Resilient Transactive Control in Microgrids under Dynamic Load Altering Attacks

Eder Baron-Prada, Estefany Osorio, and Eduardo Mojica-Nava, *Member, IEEE*
{edbaronp, estosorioarr, eamojican} @unal.edu.co

***Abstract*—A transactive control algorithm is proposed to manage distributed energy resources (DERs) and loads dynamically under cyber-physical attacks. Since demand response (DR) programs in a microgrid can be affected by cyber-physical attacks, it is studied a particular attack called dynamic-load altering attack (D-LAA). A transactive control algorithm based on population games theory is implemented in order to test the stability of the microgrid under D-LAA. A case study in a WSCC 9-bus is proposed. Finally, the main results of the transactive control algorithm are validated by simulations.**

***Index Terms*—Game theory, microgrids, transactive control, load altering attacks, cyber-physical security.**

I. Introduction

The electrical system is in a process of improvement through a continuous evolution of the technology associated with its monitoring and control, to make it more reliable, safe, and efficient. In this context, microgrids represent an alternative to ensure widespread access to electric power. Nonetheless, the inclusion of these technologies has several issues due to the discontinuity of power generation in renewable energy resources, causing instability and issues in the system operation. In order to integrate each microgrid component, it is necessary that they have communication channels, where the generators and other equipment can share data with each other. This with the purpose of making an optimum system operation, this means, there are two networks working together, i.e., the power network and the communication network. These networks have to work in perfect coordination in order to provide reliable energy to all users. The interdependency of these networks could compromise the power system if both do not work properly. Recently several models have been proposed in order to make the coordination between communications and power [1] [2]. However, these networks could be compromised through cyber-attacks.

A special issue will be treated in this paper is the coordination among different devices used at low levels, mainly generation units, and loads. The loads could be divided among vulnerable and secure loads. Then a controller has to be able to coordinate the system and maintain stability under the presence of cyber-attacks in the grid. These attacks are produced by hackers who try to insert false information into the system with the goal of generating physical changes and destabilize the network and finally generate a blackout. Accordingly, there are two problems which need to be addressed. First, it is to coordinate a vast number of devices, and second it is to protect or make the system resilient against cyber-physical attacks.

To address the first issue, transactive control is a strong strategy for the coordination of devices in power networks [3]. Transactive control uses a market mechanism that allows agents to interact between them through an economic signal in order to distribute the available resources [4], [5]. Furthermore, population dynamics is emerging as a framework for dynamic optimal dispatch in power networks, [6], [7].Then these frameworks can be used in order to integrate a vast number of devices while the optimal operation of the network is guaranteed.

On the other hand, the cyber-physical infrastructure of the power system has many aspects which need to be analyzed in order to recognize their vulnerabilities. In the consumption and distribution sectors, system can be compromised by attacks on their control devices, sensors, routers, among others; usually by injecting false data [8], [9]. Specifically, in the consumption sector, there has been some studies focus on load-altering attacks, which compromise the demand response (DR) and demand side management (DSM) programs [10], [11]. Some of these studies are focused on different kind of loads, such as industrial loads, which are in some cases remotely controllable, loads which are directly controlled, and loads controllable indirectly through different parameters such as frequency [12], [13], [14], [15].

In this paper, it is proposed a centralized transactive control algorithm for efficient coordination of microgrids. The control algorithm is based on a population games approach, through replicator dynamics, which optimize a social welfare problem. In the proposed approach, agents are non-cooperative and have diverses individual incentives determined by each agent. Those agents have to preserve stability while some optimality conditions are guaranteed.

It is proposed the following structure to present the results of this work. Section II presents a description of the system chosen to analyze the control system proposed, which is a microgrid of 9 nodes, three are loads and three are generators. Section III shows a description of the load under attack which resilient and robustness of the system is analyzed. Section IV presents the control system proposed to make the system resilient to abrupt changes of load and to permanent changes of load produced by the attack described previously. Section V describes the study of the case, with some results and analysis. Finally, Section VI, presents some conclusions about the work.

2017 IEEE 3rd Colombian Conference on Automatic Control (CCAC)
978-1-5386-0398-7/17/$31.00 ©2017 IEEE

II. Microgrid System Description

Loads can be modeled based on its load profile, which depends on the services where energy will be used, e.g., a commercial user is different than an industrial user or a house holder user. In this work, loads are modeled as an only type of load, and this kind of load has a device which is capable of making actions over the amount of load in order to optimize its behavior and obtain the greatest possible benefit, i.e., it is a demand response device.

Each user gives some value to the energy, if the value is large, more energy would be willing to buy. On the other hand, if the value of energy is small, it will not matter if the user consumes or not energy.

In addition, it is considered that each user can consume a maximum and a minimum load. For that, the utility function that represents the load is

$$U_i(P_D) = \left(2\frac{vd_i}{C_\Omega}\left(\frac{Pd_i - Pd_i^2}{Pd_{max}i - Pd_{min}i}\right)\right) \tag{1}$$

$$Pd_{max} \geq Pd \geq Pd_{min}$$

where vd_i is the value of each user gives to the energy, C_Ω is the price of energy in the system, Pd is the power demanded by each load and finally Pd_{max}, Pd_{min} are the maximum and minimum consumption of each load respectively.

The price in the system is calculated as it is shown in (2)

$$C_\Omega = \frac{\sum_i^j Pg_i * c_i}{\sum_i^j Pg_i} \tag{2}$$

On the other hand, the demanded power can be classified as a secure or a vulnerable load. The vulnerable load is the main goal of the DLAA, in order to take the control of this load and change its status, i.e., turning on and off the load with the objective of destabilizing the system, in other words making the opposite to the demand response device.

Distributed generators are connected to local loads in each node through an inverter and with the system through distribution lines. The distributed generator is modeled as a voltage source inverter, and depending on the load demanded, the voltage source inverter active power output is defined. The generation is modeled taking into account that all the generators can response dynamically to the changes in the network. Moreover each generator has a production cost, a maximum, and a minimum power generation.

$$C_k(P_G) = \left(\frac{2}{cg_k} * \left(\frac{Pg_k - Pg_k^2}{Pg_{max_k} - Pg_{min_k}}\right)\right) \tag{3}$$

$$Pg_{max_k} \geq Pg \geq Pg_{min_k}$$

where cg_k is the production cost of each generator, Pg_{max_k} and Pg_{min_k} are the maximum and minimum power generated by each generator, respectively.

Equations (3) and (1) are used since the integral logistic function can represent the system progress through time [16]. Then, modeling the utility functions of the system (generators and consumers) and the interrelation between them can be seen that cost and loads could be varying in the time, it implies that the system could optimize its behavior if it is appropriately controlled. In the next section, we present the cyber-physical attacks that affect a power system, we highlight those that can occur in distribution systems or Microgrids.

III. Attack Description

One of the main issues in the smart grid era is the raising attacks in communications systems. These attacks could be classified into three groups depending on the objective [17]. First, it is the attack directed to generators, second is the directed to the transmission and distribution lines. Finally, the last one is the attack that is directed to the consumers. The attack directed to the costumers could be classified within three types of attack. Those that could influence a load in order to spend more energy, e.g., data centers require more energy if they have more computing load. On the other hand, it is the attack that acts directly on the load, changing its behavior. Finally there is the attack that acts indirectly on the load, e.g. if a demand response device is cheated and receives false information, this device could turn on or off the loads in order to destabilize the system (see Fig 1). The attack considered here is an attack in the costumers, precisely an attack indirectly on the load called dynamic load altering attack. This kind of attack aims to destabilize the frequency of the power grid through unexpected changes of load. It is assumed that the attacker hack into a demand response (DR) program in order to perform a controller which makes the opposite actions to a DR program would do.

It is supposed that load nodes in the system are all controlled by a DR program. This means that all the load nodes have a portion of vulnerable load. As it will be described in Section V. The attacker controller is a proportional control designed in such a way that modify the load. An amount of load is added during a period of time, then, it is removed during another period of time, the same action is done in a repeatedly way.

IV. Transactive Control Design

The main contribution is to develop an algorithm for improving the resilience interdependent systems, power and

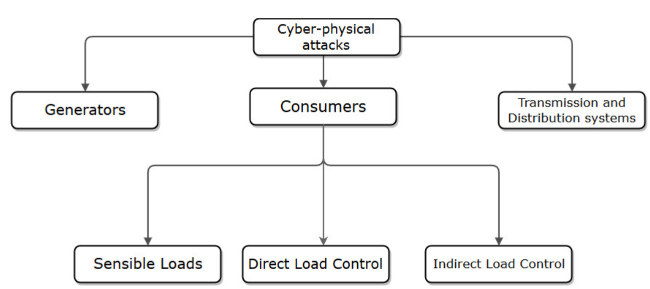

Figure 1. Types of cyber-physical attack in power systems

communications networks, considering distributed generators based on transactive control under DLAA attacks. Transactive control find the optimum equilibrium point based on the energy which must be generated by each generator. Moreover, the energy which should be consumed by the end user in order to minimize the generators cost and maximize the users utility. This is represented by the equation (4).

$$S_W = \sum_{i=0}^{M} U_i(P_D) - \sum_{k=0}^{N} C_k(P_G) \tag{4}$$

where $U(P_D)$ are the utility functions of the consumers and $C(P_D)$ are the utility functions of the generators. Equation (4) is taken from (1) and (3). M is the number of consumer units, and N is the number of generators.

The main goal is to maximize (4) as it is shown in the following problem:

$$\begin{aligned} \text{Maximize} \quad & S_W \\ \text{Subject to} \quad & \sum_{i=1}^{M} P_{D_i} - \sum_{k=1}^{N} P_{G_k} = -P_L \\ & P_{gmax} \geq P_g \geq P_{gmin} \qquad \forall N \\ & P_{dmax} \geq P_d \geq P_{dmin} \qquad \forall M \end{aligned} \tag{5}$$

Constraints could be represented by a matrix as $\mathbf{Rp} = \mathbf{r}$, where $\mathbf{p} = [P_{g1}, P_{g2}, ..., P_{gN}, P_{d1}, P_{d2}, ..., P_{dM}]^\top$ this is made possible by transforming inequalities through slack variables. In order to resolve the optimization problem (5), we have used population dynamics models [6]. Population dynamics represent how a pure population strategy progress through time. The replicator dynamics consider a N finite number of generators, who adopt a ith strategy from a finite set of pure strategies. Accordingly, to achieve an appropriate performance in steady state, the load demanded power should be the sum of all power set points [7].

The payoff function is associated with the chosen strategy, therefore, we also use a continuous time implementation. In its general form, the replicator dynamics can be represented as

$$\dot{x_i} = \beta x_i (F_i - \bar{F}) \tag{6}$$

where $x = [x_1, \ldots, x_{N+M}] = [P_{G_k}, P_{D_i}]^\top$, β is a speed parameter for the convergence of the replicator dynamics, f_i is the fitness function associated with each strategy, and $\bar{f}$ is the average fitness function [6]. In this work, we use replicator dynamics (6) to solve the economic dispatch problem dynamically. In order to integrate the restrictions within the replicator dynamics use the Lagrange function

$$L(p, \mu) = S_W + \mu^\top (\mathbf{Rp} - \mathbf{r}) \tag{7}$$

Where μ is the lagrange multipliers, the fitness functions of the game are defined as $F(p) = \left[F_1, F_2, ..., F_{(N+M)}\right]^T = \nabla_p L$ and $F(\mu) = \nabla_\mu L$. Hence the fitness functions are

$$\nabla_p L(\mathbf{p}, \mu) = \nabla S_W(\mathbf{p}) + \mathbf{R}^\top \mu \tag{8}$$

$$\nabla_\mu L(\mathbf{p}, \mu) = -\mathbf{Rp} + \mathbf{r} \tag{9}$$

The average of these fitness functions is

$$\bar{F} = \sum_{j=0}^{N} p_j * F_j$$

Here p_j is the power in each agent and F_j is the fitness function associated with this variable. In fact, this process is made two times, i.e, for each fitness equation (8) and (9) we have a fitness average function. This optimization can be made it due to the fitness functions used to represent the model are convex functions. With the above optimization problem, the microgrid can be controlled optimally taking into account not only maximizing the profits of the generators but also maximizing the profits of the users. In order to test the above algorithm the next section present a case study where the algorithm was tested obtaining strong results.

V. Case Study

For test purposes, a microgrid has been implemented in Matlab/Simulink to research about the behavior of the proposed approach. The system that we chose was a WSCC 9-bus system. In this system, we have three distributed generators, these generators are independent and they have communications between them as can be seen in Fig 2. Furthermore, we have three loads in the system, these loads are balanced and have a demand response device. These demand response devices aim to optimize the load in order to obtain the best benefit.

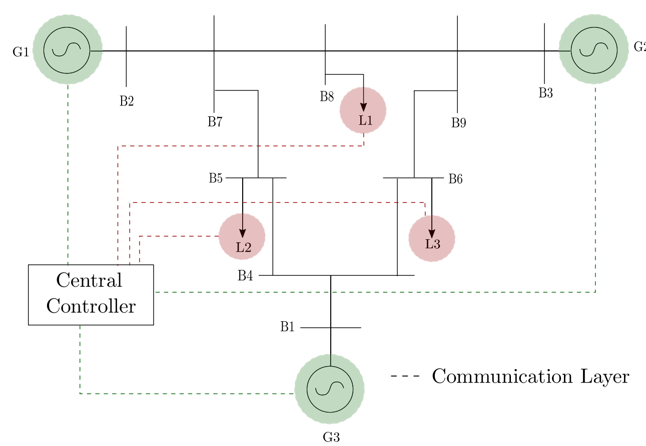

Figure 2. Illustrative general scheme of a microgrid adopted from a WSCC 9-bus with the communication network topology between distributed generators.

The table with the main data is shown in Table I

In order to make a DLAA, we assume that 500 W are vulnerable load, that could represent a 10% of the maximum demanded load. To compare the validate of our results we made two test, one without attacks and other under attacks and we could see how the response changes.

For illustration purposes, it is used a WSCC 9-bus test feeder system shown in Fig. 2.

Table I
SYSTEM PARAMETERS IN SIMULATION

General system parameters	
System Frequency ωref	60 Hz
Voltage Reference Eref	110 V
ω min	59.5 Hz
Emin	110 V
Plvulnerable	500 W
Line Impedance (Z)	1 Ω
Subsystem parameters	
Pgmax1, Pgmax2, Pgmax3	3600, 3000, 2000 W
Pgmin1, Pgmin2, Pgmin3	30, 30, 20 W
Pdmax1, Pdmax2, Pdmax3	1500, 1500, 1000 W
Pdmin1, Pdmin2, Pdmin3	30, 30, 20 W
cg1, cg2, cg3	12, 5, 10
vd1, vd2, vd3	1, 2, 0.5

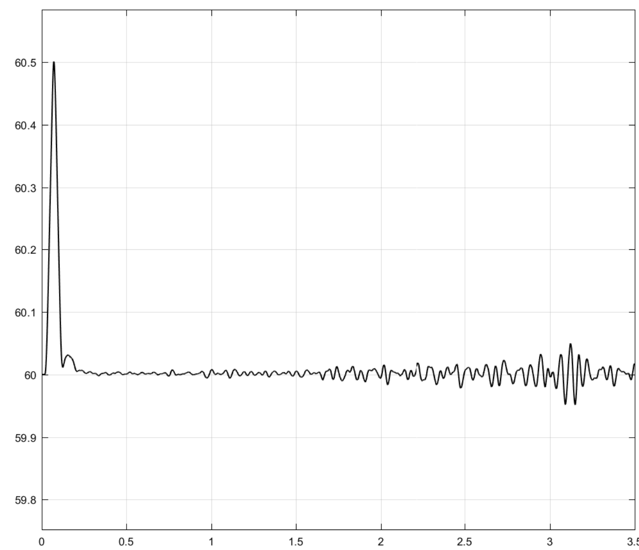

Figure 3. Frequency response of the system without attack.

A. Simulations and Results

The simulations was made during three point five seconds, in where the system was attacked three times, the attack was executed in periods of 1 second where the load is turning on and off once each 200ms, in order to destabilize the system all the vulnerable load was used by the attacker (500 W), the system respond immediately to the attack raising or lowering the power generated. In the same way, the power demanded changes in order to preserve the stability of the system.

The system without an attack is stabilized in 0.2 seconds and remains in stable mode until the end of the simulation. It is shown that the frequency remains stable around 60 Hz. Nonetheless, there is a peak in the frequency due to the initial conditions, in other words, the natural imbalance between load and generation at the beginning of the simulation and then stabilizes in the nominal frequency, i.e, 60 Hz. Additionally, is shown that the system has its optimum performance in 3000 W.

The behavior of the system under attack is different in order to preserve the stability, when the vulnerable load is changed in the system there are a peaks in the frequency which are quickly countered and the frequency returns to 60Hz. The peaks in the frequency are produced by the edges in the load variations. For this reason, it is necessary for the attacker attack with all the vulnerable load in instant of time, these peaks are dissipated in a time of 0.1 seconds and have a maximum magnitude of 60.28 Hz which is within the levels to keep the system stable and with a continuous service provision. However the system cannot resist DLAA with a load variation greater than 25%, in this point the system is destabilized and the frequency fall under 59.5 Hz.

During the attack the system maintains its optimality conditions, increasing in greater proportion the power generated from the cheapest generator. It is important to highlight that we assume that the generators can response almost instantly.

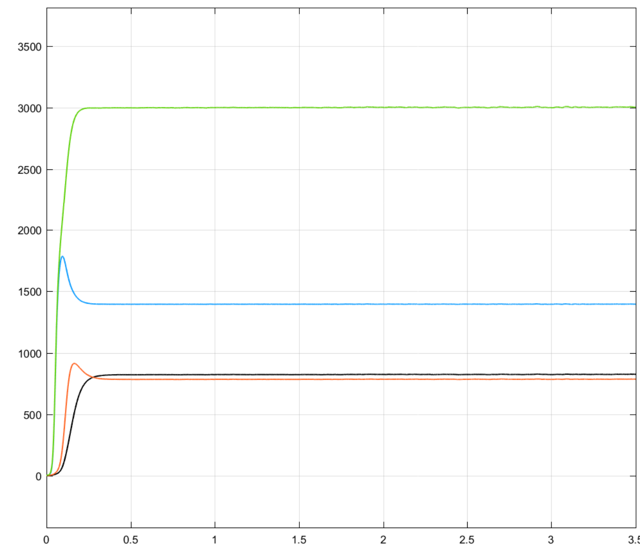

Figure 4. Power response of the system without attack. The green line correspond to the demanded load. The black, blue and orange line correspond to Pg_1, Pg_2 and Pg_3 respectively

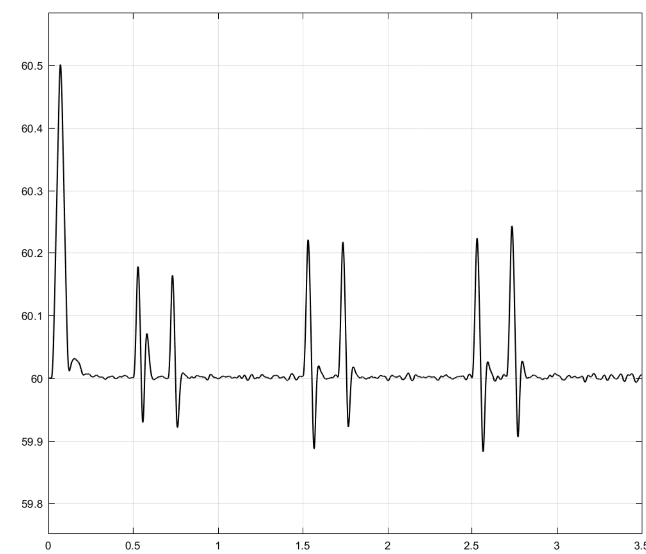

Figure 5. Frequency response of the system under attack.

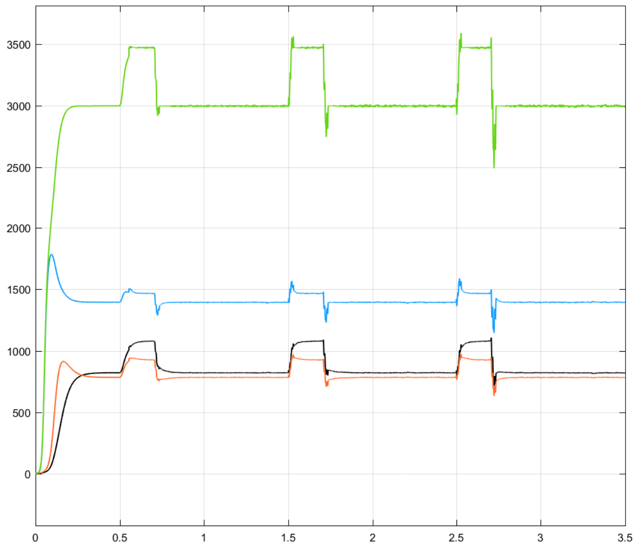

Figure 6. Power response of the system under attack.The green line correspond to the demanded load. The black, blue and orange line correspond to Pg_1, Pg_2 and Pg_3 respectively

Nonetheless, the load respond slowly than the generators and do not change the load instantly.

VI. Conclusions and Future Work

Based on transactive control framework, new economical strategies in the dispatch of distributed generators and consume of the users in microgrids have been proposed. It is possible to implement a new controller that is able to control the system in order to optimize and guarantee the constraints. We have considered some constraints in the generators and consumers with satisfactory results. Then we have obtained an optimal solution than includes, technical, economical and ensures the maximum social welfare of generators and consumers dynamically. As a future work, this algorithm need includes other constraints like lines losses, maximum generation rates, i.e, taking into account that a generator cannot change its generation instantly. Furthermore, it is necessary to consider other populations in the Microgrid like power storage (batteries), loads with different behavior, such as houses, industries and commerce.

References

[1] a. Kiani and a. M. Annaswamy, "Distributed Hierarchical Control for Renewable Energy Integration in a Smart Grid," *IEEE PES Conference on Innovative Smart Grid Technologies*, pp. 1–8, 2012.

[2] J. Hu, G. Yang, and H. W. Bindner, "Network constrained transactive control for electric vehicles integration," *IEEE Power and Energy Society General Meeting*, vol. 2015-Septe, pp. 1–5, 2015.

[3] K. Kok and S. Widergren, "A Society of Devices: Integrating Intelligent Distributed Resources with Transactive Energy," *IEEE Power and Energy Magazine*, vol. 14, no. 3, pp. 34–45, 2016.

[4] D. J. Shiltz, M. Cvetković, and A. M. Annaswamy, "An Integrated Dynamic Market Mechanism for Real-Time Markets and Frequency Regulation," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 2, pp. 875–885, 2016.

[5] J. Hu, G. Yang, K. Kok, Y. Xue, and H. W. Binder, "Transactive control: a framework for operating power systems characterized by high penetration of distributed energy resources," *Journal of Modern Power Systems and Clean Energy*, pp. 1–14, 2016.

[6] N. Quijano, C. Ocampo-martinez, J. Barreiro-gomez, G. Obando, A. Pantoja, E. Mojica-nava, and P. O. C. C. Ocampo-martinez, "The Role of Population Games and Evolutionary Dynamics in Distributed Control Systems," *IEEE Control Systems*, vol. 37, no. 1, pp. 70–97, 2017.

[7] E. Mojica-Nava, C. Barreto, and N. Quijano, "Population Games Methods for Distributed Control of Microgrids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2586–2595, 2015.

[8] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct 2010, pp. 226–231.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[10] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[11] A. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec 2011.

[12] A. K. Marnerides, P. Smith, A. Schaeffer-Filho, and A. Mauthe, "Power consumption profiling using energy time-frequency distributions in smart grids," *IEEE Communications Letters*, vol. 19, no. 1, pp. 46–49, Jan 2015.

[13] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, August 2012.

[14] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, July 2014.

[15] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2015, pp. 1–5.

[16] N. F. Britton, *Essential Mathematical Biology*, 2003, vol. 53, no. 9.

[17] A. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.