Multi-agent System for Detecting False Data Injection Attacks Against the Power Grid

E. Amullen\textsuperscript{1, 4}, H. Lin \textsuperscript{2}, Z. Kalbarczyk\textsuperscript{3}, L. Keel\textsuperscript{4}

\textsuperscript{1, 4} Tennessee State University, 3500 John A. Merritt Blvd, Nashville, TN 37217
eamullen@my.tnstate.edu, keel@gaus.tsuniv.edu

\textsuperscript{2, 3} University of Illinois at Urbana-Champaign, 1308 W. Main St., Urbana, IL 61801
hlin33@illinois.edu, kalbarcz@illinois.edu
Presentation Outline

1 Introduction
   Power grid communication structure
   Motivation

2 Preliminaries
   DC state estimation
   False data injection

3 Proposed detection system
   Multi-agent system architecture
   Threat model
   Detection Strategy

4 Results

5 Conclusion
   Summary
   Ongoing work
Basic power grid communication structure

Key components of a power grid are:

- Field Equipment
- Substations
- The Control Center

Diagram:

- Control Centre
  - SCADA
  - State Estimation
- Network
- Substation
  - Switch
  - RTU
  - IED
- Field Equipment
  - Actuators
  - Sensors
Basic power grid communication structure

Key components of a power grid are:

- Field Equipment
Basic power grid communication structure

Key components of a power grid are:

- Field Equipment
- Substations
Basic power grid communication structure

Key components of a power grid are:
- Field Equipment
- Substations
- The Control Center
Today’s power grid integrates digital computing and communication technologies alongside the grid’s physical infrastructure exposing the power grid to malicious attacks.
Motivation

- Today’s power grid integrates digital computing and communication technologies alongside the grid’s physical infrastructure exposing the power grid to malicious attacks.
- Attacks that compromise measurements are referred to as False data injection (FDI) attacks. FDI attacks can be carefully crafted to evade detection.
Today’s power grid integrates digital computing and communication technologies alongside the grid’s physical infrastructure exposing the power grid to malicious attacks. Attacks that compromise measurements are referred to as False data injection (FDI) attacks. FDI attacks can be carefully crafted to evade detection. We propose a multi-agent system for detecting FDI attacks that target measurement data used for state estimation.
Motivation

• Today’s power grid integrates digital computing and communication technologies alongside the grid’s physical infrastructure exposing the power grid to malicious attacks.

• Attacks that compromise measurements are referred to as False data injection (FDI) attacks. FDI attacks can be carefully crafted to evade detection.

• We propose a multi-agent system for detecting FDI attacks that target measurement data used for state estimation.

• The multi-agent system is composed of software agents created for each substation. Using information exchanged among substations agents can detect bad data.
Consider the following regression model describing the DC power flow of a power system

\[ z = Hx + e \] (1)
DC state estimation

Consider the following regression model describing the DC power flow of a power system

$$z = Hx + e$$  \hspace{1cm} (1)

Using the weighted least square criterion a state estimate $\hat{x}$ can be computed as follows:

$$\hat{x} = (H^T R H)^{-1} H^T R z$$  \hspace{1cm} (2)
DC state estimation

Consider the following regression model describing the DC power flow of a power system

\[ z = Hx + e \] (1)

Using the weighted least square criterion a state estimate \( \hat{x} \) can be computed as follows:

\[ \hat{x} = (H^T R H)^{-1} H^T R z \] (2)

Meter errors, incorrect configurations and malicious data introduce bad data. Bad data is detected using the \( L_2 \) norm of a residual;

\[ \| z - H \hat{x} \| > \tau \] (3)
False data injection

An FDI attack modifies the measurement vector $z$ injecting an attack vector $a$ such that:

$$z_a = Hx + e + a$$

(4)
False data injection

An FDI attack modifies the measurement vector $z$ injecting an attack vector $a$ such that:

$$z_a = Hx + e + a \tag{4}$$

The attacker requires knowledge of the topology of the network. Specifically the $H$ matrix. The attack is undetectable if the attack vector is a linear combination of the rows in the topology matrix

$$a = Hc \tag{5}$$

$$||z_a - H\hat{x}|| = ||z + a - H(\hat{x} + c)|| \tag{6}$$

$$= ||z - H\hat{x} + (a - Hc)|| \tag{7}$$

$$= ||z - H\hat{x}|| \leq \tau \tag{8}$$
Multi-agent system architecture

- Leveraging inter-substation communication specified under the IEEE standards for substation automation
Multi-agent system architecture

- Leveraging inter-substation communication specified under the IEEE standards for substation automation
- We propose deploying software based agents at each substation
Multi-agent system architecture

- Leveraging inter-substation communication specified under the IEEE standards for substation automation
- We propose deploying software based agents at each substation
- Agents collect, store and exchange measurement information with each other and the control center
Multi-agent system architecture

- Leveraging inter-substation communication specified under the IEEE standards for substation automation
- We propose deploying software based agents at each substation
- Agents collect, store and exchange measurement information with each other and the control center
- Agents can build sub-systems of the network in which the system state (phasor angle) of each substation, is consistent with that from the whole system under normal operating conditions
Multi-agent system architecture

- Leveraging inter-substation communication specified under the IEEE standards for substation automation
- We propose deploying software based agents at each substation
- Agents collect, store and exchange measurement information with each other and the control center
- Agents can build sub-systems of the network in which the system state (phasor angle) of each substation, is consistent with that from the whole system under normal operating conditions
- At each sub-system, agents carry out state estimation and bad data detection
Sub-system Creation

Consider a 5-bus power network with 3-load units, 3 generation units and 15 DC power flow measurements.
Consider a 5-bus power network with 3-load units, 3 generation units and 15 DC power flow measurements.
The subsystems created have different topology matrices \((H)\). The power flow equations are maintained for each substation. Under normal operating conditions, sub-system and whole grid state estimates are equal.
The subsystems created have different topology matrices ($H$)
The subsystems created have different topology matrices ($H$)

The power flow equations are maintained for each substation
Sub-system Creation

- The subsystems created have different topology matrices ($H$).
- The power flow equations are maintained for each substation.
- Under normal operating conditions, sub-system and whole grid state estimates are equal.
Sub-system Creation

**Procedure:** generate sub-system for agent at bus $i$

1. Include bus $i$ and its neighboring buses;
2. Include the transmission lines that connect the buses selected at (1);
3. Keep unchanged the real power flow measurements at the sending and receiving end of selected transmission lines;
4. For bus $j \neq i$
5. For transmission line $k$ not selected at (2)
6. If power flow $P$ at line $k$ is delivered into bus $j$
7. Increase power injection at bus $j$ by $P$
8. Else
9. Decrease power injection at bus $j$ by $P$
10. EndIf
11. EndFor
Threat model

• Attackers compromise measurements delivered to the control center by injecting an FDI attack vector
Threat model

- Attackers compromise measurements delivered to the control center by injecting an FDI attack vector
- Measurements collected by agents can be compromised
Threat model

- Attackers compromise measurements delivered to the control center by injecting an FDI attack vector
- Measurements collected by agents can be compromised
- The FDI attack is designed to bypass bad data detection for the whole power grid
Analysis

Formal analysis
Formal analysis

- For a power network with $n$ substations, $n$ agents are created. For a substation $i$, where $i = \{1, \ldots, n\}$, the agent $a_i$ computes a measurement vector $z_i'$ and state vector $x_i'$ as follows:

$$z_i' = H_i'x_i' \quad (9)$$
Analysis

Formal analysis

• For a power network with $n$ substations, $n$ agents are created. For a substation $i$, where $i = \{1, \ldots, n\}$, the agent $a_i$ computes a measurement vector $z_i'$ and state vector $x_i'$ as follows;

$$z_i' = H_i'x_i' \quad (9)$$

Detection
Analysis

Formal analysis

• For a power network with $n$ substations, $n$ agents are created. For a substation $i$, where $i = \{1, \ldots, n\}$, the agent $a_i$ computes a measurement vector $z'_i$ and state vector $x'_i$ as follows:

$$z'_i = H'_i x'_i$$  \hspace{1cm} (9)

Detection

• The FDI attack must satisfy the condition $a' = H'_ic'_i$ at each substation along with $a = Hc$ to remain undetectable.
Analysis

Formal analysis

• For a power network with $n$ substations, $n$ agents are created. For a substation $i$, where $i = \{1, \ldots, n\}$, the agent $a_i$ computes a measurement vector $z_i'$ and state vector $x_i'$ as follows;

$$z_i' = H_i'x_i'$$  \hspace{1cm} (9)

Detection

• The FDI attack must satisfy the condition $a' = H_i'c_i'$ at each substation along with $a = Hc$ to remain undetectable.

• The attack is detected if the condition $a' = H_i'c_i'$ is not satisfied for at least one agent.
Experiments-IEEE 9-bus system
Experiments-IEEE 9-bus system
Multi-agent system for the IEEE 9-bus system
Multi-agent system for the IEEE 9-bus system
Multi-agent system for the IEEE 9-bus system
Multi-agent system for the IEEE 9-bus system
Multi-agent system for the IEEE 9-bus system
### FDI attack IEEE 9-bus system

<table>
<thead>
<tr>
<th>$z$</th>
<th>$\hat{x}$</th>
<th>$c$</th>
<th>$a$</th>
<th>$z_a = z + a$</th>
<th>$\hat{x}_a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.6700</td>
<td>0.170969</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.6700</td>
<td>0.170969</td>
</tr>
<tr>
<td>0.2897</td>
<td>0.088326</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.2897</td>
<td>0.088326</td>
</tr>
<tr>
<td>-0.6103</td>
<td>-0.03859</td>
<td>0.0000</td>
<td>-5.8824</td>
<td>-6.4927</td>
<td>-0.03859</td>
</tr>
<tr>
<td>0.8500</td>
<td>-0.06524</td>
<td>0.0000</td>
<td>-17.0648</td>
<td>-16.2148</td>
<td>-0.06524</td>
</tr>
<tr>
<td>0.2398</td>
<td>0.038515</td>
<td>1.0000</td>
<td>9.9206</td>
<td>10.1604</td>
<td>1.038515</td>
</tr>
<tr>
<td>-0.7603</td>
<td>0.014352</td>
<td>0.0000</td>
<td>0.0000</td>
<td>-0.7603</td>
<td>0.014352</td>
</tr>
<tr>
<td>-1.6300</td>
<td>0.069095</td>
<td>0.0000</td>
<td>0.0000</td>
<td>-1.6300</td>
<td>0.069095</td>
</tr>
<tr>
<td>0.8697</td>
<td>-0.07092</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.8697</td>
<td>-0.07092</td>
</tr>
<tr>
<td>-0.3803</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.6700</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.6700</td>
<td>-0.3803</td>
</tr>
<tr>
<td>1.6300</td>
<td>0.0000</td>
<td>0.0000</td>
<td>1.6300</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.8500</td>
<td>-17.0648</td>
<td>-16.2148</td>
<td>0.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>-0.9000</td>
<td>-5.8824</td>
<td>-6.7824</td>
<td>0.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0000</td>
<td>32.8678</td>
<td>32.8678</td>
<td>0.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-1.0000</td>
<td>-9.9206</td>
<td>-10.9206</td>
<td>0.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>-1.2500</td>
<td>0.0000</td>
<td>0.0000</td>
<td>1.2500</td>
<td></td>
<td>1.2500</td>
</tr>
</tbody>
</table>
Detection results for IEEE 9-bus system

- For the whole system, a $H_\infty$ attack is undetectable if $\tau = 1.5670 \hat{10}^6$. The $L_2$-norm is computed as follows:

$$||z - H \hat{x}||^\tau$$

- At agent 5 and 8, $a_1 \neq H_1 c_1$, making the attack detectable.

$$||z - H_1 \hat{x}||^\tau$$

Detection results for IEEE 9-bus system

- For the whole system $a = Hc$. The attack is undetectable. Setting the $\tau = 1.5670 \times 10^{-6}$, $L_2$-norm is computed as follows:

$$\|z + a = H(x + c)\| = \|z - Hx\| = \tau$$
Detection results for IEEE 9-bus system

- For the whole system $a = Hc$, the attack is undetectable. Setting the $\tau = 1.5670 \times 10^{-6}$, $L_2$-norm is computed as follows:
  \[
  \|z + a = H(x + c)\| = \|z - Hx\| = \tau
  \]

- At agent 5 and 8, $a_i' \neq H_i'c_i'$ making the attack detectable:
  \[
  \|z_i' + a_i' = H_i'(x_i' + c_i')\| \neq \|z_i' - H_i'x_i'\| \neq \tau
  \]
Detection results for IEEE 9-bus system

- For the whole system \( \mathbf{a} = \mathbf{Hc} \) The attack is undetectable Setting the \( \tau = 1.5670 \times 10^{-6} \), \( L_2 \)-norm is computed as follows

\[
\| \mathbf{z} + \mathbf{a} = \mathbf{H}(\mathbf{x} + \mathbf{c}) \| = \| \mathbf{z} - \mathbf{Hx} \| = \tau
\]

- At agent 5 and 8, \( \mathbf{a}_i \neq \mathbf{H}_i \mathbf{c}_i \) making the attack detectable

\[
\| \mathbf{z}_i + \mathbf{a}_i = \mathbf{H}_i(\mathbf{x}_i + \mathbf{c}_i) \| = \| \mathbf{z}_i - \mathbf{H}_i \mathbf{x}_i \| \neq \tau
\]
Probability of successful detection by a single agent for the 9-bus, 14-bus, and 30-bus system.
Distribution of agents per attack for a 9-bus system
Distribution of agents per attack for a 14-bus system

Distribution of agents per attack for a 30-bus system
Detection at individual substations

![Graph showing number of attacks detected at individual substations](image)

- **9-bus**
- **14-bus**
- **30-bus**

• A multi-agent system for detecting false data injection attacks in the power grid is proposed.
• A multi-agent system for detecting false data injection attacks in the power grid is proposed.

• Each substation is assigned an agent equipped with communication capability.
Conclusion

- A multi-agent system for detecting false data injection attacks in the power grid is proposed.
- Each substation is assigned an agent equipped with communication capability.
- Agents create subsystems from a topology formed by a substation and its neighboring...
Conclusion

• A multi-agent system for detecting false data injection attacks in the power grid is proposed.
• Each substation is assigned an agent equipped with communication capability.
• Agents create subsystems from a topology formed by a substation and its neighboring
• The agents run state estimation and bad data detection to detect FDI attacks. All measurements must pass bad data detection for all agents.
Conclusion

- A multi-agent system for detecting false data injection attacks in the power grid is proposed.
- Each substation is assigned an agent equipped with communication capability.
- Agents create subsystems from a topology formed by a substation and its neighboring
- The agents run state estimation and bad data detection to detect FDI attacks. All measurements must pass bad data detection for all agents.
- The detection technique is demonstrated using the DC power flow and DC state estimation data of the IEEE 9-bus, 14-bus and 30-bus systems.
Ongoing Work

- Multi-agent system will be extended to include attack identification
Ongoing Work

- Multi-agent system will be extended to include attack identification
- To be implemented on real-world hardware for further analysis
Ongoing Work

- Multi-agent system will be extended to include attack identification
- To be implemented on real-world hardware for further analysis
Thank You