Executive Summary (1 page – no smaller than 11 pt. font)
Co-design of Security Aware Microgrids:
Subtitle: Sequence Hopping Algorithm for Securing IEC 61850 Layer 2 GOOSE Messages

Despite its criticality, IEC 61850 advanced in an era where substations operated in isolated proprietary networks and thus did not include cyber security measures for data communication. However, operators are moving towards open networks and remote access of substation control systems through the aid of contemporary communication technologies such as cloud services. With the realization of this modern communication infrastructure, IEC 62351 emerged in order to tackle the shortcomings of IEC 61850 in terms of communication security. IEC 62351-6 covers communication security within the boundaries of a substation covering MMS, GOOSE, and SMV protocols. IEC 61850-6 realizes the burden of implementing cryptography on IEDs with relatively low processing power by relaxing its constraints on data confidentiality and advising not to encrypt GOOSE and SMV messages, which require a strict 4ms response time. The standard suggests the use of digital signature to otherwise ensure the integrity of GOOSE and SMV multicast messages. However, digital signatures can impose even more overhead than encryption on IED's processors and computationally expensive. This fact has resulted in IEC 62351 having little acceptance in the industry.

IEC 62351-6 devises an algorithm for proper processing of GOOSE messages in order to mitigate some cyber-attacks such as replay attacks. However, the literature showed that issues with the IEC 62351 security measures are inevitable.

Realizing the deficiency in securing GOOSE messages within a 4 ms time constraint, embodiments of the present invention propose a minimal resource intensive sequence hopping algorithm for securing GOOSE messages. The result of this work will include a firmware or software update that can be uploaded to IEDs and a digital board that can be connected to IEDs to assist in secure communications (e.g., a bump-in-the-wire security solution).
This research proposal serves as an extension to our previous work on the Sequence Hopping algorithm for securing IEC 61850 GOOSE messages. The idea behind the proposed algorithm includes the addition of a new field to GOOSE messages called the HseqNum or the “sequence hopping number.” Each of the publishing and receiving IEDs has synchronized pseudo random generators (PRNG) fed with the same seed by a secure mechanism. Therefore, synchronized generation of the same random number will occur inside the publisher and the subscriber IEDs. The subscriber will only accept messages possessing a matching HseqNum as generated by its PRNG. Any message with a repeated or unmatched HseqNum can be discarded.

The upcoming work extension will focus on developing a holistic cyber-attack intrusion detection and mitigation that relies on both cyber and physical rules. The role of the Message Sequence Synchronization and Monitoring Server (MSSMS) will be extended to incorporate system topology, operation scenarios, and current system status in its intrusion detection rules. For example, if a power circuit is disconnected for maintenance, the MSSMS server can determine that any message intended to energize the circuit as invalid message and can send an alarm signal. The alarm signal can be incorporated into error reports, it can alert equipment operators of potential attacks, and it can also implement additional measures to ensure that IEDs operating on the network are in their correct operation modes (e.g., by overriding invalid messages).

Moreover, according to the results of the first round of alpha testing the sequence hopping algorithm, the current algorithm is to be extended to support dynamic packet structures and content, support multiple GOOSE messages, enable pass-through functionality for non-IEC 61850 data streams for device configuration and diagnosis purposes, and allow bidirectional GOOSE message flow for the cases where the device is configured as a publisher and subscriber simultaneously.

2. Background and Evaluation of State of the Art

The first version of the proposed sequence hopping algorithm has been successfully tested at the University of Arkansas. The tested version comprises a MSSMS server that generates a sequence of random seeds. Upon joining the network, a publisher IED can initiate an encrypted communication channel with the MSSMS server. This encrypted channel is used to exchange random seeds with the publishers. The publisher IED then uses the random seeds to generate a sequence hopping number and attach it to each transmitted message. The MSSMS also synchronize all the subscriber IED devices with the same random seeds. The subscriber IED will expect a unique sequence hopping number for each received message. Any message with an invalid or repeated sequence hopping number is discarded.

3. Proposed Novel Approach

IEC 62351-6 devises an algorithm for proper processing of GOOSE messages in order to mitigate some cyber-attacks such as replay attacks. However, Issues with the IEC
62351 security measures are inevitable. First, the standard’s solution for data integrity using RSA digital signatures will not meet the 4ms time constraint imposed on GOOSE messages given the low processing power of current IED processors. Studies have also shown that digital signatures fail to meet the 4ms time constraint even on more advanced processors. Second, the processing of state numbers set by IEC 62351 to counter replay attacks makes the system prone to Denial of Service (DoS) attacks. Since GOOSE messages travel the network unencrypted, an attacker can monitor the network and deduce the current state number. The attacker can then send a message with a very high status number. All the subscribing IEDs will then discard messages from authenticated IEDs because they will have a lesser status number than that published by the attacker.

Realizing the deficiency in securing GOOSE messages within the strict time constraint set forth by IEC 61850, the work in this research thrust proposes a minimal resource intensive sequence hopping algorithm for securing GOOSE messages. Unlike legacy IDS, the proposed system incorporates physical policies to achieve a holistic intrusion detection, situation awareness, and cyber-attack mitigation for power applications that rely of the GOOSE messaging protocol.

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

Version 1 of the proposed algorithm has been tested at the FIU Smart Grid testbed and was also alpha tested at the University of Arkansas. The project extension, which includes the hierarchical MSSMS IDS, will be tested in a safe communication network-in-the-loop framework at FIU before going to the second round of testing at the University of Arkansas and then beta-testing at Arkansas Electric Cooperative Corporation (AECC).

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 framework falls under the categories of cyber incidents detection, remediation, and automated response. The modules to be developed will use their sequence hopping number matching scheme to detect and discard manipulated packets. The MSSMS server will use cyber-physical rules to detect any possible attack. To select proper physical rules based on operation scenarios, the MSSMS server will coordinate with other servers in other areas in order to identify the system topology and states.

The outcome of this project is anticipated to be either software patches or updates to existing devices and/or distributed agents being hosted on several nodes on the power grid.

6. Risks to Project Success

Ability of the developed software to dynamically discover the structure of the messages while maintaining minimal processing time.
7. Milestones and Deliverables for Mid-Project (Y1) and End of Project (Y2)

It is expected that second round of alpha-testing is to be completed by the mid-project time (Y1) and that the framework will be ready for beta testing at AECC by the end of the project.

8. References


Relevant Data and Metrics for Project

A. Personnel

<table>
<thead>
<tr>
<th>Demographics</th>
<th>University</th>
<th>Title/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Leader</td>
<td>Osama Mohammed</td>
<td>FIU</td>
</tr>
<tr>
<td>Other Faculty</td>
<td>Tarek Youssef</td>
<td>FIU</td>
</tr>
<tr>
<td>Graduate Students</td>
<td>Mohamad El Hariri and Hani Habib</td>
<td>FIU</td>
</tr>
<tr>
<td>Undergraduate Students</td>
<td>Eric Harmon</td>
<td></td>
</tr>
</tbody>
</table>

Note: Only for Continuing Project Proposals

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

Journal Article 1

Mohamad El Hariri, Youssef TA, Mohammed OA. On the Implementation of the IEC 61850
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Article 2</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: 8/15/2017 - 8/14/2018**

**SEEDS Lead Investigator:** Osama Mohammed  
**Project Campus:** FIU  
**Project Number:** Renewal

### Salaries and Wages

<table>
<thead>
<tr>
<th># of students</th>
<th># of mo/yr</th>
<th>Monthly Rate</th>
<th>Fringe Rate</th>
<th>Grant Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-doc</td>
<td>1</td>
<td>6</td>
<td>$4,000</td>
<td>4.15%</td>
</tr>
<tr>
<td>Graduate Assistant (PhD)</td>
<td>2</td>
<td>6</td>
<td>$2,000</td>
<td>7.18%</td>
</tr>
</tbody>
</table>

### Direct Costs:

- **Domestic Travel** $2,500.00
- **Foreign Travel** $-
- **Materials and Supplies** $15,000.00
- **Services (Consultant/Computer/etc.)** $-
- **Facility Usage Fees** $-
- **Equipment (Capital Expenses greater than $2500)** $-

**Subtotal Direct Costs** $17,500.00

### Participant Costs:

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

**Subtotal Participant Costs** $-

**Total Project Direct Cost** $85,064.54

### Indirect Costs

<table>
<thead>
<tr>
<th>Rate</th>
<th>Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.50%</td>
<td>$85,064.54</td>
</tr>
</tbody>
</table>

**Unrecovered Indirects** $39,555.01

**Total Project Costs** $124,619.55