Cyber-Vulnerability of Power Grid Monitoring and Control Systems

Chee-Wooi Ten  
Iowa State University  
2215 Coover Hall  
Ames, IA 50011  
+1 (515) 294-9338  
cheewooi@iastate.edu

Chen-Ching Liu  
Iowa State University  
1117 Coover Hall  
Ames, IA 50011  
+1 (515) 294-4763  
liu@iastate.edu

Manimaran Govindarasu  
Iowa State University  
3219 Coover Hall  
Ames, IA 50011  
+1 (515) 294-9175  
gmani@iastate.edu

ABSTRACT

In this paper, a methodology is proposed for the evaluation of the impact of cyber attacks on the power grid. This is a systematical approach to evaluate the vulnerabilities of SCADA system at three levels, i.e., system, scenario, and access points. The impact of potential intrusion is evaluated based on the power flow solution. The cause-effect on the proposed method determines the likelihood of the consequence, which can be evaluated based on a substation outage. An IEEE 30 bus system is used to build a test case for the proposed method.

Keywords
Cyber-Vulnerability, Dependability Measures, and Power Automation.

1. INTRODUCTION

Technological innovation over the last decade has enabled communication protocols to become more flexible and accommodating to industry’s needs for the purpose of interoperability and maintainability in an open architecture environment [1], [2]. By introducing the standard protocols using TCP/IP, the innovation also raises concerns about cyber-related issues [3], [4]. These concerns include large scale interdependencies between computers, communication, and power infrastructures due to the complexity of required compliances [5]. Although the complex infrastructure provides the capabilities for operation, control, business, and analysis, it also increases the security risks, including threats and vulnerabilities of cybersecurity. The future needs to overcome deficiencies of the communication architecture are discussed in [6]. The drawback of technological innovations includes security breaches that may lead to electronic intrusions. A successful intrusion into the control networks can lead to undesirable switching operations executed by attackers, resulting in widespread power outages. Three modes of malicious attacks on the power infrastructure are (i) attack upon the system, (ii) attack by the system, and (iii) attack through the system [7].

The American Gas Association (AGA) 12 task group established protection guidelines for gas SCADA systems that can also apply to water and electricity SCADA systems due to the technical and operational similarity [8]. The compliance mandated by NERC CIP has established the policies for all utilities in the U.S. that are intended to reduce the risks from the compromise of critical cyber assets [9]. Furthermore, the International Electrotechnical Commission Technical Council (IEC TC 57), power systems management and associated information exchange, has advanced the standard communication protocols security in IEC62351 for improving the authentication mechanisms with stronger encryption [10]. This also assures a higher security level for access to sensitive power equipment with audit capabilities.

The high speed communication of a fully automated substation system by IEC61850 provides comprehensive application usages for control and data acquisition through an Ethernet-based network. Its distributed applications, such as GOOSE or GSSE messages, that relate to the main functions of integrated protection, control, monitoring, and archiving can be configured through the local user interface. The use of the Ethernet-based substation automation system (SAS) leads to cybersecurity issues toward power automation [11]. Regardless of the password strength, malicious intrusion attempts remain a potential threat. A typical intrusion involves the following steps: (i) identification of access points, (ii) penetration to the networks through access points, (iii) determination of the targeted systems and learning to launch an attack, and (iv) termination by executing the attack. Although conducting a cyber-attack depends on an individual’s motivation, the irregularity of the routine maintenance on a SAS may be prone to attacks. Attacks, such as disabling or changing the functionality of relay settings, can be made through the user interface in the SAS where it is linked to the intelligent electronic devices (IEDs) [12], [13]. This modification can be accomplished by accessing the web server of SAS through the web-based user interface. Such modifications may not be noticed since auditing of unmanned substations is not conducted frequently.

Conducting a cyber-attack that may lead to equipment damages requires planning and in-depth knowledge. Compliance of NERC’s cybersecurity standards has become increasingly challenging due to the complexity of interdependencies between computer communication system and physical infrastructure. This research proposes a methodology to study the impact of a cyber attack on supervisory control and data acquisition (SCADA) systems at three levels: system, scenarios, and access points. This method is embedded with firewall and password models, which is the primary mode of protection in the power industry today. A test case based on IEEE 30 bus system is formulated to evaluate...
the impact of attacks launched from outside or within the substation networks [14-16].

2. Modeling for Cyber-Vulnerability

The methodology is to model intrusions and evaluate the consequences of a cyber-attack on the SCADA system. The proposed method is used to assess the vulnerability of computer networks and the potential loss of load in a power system as a result of a cyber attack. Fig. 1 shows the relationship between the cyber attacks and resulting impact on a power system. It is composed of two aspects: 1. cyber-net model, and 2. power flow simulation. A cyber-net defines the intrusion scenarios and its events and status. Power flow simulation is to determine the steady state operating condition of a power system. The integration of these two models makes it possible to quantify the impact caused by a potential cyber attack.

![Fig. 1. Cyber-Attack upon Power Systems](image)

The proposed methodology can be used to:
1. Model the access points of control networks with a cyber-net model based on the firewall and password models.
2. Simulate a resulting impact based on power flow simulations.
3. Improve cybersecurity of the SCADA system in accordance with the vulnerability assessment results.

The proposed vulnerability assessment method is performed in three levels: system, scenarios, and access points. Fig. 2 demonstrates a scenario consisting of the access points that are embedded with firewall and password models. The system vulnerability is the maximum value among all the substations.

![Fig. 2. Combination of a Firewall with n Rules and n Computers](image)

A case study using the IEEE 30 bus test system has been set up with 24 substations. To validate the analytical approach, the attacks launched from different locations are formulated. Two cases for vulnerability evaluations are considered:
1) An attack from outside the substation-level networks
2) An attack from within the substation networks

To formulate a realistic case, actual logon data from Iowa State University information technology division was observed. The sample data is approximately 3 million records captured from the Kerberos authentication system for all users, which has been randomly generated between the range of 1e-5 and .005. This is used to calculate the probability set for firewall and password models. The rates are assumed to be constant for all computer systems and firewalls. Table I demonstrates the vulnerability level for each substation. The highlight indicates the bottleneck of system vulnerability.

<table>
<thead>
<tr>
<th>Sub.</th>
<th>From Outside</th>
<th>Within Control Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Existing</td>
<td>Improved</td>
</tr>
<tr>
<td>1</td>
<td>0.1513</td>
<td>0.0313</td>
</tr>
<tr>
<td>2</td>
<td>0.2944</td>
<td>0.1154</td>
</tr>
<tr>
<td>3</td>
<td>0.1173</td>
<td>0.022</td>
</tr>
<tr>
<td>4</td>
<td>0.4437</td>
<td>0.093</td>
</tr>
<tr>
<td>5</td>
<td>0.2798</td>
<td>0.0628</td>
</tr>
<tr>
<td>6</td>
<td>0.5386</td>
<td>0.2938</td>
</tr>
<tr>
<td>7</td>
<td>0.5054</td>
<td>0.1128</td>
</tr>
<tr>
<td>8</td>
<td>0.4173</td>
<td>0.0939</td>
</tr>
<tr>
<td>9</td>
<td>0.3126</td>
<td>0.0671</td>
</tr>
<tr>
<td>10</td>
<td>0.5218</td>
<td>0.1057</td>
</tr>
<tr>
<td>11</td>
<td>0.7225</td>
<td>0.2236</td>
</tr>
<tr>
<td>12</td>
<td>0.5594</td>
<td>0.0964</td>
</tr>
<tr>
<td>13</td>
<td>0.3007</td>
<td>0.0687</td>
</tr>
<tr>
<td>14</td>
<td><strong>1.1402</strong></td>
<td><strong>0.3625</strong></td>
</tr>
<tr>
<td>15</td>
<td>0.6633</td>
<td>0.1553</td>
</tr>
<tr>
<td>16</td>
<td>0.8287</td>
<td>0.1546</td>
</tr>
<tr>
<td>17</td>
<td>0.7949</td>
<td>0.2618</td>
</tr>
<tr>
<td>18</td>
<td>0.1745</td>
<td>0.0301</td>
</tr>
<tr>
<td>19</td>
<td>0.2798</td>
<td>0.0371</td>
</tr>
<tr>
<td>20</td>
<td>0.4075</td>
<td>0.0777</td>
</tr>
<tr>
<td>21</td>
<td>1.0377</td>
<td>0.3158</td>
</tr>
<tr>
<td>22</td>
<td>0.2329</td>
<td>0.0833</td>
</tr>
</tbody>
</table>

3. CONCLUSION AND FUTURE WORK

A comprehensive cybersecurity framework for critical infrastructure systems is needed. This paper introduces a procedure for cyber-based (electronic) intrusion attacks on a power system control network. The proposed approach opens up several opportunities for the future research:
1. Extending the proposed risk modeling approach with comprehensive economic and intrusion models.
2. Extending the proposed risk modeling to model DoS attack and their resulting consequence on the power system.
3. Developing offline and online mitigation strategies to minimize the cyber associated risks of the power control network.
4. Development of visualization techniques to deliver the vast and relevant information from geographically dispersed substations is needed to show the outcome of risk analysis.

4. ACKNOWLEDGMENTS
The authors gratefully acknowledge the support of Electric Power Research Center (EPRC), Iowa State University.

5. REFERENCES