Protecting power system operation against cyber-physical attacks in the presence of renewables

The modernization of the power system is taking place with concurrent integration of communication technologies and renewable generation which gives rise to new challenges. Whereas the integration of communication technologies can expose the power system to cyber-physical attacks, the integration of renewable generation brings randomness to the power system which can be exploited by attackers to hide manipulative acts. Consequences of cyber-physical attacks or uncertain and variable renewable generation include the possibility of destabilized grid dynamics. Therefore, it becomes necessary to analyze cyber-security threats on a system in which communication technologies (and thus security holes) and renewable generation (and thus variable generation) coexist. The proposed work here aims to study and counter a new class of intelligent and dynamic attacks that mimic renewable generation patterns to interfere with the system stability. Renewable generators interact with the power grid through two-way communication systems. Using this communication infrastructure, an attacker might gain access to the renewable generator’s SCADA system. The generator’s renewable output can be altered by false data injection (e.g., by compromising frequency sensors that send real-time information on renewable generation to the grid’s energy management system) or false power injection (e.g., by variably reducing the renewable generator’s output to the grid). Based on our knowledge, there is no intrusion detection mechanisms available to protect power system operations against such attacks.

The proposed work addresses the effect of such system attacks on grid frequency control and real time economic dispatch, both of which are two closely related systems that can be impacted by cyber-attacks as well as renewable uncertainty and variability. The repercussions of undetectable renewable generation altering attacks on frequency dynamics could be serious, ranging from load shedding to realizations of inadequate ancillary services and reserves to widespread blackouts. Such attacks could vary with different types and levels of renewable resources available on the grid at any one time. Understanding the statistical and stochastic nature of renewables will help distinguishing the dynamic attacks from system randomness.

In this work, we aim to first model renewable generation altering attacks that emerge from false data injection, assess their impact on real-time economic dispatch and frequency control, and suggest an intrusion detection tool. We then plan to devise and model power injection attacks, to study their impact in regards to load shedding and AGC, and to suggest a tool to detect these attacks that try to “hide” behind renewable variability. The difference between power injection and data injection attacks is based on the response time of the attack. The effect of power injection attack will be instantaneous whereas the data injection attack relies on the reaction time of some underlying control system. Data injection attack may be effective in the economic dispatch problem and shifting the steady state frequency after a disturbance. Power injection attack can cause a system to load shed as soon as a disturbance is sensed in the system. The detection tools we will design will aid system security of the grid with higher penetration levels of renewable power. They will also protect renewable power producers against possible attacks while providing another layer of security to SCADA systems.
Appendix B
SEEDS Project Proposal
Award Year 3

Project Detail (3 pages – no smaller than 11 pt. font)

1. Project Description and Objectives

A significant challenge for the power grid is accommodating a rapidly expanding renewable generation portfolio [1][2]. Unlike conventional power, renewables exhibit randomness, requiring new security paradigms that seek out and neutralize cyber-physical attacks that try to hide behind the variability and uncertainty of renewable generation.

In this proposed study, we will consider scenarios in which attackers can either inject false data about production levels at renewable generation sites (e.g., by compromising frequency sensors) or they can cause false power injections at these sites (e.g., by randomly reducing the power injected by the generator into the grid). The objective will be to secure grid operations from both types of attacks as they attempt to mimic their variability to match the stochasticity of renewable generation. We will first devise and model these attacks that attempt to hide behind renewable variation while trying to destabilize grid dynamics. The study will assess the dynamic behavior of renewable generation on power system operations (e.g., load shedding, frequency regulation, real-time economic dispatch) and identify the loss in the operational safety margins as the level of renewable integration grows. The study will then determine how data and power injection attacks can bring about unsafe operating regions by creating events that may appear associated to renewable power but are actually driven by an attacker.

Renewable generators interact with the power grid through a two-way communication infrastructure which an attacker might exploit to gain access to the renewable SCADA system [3]. Generally speaking, an attacker may then start launching attacks whenever an opportune time arrives and aims to remain undetected while doing so. The Stuxnet malware infecting a nuclear plant is an example of such undetected (at least for some prolonged time) attacks [4]. An attack on a renewable generator is more attractive for an attacker compared to a conventional power plant as the former’s power generation pattern is hard to predict. Thus, an attacker could randomly vary the power offloaded from a renewable generator to the grid with the aim to destabilize grid operations. We term this attack type as a Renewable Power Injection (RPI) attack. Another attack type involves compromising sensors that send real-time data on renewable generation to the grid’s energy management system. An attacker can send false information and may thus pose a threat to a number of critical grid operations, e.g., frequency regulation, real-time economic dispatch, etc. We term this attack type as Renewable Data Injection (RDI) attacks. In both attacks, the uncertain and variable nature of renewable power may help attackers who are aware of the statistical properties of the local renewable power to remain undetected. The main difference between RPI and RDI attacks is based on the response time of the attack. The effect of a RPI attack will be instantaneous whereas a RDI attack relies on the reaction time of some underlying control system. Data injection attack may be effective in the economic dispatch problem and in shifting the steady state frequency after a disturbance. Power injection attack can cause a system to shed load as soon as a disturbance is sensed. For RDI attacks, frequency sensors need to be compromised; if the frequency sensors are not compromised, then there will be a mismatch between net power imbalance and observed frequency. RPI attacks do not depend on such a constraint as their effect is immediate.

The current power grid is not yet flexible enough to respond to system abnormalities exacerbated by renewable penetration. This can be further worsened by undetectable attacks that emulate renewable variability. In this respect, the proposed work is timely. We aim to quantify the impact of renewable generation altering (RGA) attacks on a system with high levels of renewables. The risk and potential damage of cyber-attacks on frequency control, load shedding, and real-time economic dispatch applications caused by RGA attacks will be evaluated. We plan to also develop an intrusion detection mechanism against RPI and RDI attacks that can be installed in the SCADA communication network. To do so, we will employ statistical tools, optimization tools and stochastic models to develop theory and model such attacks. We will use power network models to study the impact of these attacks on system operations, focusing
Appendix B
SEEDS Project Proposal
Award Year 3

particularly on destabilizing effects caused to frequency control, load-shedding and real-time economic dispatch. Finally, we will use detection theory to suggest ways to make the system attack resilient.

2. Background and Evaluation of State of the Art (Including Literature and Commercial Technologies):

Two growing bodies of power systems research motivate the proposed work. The first addresses cyber-physical security of the power grid supported by automatic control and wide area monitoring technologies [5][6]. Successful cyber-attacks have been shown to cause grid voltage and frequency instabilities by compromising control or measurement devices or communication channels. Such attacks may hamper real time operations of grid energy management systems and SCADA networks [7][8][9]. In this regard, the cyber security of real-time dispatch coupled with state estimation and automatic generation control (AGC) have received considerable attention [10][11]. A connection between the above two applications has been established in recent literature [12][13]. Compromising sensors and false data injections to the state estimator can cause large estimation errors [14]. Load redistribution attack is another sub-class of false data injection attack that manipulates load buses measurements to modify state estimators [15]. Economic dispatch that uses incorrect state estimates leads the system into false secure or dangerously unstable operating points [16]. Data attacks on generators ramp constraints too have negative consequences on the look-ahead economic dispatch, a favorable method to dispatch renewable power [17]. Vulnerabilities of AGC system, a fully automated load frequency control, have been recently exposed in literature. Using attack models on AGC control signals that regulate frequency, Sridhar et al. [18] found the range of attack template parameters that violates frequency limits without violating Area Control Error (ACE) limits. Their proposed attack detection used ACE forecast using its past values to detect the change. In [19], a secure AGC system was proposed using authentication signals. A stealthy load altering attack on AGC system causes frequency rate change beyond permissible limits leading to unnecessary tripping of protection relays [20].

The second body of pertinent research examines challenges in grid operations vis-a-vis managing the variability and uncertainty introduced by high levels of renewable generation across different time scales. Two key applications, real-time economic dispatch and frequency control via AGC, which have been shown to be vulnerable to cyber-attacks (as discussed above), can be impacted by the uncertainty of renewable generation as well. In [21] and our paper [22], it was demonstrated that the system cost of network power flow with variable (renewable) generation tends to be higher than conventional, dispatchable generation. Scheduling of reserve resources to counter power imbalances varies dynamically with stochastic renewable power thus making it dependent on renewable resource predictability [23]. We have analyzed the predictability of ocean wave power using machine learning and studied variable nature of different renewables [24][25]. The variability of renewable generation introduces inefficiency in economic dispatch [26] and creates unintended frequency fluctuations in shorter timescales. ACE varies due to transferred renewable power through tie lines and renewable power within a balancing area; all of this motivates a secure and intelligent AGC system [27][28]. Under-frequency load shedding may occur under extreme events such as generation loss, which is further aggravated by low system inertia of renewables in the grid [29].

Based on our knowledge, the detection, identification, risk assessment and corrective actions on stealthy cyber-attacks that mimic renewable generation in a dynamic and volatile power system have not been studied yet.

3. Proposed Novel Approach:
Appendix B
SEEDS Project Proposal
Award Year 3

The novelty in our approach lies in addressing jointly the grid’s cyber security loopholes and the operational complexities caused by renewable penetration. Modeling RGA attacks and the attacker’s objectives will require a thorough knowledge of underlying system as well as statistical and/or stochastic properties of renewable generation. This study will build possible attack models mimicking different types of renewables. For example, an attack may appear to look like solar power, which may be different from wind power, and both can be different from more predictable system load. While power injection or data injection may provide incorrect renewable generation realizations, the information on actual solar irradiance or wind speed may indicate the presence of such attacks. The study intends to assess the risk of renewable generation altering attacks on real time frequency regulation and real time economic dispatch. These systems are impacted greatly by forecast error distribution of renewable power. The RPI or RDI attacks on frequency regulation via AGC can cause unexpected and/or frequent load shedding events, which our proposed intrusion detection scheme will detect in a timely manner. Our approach will also be able to minimize the occurrences of such undesirable events by adopting intelligent strategies. We plan to characterize the impact of such attacks and then develop risk assessment tools against RGA attacks on economic dispatch.

4. **What will the testing plan be for this project?**

   At the end of first year, we plan to come up with an intrusion detection tool against RDI attacks. At the end of second year, we plan to release an intrusion detection tool against RPI attacks. We also expect to test the performance of both the detection tools at Lehigh University Smart grid testbed and system models developed by simulation software.

5. **How does this project address the SEEDS Needs Document and what unique tool or direct solution does this research provide to current industry cybersecurity and grid resiliency needs?**

   The proposed technology addresses Thrust 2-Detection and Response in the list of SEEDS research needs. In this work, the cyber-attacks affect the generator’s SCADA network and also impact the control and monitoring signals sent to the grid’s energy management system. An intrusion detection tool embedded on the underlying communication network and SCADA system is necessary in a fully automated system with no human in the loop.

6. **Risks to Project Success**

   The risk components associated with the proposed research are resource related and scope related. The work will require data on short timescale renewable power for testing and validation of renewable uncertainty and variability models and the corresponding attack models. The timely availability of the data will ensure seamless research progress. The scope of the project may change from time to time based on industry requirements and feedback.

7. **Milestones and Deliverables for Mid-Project (Y1) and End of Project (Y2)**

   **Milestones for Mid-Project (Y1)**
   Q4: Renewable power and data injection attack models and impact assessment of attacks on real time frequency regulation and frequency aware economic dispatch respectively.

   **Deliverables for Mid-Project (Y1)**
   Q4: Journal paper

   **Milestones for End of Project (Y2)**
   Q6: Defensive strategy against renewable **power** injection (RPI) and renewable **data** injection (RDI) attack and its performance testing using software simulations
   Q8: Testing of intrusion detection tools against RDI and RPI attacks on a test-bed

   **Deliverables for end of Project (Y2)**
   Q8: Intrusion detection tools
Appendix B
SEEDS Project Proposal
Award Year 3

8. References (Information below not counted into the 3-page limit of Project Detail)

Appendix B
SEEDS Project Proposal
Award Year 3


Relevant Data and Metrics for Project

A. Personnel

<table>
<thead>
<tr>
<th>University</th>
<th>Title/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Project Leader: Shalinee Kishore</td>
</tr>
<tr>
<td>Other Faculty</td>
<td>Rick Blum, Parv Venkitasubramaniam</td>
</tr>
<tr>
<td>Postdoctoral Scholar</td>
<td></td>
</tr>
<tr>
<td>Graduate Students</td>
<td>Parth Pradhan, TBD</td>
</tr>
<tr>
<td>Undergraduate Students</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B
SEEDS Project Proposal
Award Year 3

*Note: Only for Continuing Project Proposals*

B. Products (Note: *include only those that explicitly acknowledge DOE support*)

<table>
<thead>
<tr>
<th>Journal Article 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal Article 2</td>
<td></td>
</tr>
<tr>
<td>Conference Article 1</td>
<td></td>
</tr>
<tr>
<td>Conference Article 2</td>
<td></td>
</tr>
<tr>
<td>Patents filed/granted</td>
<td></td>
</tr>
<tr>
<td>Seminar</td>
<td></td>
</tr>
<tr>
<td>Curriculum development</td>
<td></td>
</tr>
</tbody>
</table>
# Budget - SEEDS Center

## Proposed Start & End Dates: 10/1/2017 to 9/30/2018

**SEEDS Lead Investigator:** Shalinee Kishore  
**Project Campus:** Lehigh

### Salaries and Wages

<table>
<thead>
<tr>
<th># of mo/yr</th>
<th>Annual or Summer?</th>
<th>Monthly Rate</th>
<th>Fringe Rate (%)</th>
<th>Grant Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Investigator: Name: Shalinee Kishore</td>
<td>$15,602.40</td>
<td>33.20%</td>
<td>Salary $3,900.60</td>
<td></td>
</tr>
<tr>
<td>Co-PI: Name: Rick Blum</td>
<td>$25,000.00</td>
<td>33.20%</td>
<td>Fringes $1,295.00</td>
<td></td>
</tr>
<tr>
<td>Co-PI: Name: Parv Venkitasubraman</td>
<td>$13,200.00</td>
<td>33.20%</td>
<td>Fringes $1,095.60</td>
<td></td>
</tr>
</tbody>
</table>

### # of students | # of mo/yr | Monthly Rate | Fringe Rate (%) |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Graduate Assistant (Ph.D.)</td>
<td>2</td>
<td>12</td>
<td>$2,600</td>
</tr>
<tr>
<td>Graduate Assistant (MS)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Hourly, non-student(s) | Hourly Wage Rate | Fringe Rate (%) |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly, enrolled student</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Direct Costs:

- **Domestic Travel**: $5,000.00
- **Foreign Travel**: $-
- **Materials and Supplies**: $-
- **Services (Consultant/Computer/etc.)**: $-
- **Facility Usage Fees**: $-
- **Equipment (Capital Expenses greater than $2500)**: $-

### Participant Costs:

- **Graduate Assistant Tuition (waiver or payment)**: $25,560.00
- **Participant Stipend (for example, for an REU student)**: $-
- **Participant Support (only to support students in Stipend category)**: $-

### Total Project Direct Cost: $112,124.20

### Indirect Costs: $52,804.16

### Total Project Costs: $164,928.36