies for each player.

$$v_{dP} = \max_j \min_k U_d^{jk} \tag{6}$$

$$v_{aP} = \min_k \max_j U_d^{jk} \tag{7}$$

If the game has a Mixed Strategy Nash Equilibrium (MSNE), the Nash Equilibrium is obtained by using (8), (9), and (10).

$$E(p,q) = \sum_{j=1}^{n} \sum_{k=1}^{m} p_k q_j U_d^{jk} \tag{8}$$

$$v_{dM} = \max_p \min_q E(p,q) \tag{9}$$

$$v_{aM} = \min_q \max_p E(p,q) \tag{10}$$

Equation (8) represents the expected payoff in the case of a MSNE with p and q being the probability distributions with which the defender and the attacker choose to play their strategies, respectively.

The Nash Equilibrium of the game gives the S'_d, which is either a single strategy (in case of a PSNE) or a mixed set of strategies with an associated probability distribution (in case of a MSNE) for the defender.

III. Case Study for Evaluation of the Proposed Methodology

A. Cyber-Physical Smart Grid Model

Fig. 3 shows a schematic of a synthetic cyber-physical smart grid model of a 3-bus power system. Each bus represents a cyber-physical substation, namely, $SS-1$, $SS-2$, and $SS-3$. Each substation consists of cyber-layer components and physical-layer components. The cyber-layer components include *Firewall*, *Intrusion Detection System (IDS)*, and/or *Intrusion Prevention System (IPS)*. The phyical-layer components include, *generation control*, *relay control*, and/or *load control*.

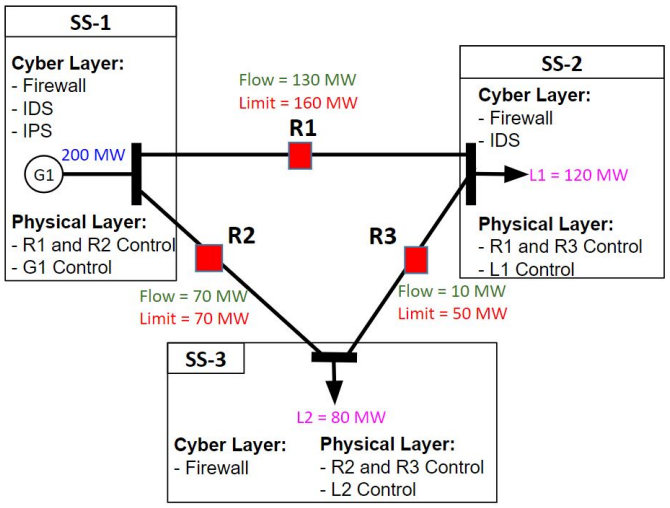

Fig. 3. Cyber-Physical Model of a 3-bus Smart Grid System

B. ADT

With the assumption that the attacker aims to cause a load loss of $100MW$ or more, the ADT for this case study is shown in Fig. 4. The ADT also shows the cost of attack and defense for each leaf node as well as the impact cost for the root node. The probability of attack for each leaf node is also indicated in the ADT. The probabilities of attack for each substation add up to 1. Instead of showing defense nodes in the ADT, only the defense cost for securing the leaf nodes are indicated in Fig 4. Suggesting possible technologies for defense against the given attacks is out of the scope of this work.

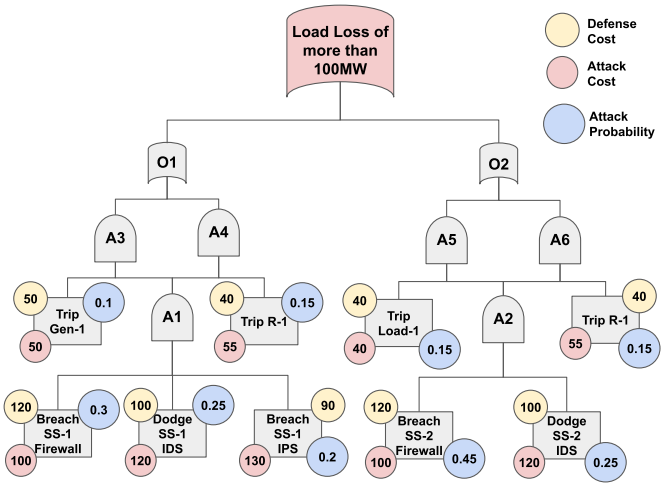

Fig. 4. Attack-Defense Tree for the 3-bus Smart Grid System

C. ADSS

The leaf nodes from Fig. 4 are labelled as shown in Table II.

1) Attack Strategy Space: The attack paths for the ADT in Fig. 4 include: (1) AP_1: $\{L_1, L_2, L_3, L_4\}$; (2) AP_2: $\{L_1, L_2, L_3, L_5\}$; (3) AP_3: $\{L_6, L_7, L_8\}$; and (4) AP_4: $\{L_6, L_7, L_9\}$. The attack strategy space is given by:

$$S_a\text{: } \{AP_1,\ AP_2,\ AP_3,\ AP_4\}$$

TABLE II
LEAF NODE LABELS FOR THE 3-BUS SMART GRID ADT

Leaf Node	Label (Attack)	Label (Defense)
Breach SS-1 Firewall	L_1	D_1
Dodge SS-1 IDS	L_2	D_2
Breach SS-1 IPS	L_3	D_3
Trip Gen-1	L_4	D_4
Trip R-1 (from SS-1)	L_5	D_5
Breach SS-2 Firewall	L_6	D_6
Dodge SS-2 IDS	L_7	D_7
Trip Load-1	L_8	D_8
Trip R-1 (from SS-2)	L_9	D_9

TABLE III
PAYOFF MATRIX

$S_d\downarrow / S_a\rightarrow$	AP_1	AP_2	AP_3	AP_4
DS_1	(-349,349)	(-276,276)	(-274,274)	(-282,282)
DS_2	(-329,329)	(-256,256)	(-254,254)	(-262,262)
DS_3	(-314,314)	(-241,241)	(-239,239)	(-247,247)
DS_4	(-329,329)	(-256,256)	(-254,254)	(-262,262)
DS_5	(-309,309)	(-236,236)	(-234,234)	(-242,242)
DS_6	(-294,294)	(-221,221)	(-219,219)	(-227,227)
DS_7	(-319,319)	(-246,246)	(-244,244)	(-252,252)
DS_8	(-299,299)	(-226,226)	(-224,224)	(-232,232)
DS_9	(-284,284)	(-211,211)	(-209,209)	(-217,217)
DS_{10}	(-319,319)	(-246,246)	(-244,244)	(-252,252)
DS_{11}	(-299,299)	(-226,226)	(-224,224)	(-232,232)
DS_{12}	(-284,284)	(-211,211)	(-209,209)	(-217,217)

2) Defense Strategy Space: The defense strategies for the ADT in fig. 4 include: (1) DS_1: $\{D_1, D_6\}$; (2) DS_2: $\{D_1, D_7\}$; (3) DS_3: $\{D_1, D_8, D_9\}$; (4) DS_4: $\{D_2, D_6\}$; (5) DS_5: $\{D_2, D_7\}$; (6) DS_6: $\{D_2, D_8, D_9\}$; (7) DS_7: $\{D_3, D_6\}$; (8) DS_8: $\{D_3, D_7\}$; (9) DS_9: $\{D_3, D_8, D_9\}$; (10) DS_{10}: $\{D_6, D_4, D_5\}$; (11) DS_{11}: $\{D_7, D_4, D_5\}$; and (12) DS_{12}: $\{D_4, D_5, D_8, D_9\}$ The defense strategy space is given by:

$$S_d\text{: } \{DS_1,\ DS_2,\ ...,\ DS_{12}\}$$

D. GTF and Optimal Defense Strategy

Using (3), (4), and (5) for the given costs and probabilities indicated in the ADT in (4), the payoffs for the attacker and defender are obtained for the ADSS $\{S_a,\ S_d\}$ and the payoff matrix is given in Table III. The defender payoffs (row player) are shown as the first element of each tuple in the table while attacker payoff (column player) are represented by the second element of each tuple. The payoffs have been approximated to the nearest integer value. The attack and defense costs indicated in Fig. 4 for the leaf nodes are equivalent $ representations of cost of attacking and defending the nodes, respectively. The impact cost, C_I, is calculated at r_L = \$1/MW_{LL}. The impact vector (in MW) for each attack path in S_a is given by:

$$C_I\text{: } [200,\ 130,\ 120,\ 130]$$

The Nash Equilibrium for the payoff matrix in Table III consists of two PSNEs at $\{DS_9, AP_1\}$ and $\{DS_{12}, AP_1\}$, and the optimal defense strategy set is given by:

$$S_d'\text{: } \{DS_9\} \text{ or } \{DS_{12}\}$$

TABLE IV
PAYOFF MATRIX FOR GAME-THEORETIC FORMULATION WITHOUT ADT

$S_d\downarrow$ /$S_a\rightarrow$	a_1	a_2	a_3
d_1	(-100,100)	(-230,230)	(-180,180)
d_2	(-270,270)	(-70,70)	(-140,140)
d_3	(-250,250)	(-180,180)	(-50,50)

The solution implies that there are two optimal strategies for the defender in this case scenario to invest in that would give the same payoff to the defender. Defense Strategy set DS_9 consists of the defenses D_3, D_8, and D_9 and the strategy set DS_{12} consists of D_4, D_5, D_8, and D_9. While D_8 and D_9 are common for both the solutions, the defender could choose to invest in either just D_3 or in both D_4 and D_5 apart from D_8 and D_9 resulting in the same payoff. Refer to Table II for the associated leaf nodes of these labels.

The advantage of using the GTF along with ADT is in the fact that GTF provides the optimal solution strategy while taking the attack cost, the impact cost for each attack path in S_a, and the probability of attack for each leaf node into consideration. On the other hand, using only ADT for choosing defense strategies can leave out defenses of high-risk attack paths that have high impact and low attack costs. At the same time, using only GTF for resource optimization is susceptible to missing out on attack access-points in the system, making those leaf nodes vulnerable to possible cyber attacks.

Table IV shows the payoff matrix of the game-theoretic formulation without using ADT with the following assumptions: (i) Defense Cost for $SS-1$, $SS-2$, and $SS-3$ is 100, 70, and 50, respectively; (ii) Impact cost is same as in previous case study; (iii) Attack cost is assumed to be same in all cases and, thus, neglected; and (iv) Impact on target substation is avoided if defender invests in the attacked substation. Defense strategy d_n defends substation $SS-n$ and attack strategy a_m attacks substation $SS-m$. Using 3, the payoff matrix in Table IV is generated and the Nash Equilibrium (mixed strategy) is:

S''_d: $\{\{d_1$: 0.61, d_1: 0.39, d_3: 0$\}$, $\{a_1$: 0.48, a_2: 0.52, a_3: 0$\}\}$

The probabilities associated with the defense strategies in the above solution can represent the percentage of budget that the defender can invest in the respective defenses but it might not secure the nodes against attacks. The quantitative comparison of the proposed methodology with just game-theoretic formulation shows the advantages furnished by the proposed methodology in assessing vulnerabilities, identifying attack paths, and providing targeted defense measures.

A summary of the attributes of ADT, GTF, and ADT+GTF methods for resource optimization for investment in defensive measures is given in Table V.

TABLE V
COMPARISON OF ATTRIBUTES OF ADT, GTF, AND ADT+GTF METHODS

Attribute$\downarrow$ /**Method** $\rightarrow$	ADT	GTF	ADT + GTF
Attack Paths	✓	x	✓
Defense Nodes	✓	x	✓
Attack Cost	x	✓	✓
Attack Probability	x	✓	✓
Defense Cost	✓	✓	✓
Impact Cost	x	✓	✓

IV. CONCLUSION AND FUTURE WORK

This paper proposed a methodology for optimizing the allocation of resources for the cybersecurity infrastructure in a smart grid using attack-defense trees and game theory. The results provide us with investment strategies that the defender of the grid can adopt in order to optimally allocate resources for the preventing cyber intrusions and the subsequent impacts in the grid. The proposed methodology provides a novel method for cybersecurity planning in the cyber-physical smart grid that takes into consideration the real-world infrastructure and applications that are used for monitoring, protection, and control implemented in today's grid both at the cyber-layer and the physical-layer. This work is currently being extended for performing cyber-physical risk assessment of the smart grid as well. For the purpose of allowing future field deployment of this work, a tool that implements the proposed methodology is also being developed that can be used by the industry and the smart grid stakeholders for cyber-physical planning and risk assessment for the grid.

REFERENCES

[1] The President's National Infrastructure Advisory Council (NIAC), "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure," 2017. [Online]. Available: https://www.cisa.gov/

[2] Electric Power Research Institute Palo Alto CA, "Cyber security strategy guidance for the electric sector," 2012. [Online]. Available: https://www.epri.com/research/products/1025672

[3] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao, "Scalable solutions of markov games for smart-grid infrastructure protection," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 47–55, 2013.

[4] M. D. Smith and M. E. Paté-Cornell, "Cyber risk analysis for a smart grid: How smart is smart enough? a multiarmed bandit approach to cyber security investment," *IEEE Transactions on Engineering Management*, vol. 65, no. 3, pp. 434–447, 2018.

[5] A. Boustani, M. Jadliwala, H. M. Kwon, and N. Alamatsaz, "Optimal resource allocation in cognitive smart grid networks," in *IEEE Consumer Communications and Networking Conference (CCNC)*, 2015.

[6] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, 2011.

[7] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Transactions on Smart Grid*, 2011.

[8] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 2010.

[9] B. Kordy, P. Kordy, S. Mauw, and P. Schweitzer, "Adtool: Security analysis with attack–defense trees," in *Quantitative Evaluation of Systems*, K. Joshi, M. Siegle, M. Stoelinga, and P. R. D'Argenio, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 173–176.

[10] X. Ji, H. Yu, G. Fan, and W. Fu, "Attack-defense trees based cyber security analysis for cpss," in *2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2016, pp. 693–698.

[11] B. Fila and W. Wideł, "Exploiting attack–defense trees to find an optimal set of countermeasures," in *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, 2020, pp. 395–410.

[12] B. Hyder and M. Govindarasu, "Optimization of cybersecurity investment strategies in the smart grid using game-theory," in *2020 IEEE PES ISGT*, 2020.

[13] B. Kordy, S. Mauw, M. Melissen, and P. Schweitzer, "Attack–defense trees and two-player binary zero-sum extensive form games are equivalent," in *Decision and Game Theory for Security*. Springer Berlin Heidelberg, 2010.

[14] P. Lau, W. Wei, L. Wang, Z. Liu, and C.-W. Ten, "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation," *IEEE Transactions on Smart Grid*, 2020.