Proceedings of the 2018 Winter Simulation Conference
M. Rabe, A. A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, eds.

SIMULATION-BASED STOCHASTIC PROGRAMMING TO GUIDE REAL-TIME SCHEDULING FOR SMART POWER GRIDS UNDER CYBER ATTACKS

Yuan Yi, Wei Xie

Department of Industrial and System Engineering
Rensselaer Polytechnic Institute
110 8th Street
Troy, NY, 12180, USA

Zhi Zhou

Energy Systems
Argonne National Laboratory
9700 Cass Ave
Lemont, IL, 60439, USA

ABSTRACT

With the integration of renewable energy and advanced communication technologies, smart power grids can enhance the cost-efficiency and reliability of energy generation, transmission, and distribution. The communication network connecting numerous remotely distributed generators, devices and controllers plays a vital role in the control of power grids. However, it is vulnerable to cyber attacks. In particular, because of its frequency and lasting impact, the Distributed Denial of Service (DDoS) attack poses an important threat to smart power grids. This paper presents a simulation-based stochastic programming approach to guide the unit commitment and economic dispatch decisions, which accounts for the prediction uncertainty of wind power and the impact from DDoS attacks. The case study demonstrates that the proposed approach can lead to a more cost-efficient and reliable operational decision guidance for smart power grids.

1 INTRODUCTION

To overcome the issues of traditional energy systems, including increasing fuel costs, declining system reliability, and limited modernization, the concept of smart power grids was proposed (Lo and Ansari 2012; Fang et al. 2012). They integrate modern technology to improve reliability, power quality and efficiency, being able to ensure electricity delivery from points of generation to end customers in a controlled and interactive manner (Li and Yao 2010). To achieve the goal, smart power grids facilitate real-time monitoring and information sharing to make dynamic decisions. Advanced communication technologies are implemented to establish a two-way dynamic, interactive and high-speed communication system (Zhou et al. 2010; Wang and Lu 2013). It connects numerous devices in the smart grid and plays a crucial role in controlling power generation and production (Wang and Lu 2013).

Such communication network is highly-distributed and hierarchical, which can be classified into three levels: the Home Area Network (HAN), the Neighborhood Area Network (NAN) and Wide Area Network (WAN) (Chhaya et al. 2017). HAN is the lowest tier in the communication network and it only covers a smart home (Wang and Lu 2013). HAN provides information sharing among smart meters and electric appliances in the smart home (Mo et al. 2012; Chhaya et al. 2017). Smart meters serve as gateway device for communication with upper tier devices. They aggregate the information from all appliances in HAN and then communicate with the control center in a bi-directional manner. The communication between smart meters from various HANs and the control center is made through NAN, the intermediate level in the smart grid communication system (Chhaya et al. 2017). A smart grid can have hundreds of NANs, and all NANs are eventually linked together by WAN, which establishes the inter-domain communication. Hence, it is the backbone communication network in a smart grid, and the general concept of the backbone communication network architecture is depicted in Figure 1 (Wang and Lu 2013).

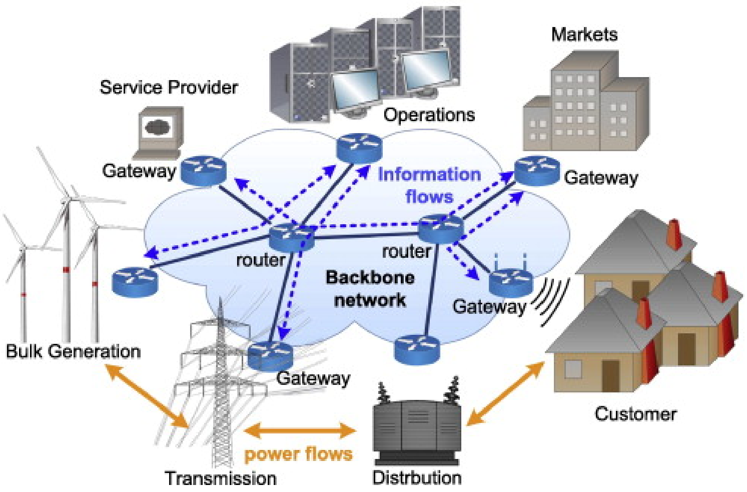

Figure 1: The backbone network in a smart grid.

In the backbone communication, to achieve long distance bulk information transmission, Supervisory Control and Data Acquisition (SCADA) is widely implemented (Niyato et al. 2012; Chhaya et al. 2017). To make the power system more efficient and reliable, the SCADA system adopts the ideas of communication technologies. Thus, it is prone to cyber attacks as follows (Sadi et al. 2015).

- Packet drop attacks. Cyber attackers make packets drop before reaching the intended destination.
- Tampering communication data/signal attacks. The signal and data are delayed and forged by the attackers.
- Distributed Denial of Service (DDoS) attacks. DDoS attacks overwhelm the communication and computational resources of the smart grid with jamming data, which result in delay or failure of data communications (Li et al. 2012; Bhuyan et al. 2015).

Among these attacks, DDoS attacks are ubiquitous and could be long-lasting (Khalimonenko et al. 2017). According to Jin et al. (2011), smart grids are quite vulnerable to DDoS attacks. Furthermore, with the expansive data collection and bi-directional data transmission through the Internet and increasing usage of social media platforms, the likelihood of DDoS attacks against communication network is on the rise, which can bring severe consequences to smart grid operation (Fadlullah et al. 2011).

DDoS can attack gateway devices which enable the information flow between the local power infrastructure and the control center. The gateway devices include smart meters, computers, routers (Wang and Lu 2013). As shown in Figure 1, there exist many gateway devices and DDoS attacks could target any of them. When DDoS attacks occur, the attacked devices are flooded by jamming data, exceeding their processing capability and thus unable to communicate with the control center. As a result, the corresponding generators connected to the attacked devices are unable to receive updated commands from the control center and they have to maintain the current production schedule. Thus, only the remaining unaffected ones can adjust the production levels. Consequently, either the smart grid is unable to produce enough power to satisfy the customer demand, in which case a heavy penalty incurs. Or the smart grid cannot wind down its production and generates too much power, in which case the incurred production cost is unnecessarily costly. Therefore, to control the operational cost, the impact of DDoS attacks should be taken into account when making scheduling decisions for smart power grids.

Due to the slow start constraint of the thermal generators, there exists a two-stage decision making process for power grid scheduling (Ruiz et al. 2009; Tuohy et al. 2009). The first-stage decision is called *the unit commitment*, which is made day-ahead. It determines the on-off status of thermal generators in the planning horizon, i.e., when a thermal generator should be turned on or off. The second-stage decision is called *the real-time economic dispatch*, which determines the actual energy output, i.e., the amount of power generation for those committed generators. Thus, to provide reliable and cost-efficient scheduling for energy systems, the two-stage stochastic unit commitment model integrating unit commitment and real-time economic dispatch is widely used; see Zheng et al. (2015) for a detailed review.

However, to the best of our knowledge, the existing unit commitment literature typically ignores the impact of cyberattacks; see for example Ruiz et al. (2009) and Tuohy et al. (2009). In this paper, we propose a simulation-based unit commitment (SBUC) model for smart grids with high wind power penetration. Here, suppose that only thermal generators can be impacted by DDoS attacks. It means that only commands altering the production schedule sent from the control center are blocked. Further accounting for the impact of DDoS attacks on wind farms is our on-going research, where both the information sharing on the real-time wind energy supply and the commands changing the production output are simultaneously blocked.

Therefore, in the proposed SBUC model, we consider two sources of risk: *the prediction uncertainty of wind power* which is caused by the inherent randomness of wind power generation and *the DDoS attack uncertainty* which arises because DDoS attacks could randomly stymie the communication and disrupt the smart power grid operation. To provide a robust and cost-efficient decision guidance, we propose the two-stage stochastic unit commitment model accounting for both sources of uncertainty.

In addition, we introduce a new constraint to model the system operating process under DDoS attacks. If a committed thermal generator is under attack and thus it losses the communication with the control center, the system operator cannot adjust its power generation. Then, the affected thermal generator continues to operate by following the previous schedule if it is also committed during the last normal communication hour before the DDoS attack. Or, it has the minimum production rate if the thermal generator is turned off when the last communication between the thermal generator and the control center happens. Compared to the classical Stochastic Unit Commitment (SUC) model, our model accounts for the impact of DDoS attacks. Thus, it can lead to more robust and cost-efficient unit commitment decisions.

To solve for the optimal unit commitment decision, the sample average approximation (SAA) is used to approximate the expected future cost occurring in the planning horizon (Shapiro et al. 2009; Wang et al. 2012). A set of scenarios is generated with each scenario representing a possible realization of future wind power prediction and DDoS attacks. Here, suppose that DDoS attackers act independently to target power plants and intrude the gateway devices. The IT team constantly monitors the power grid operation. Once a DDoS attack is detected, they start to tackle the attack and identify the attackers. Then, the power plant communication is back to normal when the DDoS attackers are eliminated. Therefore, the entire process is modeled as a queueing network. Each node is modeled by a $G/G/1$ queue with the cyber attack arrivals. The IT team is regarded as the server who handles the attacks. Discrete-Event Simulation (DES) for the queueing network is employed to generate DDoS scenarios.

The main contributions in this paper can be summarized as follows

- As far as we know, our paper presents the first study considering the impact of cyberattacks on the unit commitment decisions. The proposed model takes random DDoS attack events into account when making decisions, which leads to more robust unit commitment and dispatch decisions hedging against DDoS attacks and renewable energy prediction uncertainty. The case study on a six-bus system indicates our approach leads to more reliable and cost-efficient decisions compared to the traditional unit commitment decision model.
- We propose modeling DDoS attacks on thermal generators by a queueing network. The attack arrival and handling processes at each gateway device are modeled as a $G/G/1$ queue. Then, the discrete-event simulation is used to generate DDoS scenarios. Our proposed approach can be extended to other types of cyber attacks.

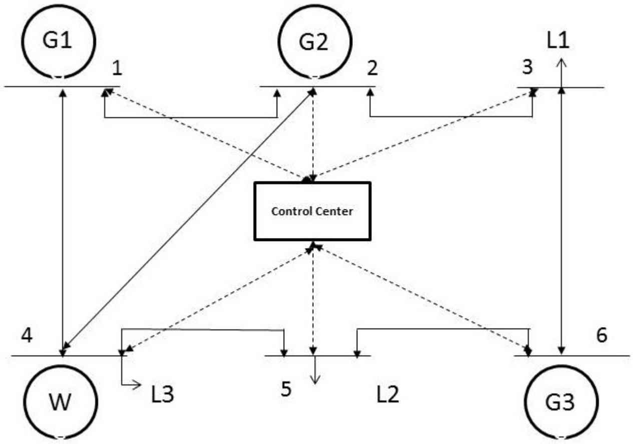

Figure 2: A six-bus system.

The remaining sections are organized as follows. In Section 2, we state the problem of interest and propose our method. In Section 3, we use a six-bus smart grid to empirically study the performance of our proposed model. We draw conclusions and suggest future research directions in Section 4.

2 PROBLEM STATEMENT

We consider a smart power grid system, including both thermal generators and renewable energies. It consists of B buses with I thermal generators and W wind farms. In this paper, we use the six-bus system in Figure 2 for illustration. The three thermal generators are denoted by $G1$, $G2$ and $G3$ located on buses 1, 2 and 6. There is one wind farm, denoted by W, located on bus 4. The power generation needs to meet the loads, denoted by $L1$, $L2$ and $L3$, at Buses 3, 4, 5. The buses are connected by seven transmission lines, denoted by solid lines. The produced electricity can be transmitted through those lines in a bi-directional manner as shown in Figure 2. In the system, a control center is used to guide the electricity production and transmission processes, which is connected to loads, wind farm and thermal generators by the communication network, denoted by the dash lines. Smart meters or computers can serve as gateways for the buses to connect with the control center (Mo et al. 2012; Wang and Lu 2013). The information flow is also in bi-directional fashion. The gateway devices collect and aggregate the load information, and then send it to the control center through the communication network. At the same time, the devices receive commands from the control center and adjust the energy production and transmission.

The decision makers need to make two sets of decisions. The first one is the unit commitment decisions, which is made one day ahead. Denote the unit commitment decision for thermal generator i at the t-th hour as $u_{i,t}$, where $t = 1,\dots,T$ and T represents the planning horizon length. It is a binary variable: $u_{i,t} = 1,0$ means the thermal generator will be on or off at the t-th hour. The second set of decisions is the real-time economic dispatch, which is the actual hourly power production for committed thermal generators and wind farms. Let $P_{i,t}$, $P^{wc}_{w,t}$ and $P^{ens}_{b,t}$ denote the output for thermal generator i, the wind farm curtailment for wind farm w and the amount of unsatisfied demand on bus b at time period t.

The objective is to minimize the expected cost occurring in the planning horizon with length $T = 24$ hours,

$$\begin{aligned}\min \quad G(u_{i,t}) = & \sum_{t=1}^{T}\sum_{i=1}^{I}(C^i F_{mi} u_{i,t} + SU_{i,t} + SD_{i,t}) \\ & + \mathrm{E}\left[\min_{P_{i,t},P^{ens}_{b,t},P^{wc}_{w,t}} \sum_{t=1}^{T}\sum_{i=1}^{I} C^i F_{ai} P_{i,t} + \sum_{t=1}^{T}\sum_{b=1}^{B} C^{ens} P^{ens}_{b,t} + \sum_{t=1}^{T}\sum_{w=1}^{W} C^{wc} P^{wc}_{w,t}\right].\end{aligned} \tag{1}$$

Six types of costs are included in the objective, while the costs, $SU_{i,t}$, $SD_{i,t}$ and $C^iF_{mi}u_{i,t}$, incur at the fist stage and the remaining three incur at the second stage. The start-up cost $SU_{i,t}$ incurs when the generator i is turned on, and it is defined as $SU_{i,t} \equiv P_i^{on}\max(u_{i,t} - u_{i,t-1}, 0)$, where P_i^{on} is the start-up cost per time for generator i. If generator i is not committed at hour $(t-1)$, i.e., $u_{i,t-1} = 0$ while it is committed at hour t, i.e., $u_{i,t} = 1$. Then, $u_{i,t} - u_{i,t-1} = 1$. Hence, a start-up cost for generator i happens at hour t. Similarly, the turn-off cost $SD_{i,t}$ happens when generator i is shut-down and $SD_{i,t} \equiv P_i^{off}\max(u_{i,t-1} - u_{i,t}, 0)$, where P_i^{off} is the turn-off cost per time for generator i. If a generator is committed at hour $(t-1)$, i.e., $u_{i,t-1} = 1$ while it is not committed at hour t, i.e., $u_{i,t} = 0$. Then, the generator is shut down at hour t and a turn-off cost incurs. In addition, once thermal generator i is committed, it has to produce above the minimal production level. Thus, a minimal thermal operation cost incurring at the first-stage is denoted by $C^iF_{mi}u_{i,t}$, where C^i is the fuel price and F_{mi} is the amount of fuel consumption for the minimal output for generator i (Wang et al. 2018). The remaining three costs incur at the second-stage. Since the thermal generator consumes the extra fuel to produce $P_{i,t}$, the additional production cost is $C^iF_{ai}P_{i,t}$, where F_{ai} is the additional fuel consumption requirement needed to generate $P_{i,t}$ power production. If the smart grid could not produce enough energy to satisfy the load demand, a shortage penalty may incur. Then, the penalty cost of non-satisfactory demand for bus b at time period t is $C^{ens}P_{b,t}^{ens}$, where C^{ens} is the unit load shedding price and $P_{b,t}^{ens}$ is the amount of unmet load at bus b in time period t. Lastly, for the wind power, we may not use up all its capacity $P_{w,t}^{c}$ and there exists a wind farm curtailment $P_{w,t}^{wc}$. Since the monetary incentives are provided for wind power production, we loss the monetary reward if we curtail wind farm production (Wang et al. 2018). Then, the wind curtailment cost at the t-th hour for wind farm w is $C^{wc}P_{w,t}^{wc}$, where C^{wc} is the per unit monetary reward for the wind production and $P_{w,t}^{wc}$ is the amount of wind curtailment.

The smart power grids composing of power system and its communication network can be studied as a cyber-physical system. In the unit commitment problem, various sources of uncertainty exist. On the physical side, there exists the wind power prediction uncertainty (Zhou et al. 2013; Hargreaves and Hobbs 2012; Jiang et al. 2012). In addition, the load could be uncertain. However, in the short term, the prediction on wind energy is much more uncertain than the load forecasting (Bessa et al. 2012). Hence, without loss of generality, we assume that the load demand is deterministic in our formulation (Tuohy et al. 2009; Wang et al. 2018).

On the cyber side, there exists the DDoS attack uncertainty. When a DDoS attack occurs, it prevents the normal communication between attacked thermal generators and the control center. If the time-sensitive real-time dispatch decisions made by the control center are impacted by DDoS attacks, the affected thermal generator cannot receive the command on time, which can cause the disruption of smart grid operation (Lu et al. 2011). Since both DDoS attacks and wind power generation uncertainty bring sudden and unexpected changes to smart grid power production, they should be accounted for. Let ξ and η represent random wind power generation and DDoS attack events. Therefore, the expectation in Objective (1) is taken over both ξ and η.

Constraints in Equations (2)–(8) are for both first- and second-stage decision variables. The first stage decision variable $u_{i,t}$ is binary. Any thermal generator i must keep the same operating status for a minimal amount of time and it cannot be changed too frequently. Specifically, if generator i is turned on at time t, it must keep operating for a minimum of T_i^{on} hours (Wang et al. 2018). At the same time, if generator i is turned off at time t, it has to be off for a minimum of T_i^{off} hours. Constraints (2) and (3) formulate the minimum up and down time requirements. To give readers a better understanding how these two constraints work, we use the six-bus system in Figure 2 as an example for demonstration. In the six-bus system, the thermal generator $G1$ has a four-hour requirement for both minimum on and off requirements, i.e., $T_1^{on} = 4$ and $T_1^{off} = 4$. Suppose that $G1$ is turned on at the 9-th hour. It means $u_{1,9} = 1$ while $u_{1,8} = 0$. Hence, $u_{1,9} - u_{1,8} = 1$. Equation (2) dictates that $u_{1,k} \geq u_{1,9} - u_{1,8} = 1$ for $k = 9, \ldots, 12$. Hence, $u_{1,9} = u_{1,10} = u_{1,11} = u_{1,12} = 1$ is mandated in Equation (2). Similar restrictions can be obtained from Equation (3) if $G1$ is turned off at 9-th hour, in which case, $u_{1,9} = u_{1,10} = u_{1,11} = u_{1,12} = 0$.

$$u_{i,t} - u_{i,t-1} \leq u_{i,k} \quad \forall k = t, \ldots, \min(T, t + T_i^{on} - 1) \tag{2}$$

$$u_{i,k} \leq 1 + u_{i,t} - u_{i,t-1} \quad \forall k = t, \ldots, \min(T, t + T_i^{off} - 1) \tag{3}$$

$$\sum_{i=1}^{I} P_{i,t} + \sum_{w=1}^{W} (P_{w,t}^{c} - P_{w,t}^{wc}) = \sum_{b=1}^{B} (P_{b,t}^{D} - P_{b,t}^{ens}) \tag{4}$$

$$-PL_{\ell,\max} \leq \sum_{b=1}^{B} G_{\ell-b} P_{b,t}^{D} + \sum_{i=1}^{I} G_{\ell-i} P_{i,t} + \sum_{w=1}^{W} G_{\ell-w} (P_{w,t}^{c} - P_{w,t}^{wc}) \leq PL_{\ell,\max} \tag{5}$$

$$u_{i,t} P_{i,\min} \leq u_{i,t} P_{i,t} \leq u_{i,t} P_{i,\max} \quad \forall i, \quad \forall t \tag{6}$$

$$u_{i,k} P_{i,k} = u_{i,k} \cdot [u_{i,t-1} P_{i,t-1} + (1 - u_{i,t-1}) P_{i,\min}] \quad \forall k = t, \ldots, \min(T, t') \tag{7}$$

$$u_{i,t} \quad \text{binary} \tag{8}$$

For second-stage economic dispatch decisions $P_{i,t}$, $P_{w,t}^{wc}$ and $P_{b,t}^{ens}$, four sets of constraints exist. Constraint (4) is the nodal power balance equation, which enforces the amount of production by wind farms and thermal generators equal to the amount of power consumption. Notice $\sum_{w=1}^{W} (P_{w,t}^{c} - P_{w,t}^{wc})$ is the actual wind farm production and $\sum_{b=1}^{B} (P_{b,t}^{D} - P_{b,t}^{ens})$ is the actual amount of demand the smart grid is able to satisfy, where $P_{b,t}^{D}$ denotes the load from bus b at time t. Constraint (5), called the DC power flow constraint, models the power flows through the transmission network (Van den Bergh et al. 2014; Wang et al. 2018). The total power flow on any transmission line ℓ is $\sum_{b=1}^{B} G_{\ell-b} P_{b,t}^{D} + \sum_{i=1}^{I} G_{\ell-i} P_{i,t} + \sum_{w=1}^{W} G_{\ell-w} (P_{w,t}^{c} - P_{w,t}^{wc})$ and it must be within a specified range, denoted by $[-PL_{\ell,\max}, PL_{\ell,\max}]$, where $G_{\ell-b}$, $G_{\ell-i}$ and $G_{\ell-w}$ are corresponding shift factor matrices for transmission line ℓ. For a detailed introduction on the DC power flow, see Van den Bergh et al. (2014). The actual output from generator i must be within a predetermined range, between the minimum output $P_{i,\min}$ and the maximum $P_{i,\max}$. Constraint (6) enforces that requirement.

Finally, Constraint (7) stipulates the power production constraint resulted from DDoS attacks. DDoS attacks affect the smart grid operation if they delay the delivery of the time-critical real-time dispatch commands. Specifically, suppose the control center sends the t-th hour real-time dispatch decision exactly at the t-th hour sharp to generators. If a DDoS attack on generator i is launched right before the t-th hour and ends right after hour t'. Then, between hour t and t', the communication between the control center and the generator is not available. Hence, the last information update of generator i happens at the $(t-1)$-th hour and the communication resumes its normal function after the t'-th hour. Therefore, if generator i is committed any time between t-th hour to t'-th hour, it cannot receive the corresponding dispatch command from the control center during the attack. Specifically, if generator i is committed at the k-th hour during the attack, the generator either operates based on the last available production command from the $(t-1)$-th hour if generator i is also committed at time $t-1$. Or, the generator i keeps the minimum output level $P_{i,\min}$ if the generator is turned off at hour $t-1$.

We use the six-bus system in Figure 2 to demonstrate how Constraint (7) works. Suppose that the thermal generator $G1$ is attacked by DDoS cyber-attackers and loses its connection with the control center. The attack is launched before the 9-th hour and ends after the 11-th hour. Then, three hours are affected, namely, $t = 9, 10, 11$ and the last communication between $G1$ and the control center occurs at the 8-th hour. During the three-hour period, $G1$ cannot receive the updated commands to alter its power production if it is committed. If $G1$ is also committed during the 8-th hour, i.e., $u_{1,8} = 1$, for any committed hour during the attack period, its energy generation is set equal to that at the 8-th hour, $u_{1,k} P_{1,k} = u_{1,k} P_{1,8}$, for $k = 9, 10, 11$. Otherwise, $G1$ is turned off at 8-th hour, i.e. $u_{1,8} = 0$, there is no existing power production schedule. Then, the minimal output is maintained for any committed hour during the three-hour attack period, $u_{1k} P_{1,k} = u_{1,k} P_{1,\min}$, for $k = 9, 10, 11$. Combining these two cases, we obtain Constraint (7).

2.1 Scenario Generation

Since $\mathrm{E}[\min_{P_{it},P_{bt}^{ens},P_{wt}^{wc}} \sum_{t=1}^{T}\sum_{i=1}^{I} C^i F_i P_{i,t} + \sum_{t=1}^{T}\sum_{b=1}^{B} C^{ens} P_{b,t}^{ens} + \sum_{t=1}^{T}\sum_{w=1}^{W} C^{wc} P_{w,t}^{wc}]$ usually does not have a close-form expression, we use the sample average approximation (SAA) to estimate the total cost,

$$\begin{aligned}\min_{u_{i,t}} \bar{G}(u_{i,t}) = \sum_{t=1}^{T}\sum_{i=1}^{I}(C^i F_{mi} u_{i,t} + SU_{i,t} + SD_{i,t}) \qquad (9)\\ + \tfrac{1}{S}\textstyle\sum_{s=1}^{S} \min_{P_{i,t}^{s},P_{bt}^{s,ens},P_{wt}^{s,wc}} \left[\textstyle\sum_{t=1}^{T}\sum_{i=1}^{I} C^i F_{ai} P_{i,t}^{s} + \sum_{t=1}^{T}\sum_{b=1}^{B} C^{ens}\cdot P_{b,t}^{s,ens} + \sum_{t=1}^{T}\sum_{w=1}^{W} C^{wc} P_{wt}^{s,wc}\right]\end{aligned}$$

where $s = 1,\dots,S$ denotes the index of scenarios for wind power ξ and DDoS attack η.

Suppose that the wind power ξ follows F, i.e., $\xi \sim F$. The Monte-Carlo sampling can be used to generate the scenarios of ξ (Ruiz et al. 2009). For the DDoS attack scenario generation, we propose a queueing network model consisting of independent $G/G/1$ queues. Specifically, for each thermal generator i, suppose that cyber-attackers randomly intrude the communication network and act independently without cooperation. Thus, DDoS attacks can be modeled as an arrival process. Denote the distribution of the inter-arrival time as F_i^A for $i = 1,\dots,I$. A DDoS attack then causes generator i to loss its connection with the control center and blocks the information flow between them. On the other hand, an IT team constantly monitors the communication network. Once the team detects a DDoS attack event, the team is occupied to address attackers. The attack terminates when the IT team successfully eliminates the intruders. The team addresses attackers at the gateway for the generator one-by-one, and the communication network gets back to the normal operation status when all attacks are successfully eliminated. The IT team handling time is independent for each attack. Thus, the attack elimination process can be modeled as a serving process. The distribution of the serving time follows F_i^D. Thus, the DDoS attack arrival-addressing process can be modeled as a $G/G/1$ queue with the distributions for inter-arrival and service times following F_i^A and F_i^D. Since attacks on generate i do not impact other generators, the cyberattacks to a smart grid can be modeled as a queueing network having mutually independent $G/G/1$ queues. Then, the discrete-event simulation model can be implemented to generate DDoS realizations.

3 CASE STUDY

The six-bus system in Figure 2 is used for the case study; see the detailed information of this example in Wang et al. (2018). It consists of three thermal generators, one wind farm and seven transmission lines, through which the electricity is transmitted to customers. For the transmission lines on the six-bus system, Table 1 provides the basic information. Table 2 describes the characteristics of three thermal generators, the start-up cost of generator i per unit time is the product of the start-up fuel consumption and the fuel price C^i. Similarly, the shut down cost for generator i is the product of C^i and the shut down fuel consumption. For generator i, the actual power production follows $F_i = a_i + b_i \cdot P_i + c_i \cdot P_i^2$. Thus, the minimal production fuel consumption is $F_{mi} = a_i + b_i \cdot P_{i,\min} + c_i \cdot P_{i,\min}^2$, and the additional production fuel consumption F_{ai} is $F_{ai} = a_i + b_i \cdot P_i + c_i \cdot P_i^2 - F_{mi}$. Linearization techniques are used to transfer F_{ai} into a piecewise linear function (Wood and Wollenberg 2014).

We consider the day-ahead unit commitment decision problem for the six-bus system under high wind penetration and potential DDoS attacks. The goal is to find the unit commitment decision for thermal generators minimizing the total expected cost. According to Objective (1), the total operational cost for the six-bus system includes the start-up cost, the turn-off cost, the minimal production cost, the additional thermal generator production cost, and the load shredding penalty cost and the wind curtailment penalty. The first four types of cost are related to the fuel consumption of thermal generators. The corresponding consumption costs are provided in Table 3. Additionally, the load shedding penalty C^{ens} is set at $3500\$/MWh$ and the wind curtailment penalty C^{wc} is fixed at $50\$/MWh$ for unused wind power capability (Wang et al. 2018).

Table 1: Transmission line data.

Line No.	From Bus	To Bus	Flow Limit (MW)
1	1	2	200
2	1	4	100
3	2	4	100
4	5	6	100
5	2	3	200
6	4	5	200
7	3	6	200

Table 2: Thermal generator data.

Unit	Pmax(MW)	Pmin(MW)	Ini.State (h)	Min Off(h)	Min On (h)
G1	220	90	4	-4	4
G2	100	20	2	-3	2
G3	30	10	-1	-1	1

Table 3: Thermal generator data.

Unit	Fuel consumption function.			Start up Fuel (MBtu)	Shut down Fuel (MBtu)	Fuel Price ($)
	a (MBtu)	b (MBtu/MWh)	c (MBtu/MW2h)			
G1	176.9	13.5	0.0004	180	50	1.2469
G2	129.9	32.6	0.001	360	40	1.2461
G3	137.4	17.6	0.005	60	0	1.2462

3.1 Wind Power Sampling

Since in the short term, the load forecasting is significantly more accurate than the wind energy forecasting (Bessa et al. 2012), without loss of generality, we assume deterministic loads and focus on stochastic wind power supply in our study (Tuohy et al. 2009). Following Wang et al. (2018), we use the 2006 data of the U.S. Illinois power system for the load and the wind supply. In particular, one representative day (September 10th) data is selected for discussion in this section. The normal distribution is one of the widely used distributions for the wind power in the research community. Hence, in the study, the wind power is assumed to be normally distributed, i.e., for each time t, the wind power follows a normal distribution with mean μ_t and standard deviation σ_t. Further, the standard deviation σ_t are assumed to be proportional to corresponding mean μ_t (Wang et al. 2008; Wang et al. 2012). To test our proposed SBUC approach under varying environments, we consider different settings for the standard deviation σ_t, namely $\sigma_t = 1\%\mu_t, 5\%\mu_t, 10\%\mu_t, 20\%\mu_t$.

3.2 DDoS Scenario Generation

We use DES to generate DDoS attack scenarios. For the three thermal generators in the six-bus communication network, we assume the same attack arrival and service processes, i.e., $F_i^A = F^A$ and $F_i^D = F^D$. Here, we use the $M/M/1$ queue to model the impact of cyberattacks. Assume that the attack arrivals follow the Poisson distribution, i.e., $F^A \sim \text{Poi}(\lambda)$ and the duration distribution follows the exponential distribution, i.e. $F^D \sim \text{Exp}(\alpha)$. The summary statistics of DDoS attacks on the Internet reported by Arbor (2016) is used in this study. Tables 4 and 5 report the frequency and duration of general DDoS statistics from the report.

To obtain the parameters λ and α, the last columns in Tables 4 and 5 provide the empirical cumulative distribution functions (ECDF) for the frequency and duration of DDoS attacks. Therefore, we can use the least square fitting to find the λ and α parameter estimates (Brunel and Comte 2009). Specifically, for the k-th row in Tables 4 and 5, the ECDFs of duration and arrival can be denoted by $\text{ECDF}^D(t(k))$ and $\text{ECDF}^A(n(k))$, where $t(k)$ and $n(k)$ are the corresponding upper bounds of duration and frequency reported in the k-th row. Then we want to find the parameters λ and α that minimize the sum of least squares between the input models and ECDF for the first six rows. The last row is ignored since all distributions

Table 4: Frequency of DDoS attacks per month.

Frequency Per Month	Percentage	Cumulative Probability
less than 1	14.6%	0.146
1-10	30.9%	0.455
11-20	10.6%	0.561
21-50	6.5%	0.626
51-100	12.2%	0.748
101-500	13.0%	0.878
Over 500	12.2%	1

Table 5: Duration of DDoS attacks.

Duration in Hours	Percentage	Cumulative Probability
less 0.5 h	86.0%	0.86
0.5 -1 h	5.0%	0.91
1-3 h	4.0%	0.95
3-6 h	1.0%	0.96
6-12h	1.0%	0.97
12-24h	2.0%	0.99
over 24 h	1.0%	1

have probability 1 for the last row. Hence, for the duration, we want to find α such that

$$\min_{\alpha} \sum_{k=1}^{6} \left(1 - e^{-\alpha t(k)} - \mathrm{ECDF}^{D}(t(k))\right)^2$$

where $1 - e^{-\alpha t}$ is the CDF of the exponential distribution. Denote the fitted α as $\widehat{\alpha}$. Similarly, for the cyberattack arrivals, we want to find λ such that

$$\min_{\lambda} \sum_{k=1}^{6} \left(e^{\lambda} \sum_{i=0}^{n(k)} \frac{\lambda^i}{i!} - \mathrm{ECDF}^{A}(n(k))\right)^2$$

where $e^{\lambda} \sum_{i=0}^{n(k)} \frac{\lambda^i}{i!}$ is the CDF of the Poisson distribution. Then, the fitted parameters $\widehat{\alpha} = 3.6$ and $\widehat{\lambda} = 94.1$ are used in the simulation.

3.3 Numerical Test

In this section, we compare the performance of our model with the classical SUC model, which ignores the impact of DDoS attacks on the system operation. Denote $\widehat{u}_{i,t}^{sbuc,\star}$ as the optimal unit commitment decisions obtained by our SBUC model and denote the optimal decision obtained by the classical SUC as $\widehat{u}_{i,t}^{suc,\star}$. Then, we evaluate their true objective values $G(\widehat{u}_{i,t}^{sbuc,\star})$ and $G(\widehat{u}_{i,t}^{suc,\star})$. Since $\mathrm{E}[\min_{P_{i,t},P_{b,t}^{ens},P_{w,t}^{wc}} \sum_{t=1}^{T} \sum_{i=1}^{I} C^i F_i P_{i,t} + \sum_{t=1}^{T} \sum_{b=1}^{B} C^{ens} \cdot P_{b,t}^{ens} + \sum_{t=1}^{T} \sum_{w=1}^{W} C^{wc} P_{w,t}^{wc}]$ does not have a close-form expression, the SAA for Objective (9), denoted as $\bar{G}(\widehat{u}_{i,t}^{sbuc,\star})$ and $\bar{G}(\widehat{u}_{i,t}^{suc,\star})$, are used for evaluation. To determine a proper scenario size S_e that can correctly estimate the true value $G(\widehat{u}_{i,t}^{sbuc,\star})$ and $G(\widehat{u}_{i,t}^{suc,\star})$, we conducted a side experiment, including 10 macro-replications. Here, we focus on the setting $\sigma_t = 20\%\mu_t$, since it is the most volatile setting tested in our study and hardest to obtain the accurate estimation for the objective value. Furthermore, we consider our model since it accounts for both wind power prediction uncertainty and random DDoS attacks.

Therefore, in each macro-replication, we first solve our SBUC model with the scenario size $S = 50$ and obtain a unit commitment decision $\widehat{u}_{i,t}^{sbuc,\star}$. Then, we draw S_e scenarios and obtain $\bar{G}(\widehat{u}_{i,t}^{sbuc,\star})$ by solving the second-stage problem in Equation (9) given the first-stage commitment $\widehat{u}_{i,t}^{sbuc,\star}$ and calculate the relative error, relativeError $\equiv |\bar{G}(\widehat{u}_{i,t}^{sbuc,\star}) - G(\widehat{u}_{i,t}^{sbuc,\star})|/G(\widehat{u}_{i,t}^{sbuc,\star})$, where $G(\widehat{u}_{i,t}^{sbuc,\star})$ denotes the objective value obtained by using 10^5 scenarios. Suppose that 10^5 is large enough so that the estimation error of $G(\widehat{u}_{i,t}^{sbuc,\star})$ is negligible. The maximum relative error obtained from 10 macro-replications is recorded in Table 6. We observe that $S_e = 1000$ achieves accuracy with the maximum relative error not exceeding 1.5%. Balancing the computational cost and the accuracy, we use $S_e = 1000$ in the true objective evaluation.

We consider various settings with $\sigma_t = 1\%\mu_t, 5\%\mu_t, 10\%\mu_t, 20\%\mu_t$. For each setting, we set the scenario size $S = 50$. The simulation is utilized to generate scenarios for DDoS attacks by using the

Table 6: The maximum absolute relative difference for $G(\widehat{u}_{i,t}^{sbuc,\star})$ estimation.

S_e	10^2	5×10^2	10^3	5×10^3	10^4	5×10^4
relativeError	3.0%	1.7%	1.2%	1.1%	0.9%	0.1%

Table 7: Statistical performance of SBUC and SUC approaches.

	$G(\widehat{u}_{i,t}^{sbuc,\star})$		$G(\widehat{u}_{i,t}^{suc,\star})$		ΔG_p	
	mean	SE	mean	SE	mean	SE
$\sigma_t = 1\%\mu_t$	91501	969	93308	728	-1807	789
$\sigma_t = 5\%\mu_t$	98989	1633	99641	1404	-653	1360
$\sigma_t = 10\%\mu_t$	108440	2770	112380	3050	-3940	1790
$\sigma_t = 20\%\mu_t$	146967	6152	158332	5743	-11365	3722

fitted $M/M/1$ queue with $\widehat{\alpha} = 3.6$ and $\widehat{\lambda} = 94.1$. Then, we implement the proposed SBUC model to find the optimal unit commitment decision $\widehat{u}_{i,t}^{sbuc,\star}$ accounting for both random wind power and DDoS attacks. Since the classical SUC only accounts for wind power prediction uncertainty and it does not account for the impact of DDoS attacks, Constraint (7) is not included in the SUC model. Denote the optimal unit commitment decision obtained by the SUC model as $\widehat{u}_{i,t}^{suc,\star}$. To evaluate the performance of our model, we estimate the true objectives $G(\widehat{u}_{i,t}^{sbuc,\star})$ and $G(\widehat{I}_{i,t}^{suc,\star})$ with S_e number of scenarios. We record the pair-wise objective difference between $G(\widehat{u}_{i,t}^{sbuc,\star})$ and $G(\widehat{u}_{i,t}^{suc,\star})$ obtained from each macro-replication, and denoted it as $\Delta G_p \equiv G(\widehat{u}_{i,t}^{sbuc,\star}) - G(\widehat{u}_{i,t}^{suc,\star})$. A negative difference suggests that the optimal unit commitment decision $\widehat{u}_{i,t}^{sbuc,\star}$ leads to a lower cost.

The mean and standard error (SE) results obtained from 100 macro-replications are recorded in Table 7. The results show that our model outperforms the SUC model in all four cases. Specifically, when the wind power penetration is low and the system operating uncertainty is also small, the impact of DDoS attack is limited and the performances of two methods are relatively close. For two low uncertainty cases with $\sigma_t = 1\%\mu_t$ and $\sigma_t = 5\%\mu_t$, our proposed approach brings 1.9% and 0.6% cost savings, respectively. When the wind power prediction uncertainty or penetration is high, the impact of DDoS attack is substantial and our proposed SBUC model can provide the significant savings compared the classical SUC model. For $\sigma_t = 10\%\mu_t$, our model can provide the 3.5% savings on average, while the average saving increases to 7.1% when $\sigma_t = 20\%\mu_t$.

4 CONCLUSION

In this paper, we propose a new simulation-based unit commitment model for smart power grid scheduling decision making, which takes into account of potential DDoS cyberattacks and renewable energy prediction uncertainty. Specifically, we consider the case that the gateway devices in the smart grid system could be under attack. Consequently, the relevant thermal generators in the smart grid system would loss the communication connection with the control center and they cannot receive real-time production schedule demands from the control center. The case study over the six-bus example indicates that our proposed SBUC is more cost-efficient and robust when there are high wind power penetration and DDoS attacks. Possible future research directions include incorporating wind farms as potential attack victims, and consider the generator failures caused by DDoS attacks.

ACKNOWLEDGMENTS

The authors thank Prof. Joe H. Chow for his insightful suggestions and helpful advice.

REFERENCES

Arbor 2016. "Worldwide Infrastructure Security Report". *available at https://www.arbornetworks.com/images/documents*.

Bessa, R. J., V. Miranda, A. Botterud, Z. Zhou, and J. Wang. 2012. "Time-adaptive quantile-copula for wind power probabilistic forecasting". *Renewable Energy* 40 (1): 29 – 39.

Bhuyan, M. H., D. K. Bhattacharyya, and J. K. Kalita. 2015. "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection". *Pattern Recognition Letters* 51 (1): 1 – 7.

Brunel, E., and F. Comte. 2009. "Cumulative distribution function estimation under interval censoring case 1". *Electron. J. Statist.* 3:1–24.

Chhaya, L., P. Sharma, K. Brancik, G. Bhagwatikar, and A. Kumar. 2017. "Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control". *Electronics* 6 (1): 1 – 22.

Fadlullah, M., M. M. Fouda, N. Kato, X. Shen, and Y. Nozaki. 2011. "An Early Warning System against Malicious Activities for Smart Grid Communications". *IEEE Network* 25 (5): 50 – 55.

Fang, X., S. Misra, G. Xue, and D. Yang. 2012. "Smart Grid - The New and Improved Power Grid: A Survey". *IEEE Communications Surveys & Tutorials* 14 (4): 944–980.

Hargreaves, J. J., and B. F. Hobbs. 2012. "Commitment and Dispatch with Uncertain Wind Generation by Dynamic Programming". *IEEE Transactions on Sustainable Energy* 3 (4): 724 – 734.

Jiang, R., J. Wang, and Y. Guan. 2012. "Robust Unit Commitment With Wind Power and Pumped Storage Hydro". *IEEE Transactions on Power Systems* 27 (2): 800–810.

Jin, D., D. M. Nicol, and G. Yan. 2011. "An event buffer flooding attack in DNP3 controlled SCADA systems". In *Proceedings of the 2011 Winter Simulation Conference*, edited by S. Jain, R. R. Creasey, J. Himmelspach, K. P. White, and M. Fu, 2619–2631: IEEE Computer Society, Washington, DC.

Khalimonenko, A., O. Kupreev, and K. Ilganaev. 2017. "DDoS attacks in Q3 2017". *available at https://securelist.com/ddos-attacks-in-q3-2017/83041/*.

Li, X., X. Liang, R. Liu, X. Shen, X. Lin, and H. Zhu. 2012. "Securing smart grid: cyber attacks, countermeasures, and challenges". *IEEE Communications Magazine* 50 (8): 38 – 45.

Li, Z., and T. Yao. 2010. "Renewable Energy Basing on Smart Grid". In *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, 1–4.

Lo, C. H., and N. Ansari. 2012. "The Progressive Smart Grid System from Both Power and Communications Aspects". *IEEE Communications Surveys & Tutorials* 14 (3): 799–821.

Lu, Z., W. Wang, and C. Wang. 2011. "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic". In *2011 Proceedings IEEE INFOCOM*, 1871–1879.

Mo, Y., T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. 2012. "CyberPhysical Security of a Smart Grid Infrastructure". *Proceedings of the IEEE* 100 (1): 195 – 209.

Niyato, D., P. Wang, and E. Hossain. 2012. "Reliability analysis and redundancy design of smart grid wireless communications system for demand side management". *IEEE Wireless Communications* 19 (3): 38 – 46.

Ruiz, P. A., C. R. Philbrick, and P. W. Sauer. 2009. "Wind power day-ahead uncertainty management through stochastic unit commitment policies". In *2009 IEEE/PES Power Systems Conference and Exposition*, 1–9.

Sadi, M. A. H., M. H. Ali, D. Dasgupta, and R. K. Abercrombie. 2015. "OPNET/Simulink Based Testbed for Disturbance Detection in the Smart Grid". In *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, CISR '15, 17:1–17:4. New York, NY, USA: ACM.

Shapiro, A., D. Dentcheva, and A. Ruszczynski. 2009. *Lectures on Stochastic Programming: Modeling and Theory*. Philadelphia: SIAM.

Tuohy, A., P. Meibom, E. Denny, and M. O'Malley. 2009. "Unit Commitment for Systems With Significant Wind Penetration". *IEEE Transactions on Power Systems* 24 (2): 592 – 601.

Van den Bergh, K., E. Delarue, and W. D'haeseleer. 2014. "DC power flow in unit commitment models". *available at https://www.mech.kuleuven.be/en/tme/research/energy.../Pdf/wpen2014-12.pdf*.

Wang, J., M. Shahidehpour, and Z. Li. 2008. "Security-constrained unit commitment with volatile wind power generation". *IEEE Transactions on Power Systems* 23 (3): 1319 –1327.

Wang, Q., Y. Guan, and J. Wang. 2012. "A Chance-Constrained Two-Stage Stochastic Program for Unit Commitment With Uncertain Wind Power Output". *IEEE Transactions on Power Systems* 27 (1): 592 – 601.

Wang, W., and Z. Lu. 2013. "Cyber security in the Smart Grid: Survey and challenges". *Computer Networks* 57 (5): 13441371.

Wang, Y., Z. Zhou, A. Botterud, and K. Zhang. 2018. "Optimal Wind Power Uncertainty Intervals for Electricity Market Operation". *IEEE Transactions on Sustainable Energy* 9 (1): 199 – 210.

Wood, A. J., and B. F. Wollenberg. 2014. *Power generation, operation, and control*. Handbook of Simulation Optimization. John Wiley & Sons.

Zheng, Q. P., J. Wang, and A. L. Liu. 2015. "Stochastic Optimization for Unit Commitment - A Review". *IEEE Transactions on Power Systems* 30 (4): 1913 – 1924.

Zhou, H. J., C. X. Guo, and J. Qin. 2010. "Efficient application of GPRS and CDMA networks in SCADA system". In *IEEE PES General Meeting*, 1–6.

Zhou, Z., A. Botterud, J. Wang, R. Bessa, H. Keko, J. Sumaili, and V. Miranda. 2013. "Application of probabilistic wind power forecasting in electricity markets". *Wind Energy* 16 (3): 321–338.

AUTHOR BIOGRAPHIES

YUAN YI is a Ph.D. candidate in the Department of Industrial and Systems Engineering at Rensselaer Polytechnic Institute. His research interests are in the interplay of data analytics, optimization, and risk management with a focus on decision-making for complex systems. His email address is yiy2@rpi.edu.

WEI XIE is an assistant professor in the Department of Industrial and Systems Engineering at Rensselaer Polytechnic Institute. She received her M.S. and Ph.D. in Industrial Engineering and Management Sciences at Northwestern University. Her research interests are in data analytics, computer simulation, and data-driven stochastic optimization for complex cyber-physical system risk management. Her email address is xiew3@rpi.edu and her web page is http://homepages.rpi.edu/~xiew3/.

ZHI ZHOU is a Principal Computational Scientist in the Center for Energy, Environmental, and Economic System Analysis at Argonne National Laboratory. His research interests include optimization, statistical forecasting, decision making under uncertainty, and the applications on power grid, electricity markets, renewable energy, and the interdependency between power grids and other infrastructure systems. Dr. Zhou received the M.S. in Operations Research and Statistics, and Ph.D. in Decision Sciences and Engineering Systems from Rensselaer Polytechnic Institute. His email address is zzhou@anl.gov.