Web-Based Platform for Evaluation of Resilient and Transactive Smart-Grids

Conference Paper · March 2019

DOI: 10.1109/MSCPES.2019.8738796

4 authors, including:

Harsh Vardhan
Vanderbilt University
5 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Web-Based Platform for Evaluation of Resilient and Transactive Smart-Grids

Himanshu Neema , Harsh Vardhan, Carlos Barreto, and Xenofon Koutsoukos
Institute for Software Integrated Systems, Vanderbilt University, Nashville, TN, USA

***Abstract*—Today's smart-grids have seen a clear rise in new ways of energy generation, transmission, and storage. This has not only introduced a huge degree of variability, but also a continual shift away from traditionally centralized generation and storage to distributed energy resources (DERs). In addition, the distributed sensors, energy generator and storage devices, and networking have led to a huge increase in attack vectors that make the grid vulnerable to a variety of attacks. The interconnection between computational and physical components through a largely open, IP-based communication network enables an attacker to target physical damage through remote cyber-attacks or attack on software-controlled grid operations via physical- or cyber-attacks. Transactive Energy (TE) is an emerging approach for managing increasing DERs in the smart-grids through economic and control techniques. Transactive Smart-Grids use the TE approach to improve grid reliability and efficiency. However, skepticism remains in their full-scale viability for ensuring grid reliability. In addition, different TE approaches, in specific situations, can lead to very different outcomes in grid operations. In this paper, we present a comprehensive web-based platform for evaluating resilience of smart-grids against a variety of cyber- and physical-attacks and evaluating impact of various TE approaches on grid performance. We also provide several case-studies demonstrating evaluation of TE approaches as well as grid resilience against cyber and physical attacks.**

***Index Terms*—Power-grid simulation, smart-grids, transactive energy, power-grid security, resilience, modeling and simulation, collaboration platform, design studio.**

I. Introduction

The power-grids of today are transforming dramatically in a number of ways to become much more digitally controlled as well as intelligently operated [1] [2]. Several new features have emerged that make a power-grid more 'smart'. The key aspect being increased participation by consumers in the demand response. The increased digital connectivity and access to sophisticated meters has enabled the power consumers to make more informed decisions about how much and when to consume power. In addition, increased availability of DERs (e.g., solar panels, wind turbines, and storage batteries) has enabled consumers to send excess power back to the grid. These consumers are referred to as '*prosumers*' as they both produce and consume power. Thus, the model of previously largely centralized electrical grid is morphing heavily into a rather distributed grid with smart meters, and one that must be managed for demand response in a dynamic manner.

Fig. 1 depicts a large number of concerns that must be addressed for a holistic evaluation of smart-grids as well as several higher-level objectives for their end-to-end analysis.

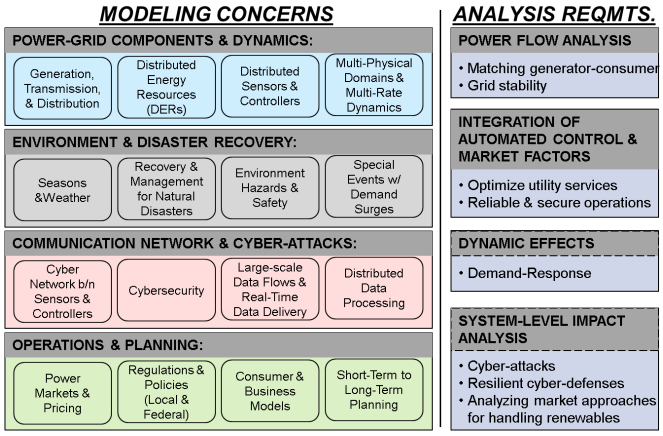

Fig. 1: Smart-Grid Modeling & Evaluation Requirements

The increase in DERs and sophisticated control methods has enabled multiple power markets and mirco-grids to co-exist. This makes power-grids even more dynamic and complex to manage. *Resilient power-grids* have enough redundancies, security mechanisms, and diversity built into its components and systems such that the overall grid operations are not excessively impacted even in the presence of cyber- and/or physical disruptions. *Reliable power-grids* are not only resilient, but also provide an assurance of the availability, quality, and security of the power supply. Managing resilience and reliability of smart-grids in a way that addresses all of the concerns depicted in Fig. 1 is highly challenging. Yet the DERs and digital connectivity among them enables one to operate grid more efficiently by dynamically managing the demand response through economic and digital control techniques such as Transactive Energy (TE) [3]. However, analyzing different TE approaches and evaluating grid for resilience against attacks requires a comprehensive platform that supports end-to-end analysis of a various grid configurations.

A significant concern due to increased DERs and digital control is a huge increase in grid's attack surface. Grids are more vulnerable to a variety of attacks, both cyber and physical. Grid's physical components and the digital monitoring and control equipment are interconnected using largely Internet Protocol (IP) based communication networks. This can enable adversaries to deploy sophisticated cyber-attacks to disrupt the critical grid operations and even cause blackouts. For example, the cyber-attack deployed on Ukraine power-grid caused many substations to fail leading many communities

without power [4]. Adversaries could also deploy *integrity* attacks that modify network packets in a subtle manner such that the attack becomes apparent only after its cumulative effect over time. In addition, faults can be introduced to cause spikes in demand response, and as these components exchange sensor data and control inputs, attacks causing faults in one component can result in *cascading faults* throughout the grid.

Continuous monitoring using edge devices and smart meters can help with detecting attacks on the grid. However, operating the grids that deploy large number of DERs is still highly challenging [5]. Evaluation of grid operations with DERs and transactive energy systems, along with impact of cyber- and physical-attacks, require a comprehensive platform where different combinations of such scenarios can be analyzed for a variety of grid configurations.

This paper describes a novel web-based platform that allows evaluating smart-grids for resilience against cyber-physical attacks and for their behavior when different transactive energy approaches are used. The platform provides a highly configurable and extensible web-based metamodeling environment to model power-grids, market behavior, and various attack configurations. This platform also provides a *simulation backend* for power-grid simulation (using GridLAB-D [6]) of the modeled grid configurations and experiments. Section II presents the overall architecture of the platform including the workflow for using it for smart-grid evaluations, as well as how the entire system is implemented. In Sections III and IV, we respectively describe how power-grids should be evaluated against cyber-physical attacks and for transactive energy approaches. A few relevant use-cases are demonstrated with experiment results in Section V. Finally, Section VI concludes the paper and highlights directions for future work.

II. Platform Architecture

The platform [7] aims to provide a web-based platform for modeling and simulating power-grids that supports evaluation of grid operations for different transactive energy (TE) approaches and evaluating grid's resilience against variety of cyber-physical attacks. It is accessible via a web-browser and does not require any software installations. Fig. 2 shows the modeling and simulation workflow for using the platform. The optional elements are shown by dashed boxes. The user starts with modeling the grid, which can also be input optionally as an external input as a *GridLAB-D model* file (.GLM). Other configurations for time-series parameter values can be input as *player* files. Statistics to collect from simulation can be specified in *recorder* files. *Weather* information - relevant to many grid modules like solar panels - can also be provided. The grid model can directly be simulated in the *backend*. Several *global* parameters are also supported such as the physical time being simulated (e.g., to match against weather data). Researchers can also experiment with different market and cyber-physical attack models in the grid simulation. Upon simulation completion, the results including recorder statistics are given to the user. Continues feedback is also presented to monitor the simulation progress.

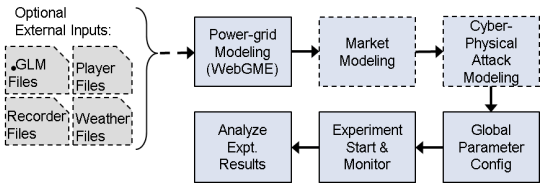

Fig. 2: Modeling & Simulation Workflow

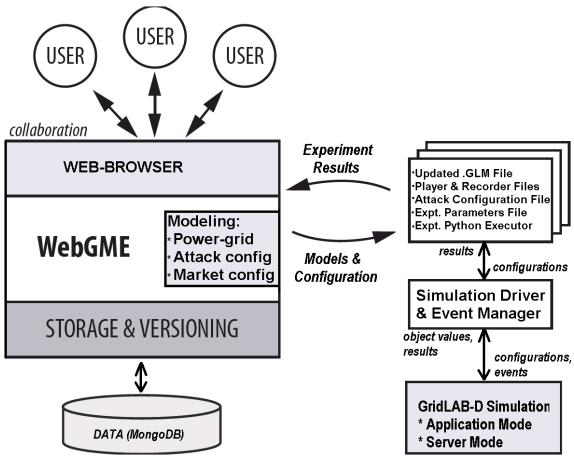

Fig. 3: Implementation Architecture

A. Overview

As shown in Fig. 3, the platform utilizes a web-based metamodeling framework, called WebGME [8], to provide a graphical modeling language for designing power-grids based on concepts from the GridLAB-D simulator. The language also allows modeling different market approaches and attack configurations. When GridLAB-D adds or modifies its concepts, those can be automatically imported in the language. A model interpreter can automatically synthesize executable code and associated configurations for setting up and running corresponding power-grid simulations. Experiment results are also provided to the user using the same interface. WebGME also permits multiple users to collaborate on the model simultaneously by maintaining change history and versions through a MongoDB database. Our platform is hosted on the CPS-VO portal [9] that enables creating users and user-groups, managing authentication and authorization, and providing secure and private collaboration among group users.

Fig. 4 shows a sample grid modeled in our platform. It consists of a grid with two *nodes* connected through *underground line* (green dashed line). Each *node* is connected to primary side of center-taped *transformer*. The secondary side of *transformer* is connected with *triplex node*, which itself is connected to *triplex meters* using *triplex overhead lines*. There is one *triplex meter* for each *house*, which provides net-metering. Each *house* is connected through a *zip-load* and a *water-heater*. One of the *net-meter* (triplex meter) is connected to a *solar-inverter* pair through another meter which measures the power generated by *solar-panel*. The *solar-panel* generates power based on climate data (as TMY3 file

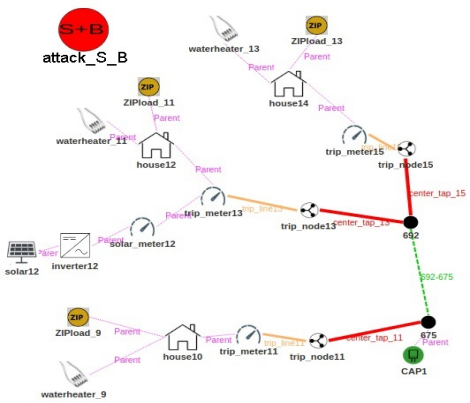

Fig. 4: Sample Grid Model with Attack Configuration

from NOAA), power rating, and other parameters. The grid is simulated using initial parametric values and using *forward-back sweep* method. Component 'attack_S_B' (in red) is an *attack configuration* for both seller and buyer prices. The platform provides a library of many such components.

B. Simulation Backend

The backend of our platform consists of a *Simulation Driver & Event Manager* module (Section II-C) and a configurable GridLAB-D simulation infrastructure in a cloud environment. We chose GridLAB-D power-grid simulator as it is open-source, calculates power-flow variable values before every simulation step, and supports modeling of end-use load models that incorporate weather and market behaviors. This enables modeling of distribution systems and evaluation of DERs and TE approaches. However, precise description of events must still be supported in an efficient way when large power-grid components are used. An additional challenge is that GridLAB-D restricts the parameters to be linear combinations of variables. Our platform overcomes these challenges by extending high-level modules in GridLAB-D for supporting power-grid simulations with capability to model market variations as well as attacks that are *specific* (e.g., on a single component) or *generic* (i.e., affecting multiple components).

C. Simulation Driver & Event Manager

As shown in Fig. 3, the WebGME generated artifacts are sent to a *Simulation Driver (SM) & Event Manager (EM)* module. *SM* executes and controls the simulation. *SM* executes GridLAB-D simulation in *server mode* if attacks or market approaches are configured because that requires adding new events during run-time. Algorithm 1 describes the behavior of *EM*. *EM* processes the schedules specified in WebGME to create corresponding events-list for grid objects. The simulation loop incorporates the actions with intervening pauses during which object values are updated.

D. Modeling Physical Attacks

We leverage the *reliability* module from GridLAB-D to model physical attacks that disconnect segments of the grid.

Algorithm 1 Event manager

Require: List of schedules, start time t_0, and stop time t_f.

```
Pause the simulation at t_0.
Add future events from schedules in an ordered list.
t ← t_0
while t ≤ t_f do
    Wait for a pause in the simulation.
    Update the simulation time t.
    for Each event occurring at time t do
        Execute the event.
        Update the list of future events.
    Continue the simulations.
```

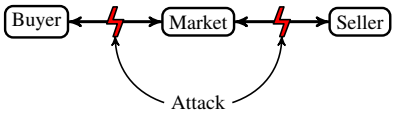

Fig. 5: Exploiting Market Infrastructure for Attacks

The reliability module allows the analysis of the system's state before and after a fault, but ignores the transient between these states. Moreover, it only handles faults in lines, fuses, and switches, causing topology changes (e.g., disconnections).

We simulate attacks creating events that change the connectivity of the system's conductors (e.g., current flow can be interrupted by changing status of lines to 'OPEN'. Disconnection of specific switches and fuses is also supported.

E. GridLAB-D Extensions

Fig. 5 shows the general structure of a market that accepts bids from both buyers and sellers. Attacks on this market type of system usually pursues two objectives, namely damage the system or profit from the attack. GridLAB-D models represent mostly physical connections among components, except communications for market interactions. A communication network among market participants is not supported. Instead, the components communicate through internal functions.

The market's communication structure makes it difficult to implement the false data injection attacks. The bids sent by controllers to the *Main Market (MM)* cannot be directly modified, but we can estimate them. Secondly, the controllers observe the market's clearing prices, which invalidates the reported fake prices. We handle these by introducing *Auxiliary Market (AM)* (see Fig. 6). Here, the buyer bids directly in *AM* and makes decisions based on the prices in *AM*. We

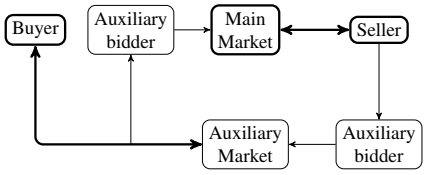

Fig. 6: False Data Injection via Auxiliary Market and Bidder

estimate the bids because precide bids are not observable. Thus, we implement an *Auxiliary Bidder (AB)* that sends the estimated bids to *MM*. *AB* also replicates seller's bids in *AM*, but precisely because in our model seller's bids are constant.

Without external interventions, the models in Figs. 5 and 6 are equivalent. Both markets will reach the same equilibrium if *ABs* make the same bids as the buyer and seller.[1] However, the modification shown in Fig. 6 enables one to modify the bids by targeting the *ABs*.

III. Evaluating Grid Resilience against Attacks

Smart-grids utilize a large number of components which exchange data through largely IP-based communication networks for relaying data. The increased digital connectivity and DERs have made grids highly vulnerable to many different types of cyber-physical attacks. The cyber-attacks could even be carried out in a subtle manner such that they go unnoticed for long periods of time or exploit connectivity among devices to reach remote systems through multi-hop network propagation. Even the physical-attacks on devices can lead to transients in the grid causing faults to propagate to remote regions that were the real intended targets of the attacker.

The attacks mainly serve two purposes for the attackers, viz. derive profit by manipulating the market's prices or damage the system by creating imbalances in the system, which translate into frequency instability. For example, in the aurora attack study, Idaho National Lab used fast opening and closure of the circuit breakers of a generator that desynchronized it and even damaged it permanently. Other attacks against the transmission system could even disconnect lines, transformers, and generators, thus changing the topology of the system.

Depending on how the attack directly impacts the grid operations, they can be classified as *specific* (i.e., on a single component such as solar-panel or a load) or *generic* (i.e., affecting multiple components such as varying the market behavior). In our platform, we support modeling of these types of attacks and executing the power-grid simulation to determine their performance amidst these attacks.

IV. Evaluating Transactive Energy Approaches

Transactive energy (TE) [3] is a distributed management approach that expands electricity markets into the retail domain. The TE paradigm relies on economic and control mechanisms to balance supply and demand dynamically. Some widely analyzed TE price schemes are *time of use* (TOU) rates, *critical peak pricing* (CPP), and *real time pricing* [10]. However, unlike some price mechanisms, the TE can implement a market to allow transactions among the system's elements. However, TE creates uncertainities about grid operations due to the use of DERs, widely varying consumer behaviors, and increased risks associated with the large number of connected and heterogeneous components [11], [12]. Both industry and academia have focused their efforts [13], [14], [15] on evaluating the impact of TE on grid operations. In addition, NIST has organized a large program specifically to address challenges with TE [16].

In our platform, we utilize the modules available in GridLAB-D to support evaluation of TE approaches. For example, using the transactive controller modules - which manage appliances and submit market bids based on both current prices and system's state [17] - we support modeling different market mechanisms [18] such as *buyers-only*, *sellers-only*, and *auctions*. Our platform supports not only the evaluation of different TE approaches, but also allows incorporating cyber-physical attacks on the grid at the same time. Taken together, the platform can be a powerful tool for analyzing a variety of power-grid scenarios with many different types of market and attack models.

V. Experiment Results

A. Power System Model

In this case we make a detailed simulation of an electric distribution system using GridLAB-D and the prototypical distribution feeder models provided by the Pacific Northwest National Laboratory (PNNL) [19]. The distribution models capture fundamental characteristics of distribution utilities from the U.S. In this case, we use the prototypical feeder *R1-12.47-3*, which represents a moderately populated area. Furthermore, we added representative residential loads to the distribution model using the script in [20].

In summary, our distribution model has 109 commercial and residential loads, which in turn incorporate appliances such as heating, ventilation, and air conditioning (HVAC) systems, water heaters, and pool pumps. GridLAB-D allows us to model the response of the loads to weather and market's prices, giving realism to the simulations. In particular, we emulate the temperature in Nashville, TN, during summer time. On the other hand, we assume that the system has 50 generators, that can output a maximum of 2 MW.

B. Attacks Utilized

In our attack scenarios we illustrate attacks that directly manipulate control commands or inject false data in the system. In the first case, the adversary attempts to manipulate the market's equilibrium to profit (e.g., with higher market clearing prices). In this case, the success depends solely on the attacker's capacity to manipulate the market's equilibrium, in other words, in its resources to implement the attack.

In the second case, the adversary exploits the market infrastructure to influence users and induce a peak in demand. Thus, the attacker has to manipulate the market in such a way that the users concentrate their demand at a particular time. The success of this attack depends on both the attack resources and the response of users to the market's equilibrium.

C. Attack scenario 1: Create Peaks in Demand

This attack attempts to create peaks in demand by modifying the prices that the controllers (buyers) observe. Due to the system's restrictions, the adversary cannot change directly the prices that the controllers observe. Instead, it can modify the

[1] In practice, the equilibrium of both the main and the auxiliary markets have minor differences because of errors and delays calculating the bids.

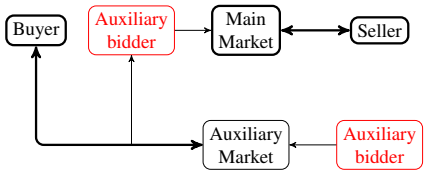

Fig. 7: Market Price Manipulation via Auxiliary Bidders

bids submitted by sellers to the auxiliary market (see Fig. 7). In particular, an adversary with enough resources can decide the future market's price by setting all the bids with the same price. Thus, in the worst case, the adversary has the power to (indirectly) set the prices.

Although manipulating the market's price is essential, the adversary cannot succeed unless the users (or more precisely, the transactive controllers) increase their demand at a particular time. Since the power system has mechanisms to deal with uncertainties demand and operational failures, the adversary must achieve a fast and large imbalance in the system. Hence, the coordination of users plays a critical role.

In this scenario, an adversary targets HVAC with its attack. These controllers choose the appliances set points (which in turn determine the energy consumption) based on the system's state (internal and outdoor temperature) and both the current and previous prices. For instance, the transactive controllers can turn off (on) the HVAC when it observes high (low) prices to reduce the cost of energy. The precise decisions follow the preferences of users (e.g., their tolerance to temperature changes as a function of monetary compensations).

In this case the adversary leverages the behavior of the transactive controllers to create peaks in demand. The attack first increases the price, which forces the HVAC to use less energy at the expenses of allowing higher indoor temperatures. Later, when the indoor temperature is high enough, the attacker suddenly reduces the price. This encourages higher energy usage to reduce the indoor temperature. However, this signal has a coordinating effect that raises the energy demand almost simultaneously, resulting in a demand peak.

1) Experiments: Fig. 8 illustrates the impact of attacks with different resources (fraction of bidders compromised) that causes a demand peak at 12 pm. The attack starts at 10 am, when the adversary modifies the seller's bids to the maximum price accepted by the market (0.63). The high price signal induces demand reduction because the controllers choose a higher cooling set point (see Fig. 9). Despite of the sudden price change, the controllers do not react simultaneously; hence, this first stage doesn't harm the system.

The adversary then lowers the prices suddenly at 12 pm, which changes the cooling set points of HVAC systems (see Fig. 9). By this time, most of the houses had high temperatures. Consequently, the HVACs immediately turn on their cooling systems, creating a demand peak. Fig. 10 shows that peak demand can be created even when attacker compromises only 20% of bidders. despite the lower impact on the market's price.

An attack's timing is crucial for its success. In particular,

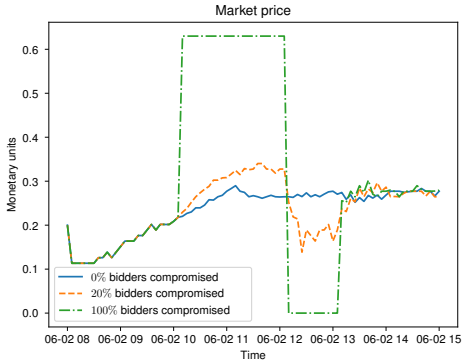

Fig. 8: Market Price Changes by Modified Seller Bids

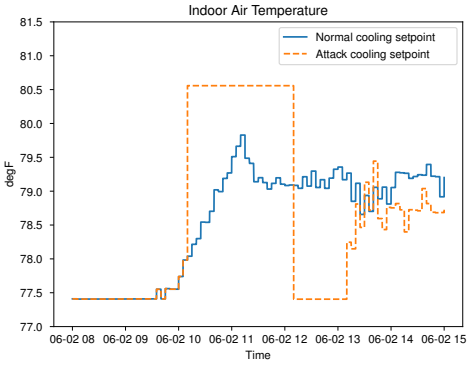

Fig. 9: Indoor Temperature Setpoint of HVAC System

the price change can induce a peak because most of the houses reached high temperatures, which created a coordinating effect in the demand. Thus, the adversary needs continuous access to the cooling system and enough time to execute the attack.

D. Attack Scenario 2: Modifying the Controllers' Bids

This attack seeks to change the bids of the buyers to raise the prices and benefit the sellers. The adversary compromises

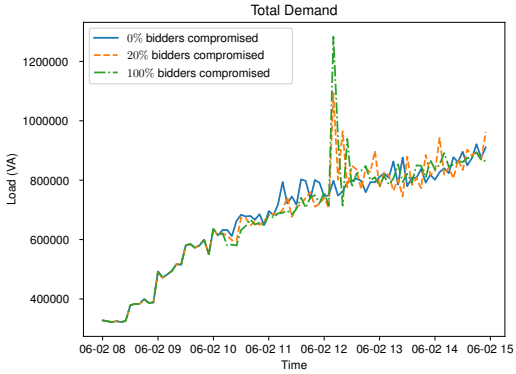

Fig. 10: Demand Peak Created in Attack Scenario 1

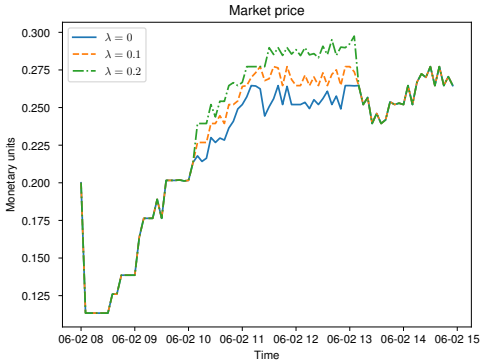

Fig. 11: Deviation in Market Price in Attack Scenario 2

the bids of buyers (controllers) and sends the following price:

$$\hat{p}_c = p_c + \lambda p_m, \tag{1}$$

where p_c represents the price submitted by the controller, p_m represents the market price, λ represents the control parameter, and $\lambda \geq 0$ represents the intensity of the attack. When $\lambda = 0$ the attack doesn't change the bids; however, $\lambda > 0$ raises the bid for energy, which increases the market's clearing price. The adversary may select a small value of λ to prevent attack discovery.

1) Experiments: Fig. 11 show the market prices in the second attack scenario (the attack runs from 10am till 13pm). The deviation from the normal price occurs due to the attack that raises the prices, and depends on the parameter λ.

VI. Conclusions & Future Work

Power-grids are a complex system involving many different components. Recent increase in DERs have put tight operational constraints for balancing power demand and generation. In addition, the increase in digital connectivity among grid components and controllers has significantly increased grid's vulnerability to cyber- and physical-attacks.

Transactive Energy approaches (TE) can mitigate some of the demand response issues and also improve resource utilization and operational efficiency. However, for safe and reliable grid operations to ensure availability, security, and reliability of power supply, the grid must incorporate security mechanisms and redundant and diverse components. These are complex considerations that must be effectively used based on comprehensive evaluations.

In this paper, we described a web-based platform that enables researchers to evaluate such complex considerations. We also presented the platform's implementation architecture and discussed how it can be used to evaluate resilience of smart-grids against a variety of cyber- and physical-attacks and to model and evaluate various TE approaches for their effect on grid performance. We also provided several case-studies with experiment results that demonstrate the platform's capabilities for conducting such modeling and simulation experiments.

In the future, we plan to extend the platform to allow specification of a design of experiments (DOE) for different combinations of topological and parametric variations and to automatically execute simulations for all such combinations. We also plan to extend and further parameterize the current library of reusable models for grid components, markets, and attack configurations. Better visualization of experiment results both during and after simulation is also proposed. Another research direction is apply the platform's tools and techniques for higher-level evaluations such as societal implications of the ongoing increase in renewable energy implementations.

Acknowledgments

This work is supported in part by the NSF FORCES program under grant CNS-1238959, by the NSF PIRE and CPS program under award #1521617, and by NIST under awards #70NANB18H269 and #70NANB17H266.

References

[1] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power and Energy Magazine*, vol. 8, no. 2, pp. 41–48, 2010.
[2] J. J. Conti, P. D. Holtberg, J. A. Beamon, A. M. Schaal, J. Ayoub, and J. T. Turnure, "Annual energy outlook 2014," *US Energy Information Administration*, 2014.
[3] GridWise Architecture Council, "Gridwise transactive energy framework: Version 1.0," *Pacific Northwest National Laboratory, PNNL-22946 Ver 1.0*, 2015.
[4] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.
[5] E. F. Camacho, T. Samad, M. Garcia-Sanz, and I. Hiskens, "Control for renewable energy and smart grids," *The Impact of Control Technology, Control Systems Society*, pp. 69–88, 2011.
[6] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "Gridlab-d: An open-source power systems modeling and simulation environment," in *Transmission and distribution conference and exposition, 2008. t&d. IEEE/PES*. IEEE, 2008, pp. 1–5.
[7] "Power-grid analysis framework," Feb. 2019. [Online]. Available: https://cps-vo.org/group/gridlabd
[8] M. Maróti, R. Kereskényi, T. Kecskés, P. Völgyesi, and A. Lédeczi, "Online collaborative environment for designing complex computational systems," *Procedia Computer Science*, vol. 29, pp. 2432–2441, 2014.
[9] "Cyber-Physical Systems Virtual Organization (CPS-VO)," Feb. 2018. [Online]. Available: https://cps-vo.org
[10] P. Siano, "Demand response and smart gridsa survey," *Renewable and sustainable energy reviews*, vol. 30, pp. 461–478, 2014.
[11] S. Weerakkody and B. Sinopoli, "Challenges and opportunities: Cyber-physical security in the smart grid," in *Smart Grid Control*. Springer, 2019, pp. 257–273.
[12] C. Barreto and A. Cardenas, "Impact of the market infrastructure on the security of smart grids," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2018.
[13] D. J. Hammerstrom, R. Ambrosio, T. A. Carlon, J. G. DeSteese, G. R. Horst, R. Kajfasz, L. L. Kiesling, P. Michie, R. G. Pratt, M. Yao *et al.*, "Pacific northwest gridwise testbed demonstration projects; part i. olympic peninsula project," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), Tech. Rep., 2008.
[14] A. Ohio, "gridsmart (sm) demonstration project," 2016.
[15] R. Melton, "Pacific northwest smart grid demonstration project technology performance report volume 1: Technology performance," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), Tech. Rep., 2015.
[16] "NIST Transactive Energy Challenge," Feb. 2019. [Online]. Available: https://pages.nist.gov/TEChalleng
[17] J. C. Fuller, K. P. Schneider, and D. Chassin, "Analysis of residential demand response and double-auction markets," in *Power and Energy Society General Meeting, 2011 IEEE*. IEEE, 2011, pp. 1–7.
[18] T. Broeer, J. Fuller, F. Tuffner, D. Chassin, and N. Djilali, "Modeling framework and validation of a smart grid and demand response system for wind power integration," *Applied Energy*, vol. 113, pp. 199–207, 2014.
[19] K. P. Schneider, Y. Chen, D. P. Chassin, R. G. Pratt, D. W. Engel, and S. E. Thompson, "Modern grid initiative distribution taxonomy final report," Pacific Northwest National Laboratory, Tech. Rep., 2008.
[20] https://github.com/gridlab-d/Taxonomy_Feeders/tree/master/PopulationScript, 2015, accessed: January 12, 2019.