Privacy Preservation Intrusion Detection Technique for SCADA Systems

Marwa Keshk, Nour Moustafa, Elena Sitnikova, and Gideon Creech
Agenda

• IDS And Its Relation To SCADA Systems
• Research Methodology Of IDS And Privacy Preservation
• Dataset For Evaluation And Evaluation Criteria
• Experimental Results And Discussion
• Concluding Remarks
**IDS And Its Relation To SCADA Systems**

- **Supervisory Control and Data Acquisition (SCADA)** systems face the absence of a protection technique that can beat different types of intrusions and protect the data from disclosure while handling this data using other applications, specifically *Intrusion Detection System (IDS)*.

- **The SCADA system** can manage the critical infrastructure of industrial control environments. Protecting sensitive information is a difficult task to achieve in reality with the connection of physical and digital systems.

- Hence, *privacy preservation techniques* have become effective in order to protect sensitive/private information and to detect malicious activities, but they are not accurate in terms of error detection, sensitivity percentage of data disclosure.
Networked SCADA

Mission
Critical
Reliability...

Data Concentrator

Field Data Acquisition & Local control

Fiber Optic Cable

Fiber Optic Converter

Modem & Radio

RTU 1

Serial Line

Fiber Optic Converter

Modem & Radio

RTU 2

Serial Line

Fiber Optic Converter

Modem & Radio

RTU 3

Serial Line

Redundant Ethernet LAN 802.3

Alarm/Event Printer

Print Server

Print Server

SCADA Server

Historical Archiving

SCADA Server

Data Acquisition

SCADA Server

Historical Archiving

Data Acquisition

RTU 1

RTU 2

RTU 3

Print Server

Print Server
**IDS and its components**

- **Modeling**
  - Features: evidences extracted from audit data
  - Analysis approach: piecing the evidences together
    - Misuse detection (a.k.a. signature-based)
    - Anomaly detection (a.k.a. statistical-based)

- **Deployment (Network-based or Host-based)**
  - Network based: monitor network traffic
  - Host based: monitor computer processes
IDS and its components (cont.)

**system activities are observable**

Audit Data

Preprocessor

Audit Records

Activity Data

Detection Engine

Alarms

Decision Table

Detection Models

Decision Engine

normal and intrusive activities have distinct evidence

Action/Report
Privacy Preservation Methods

• Some recent studies have focused on designing IDS for SCADA systems, and these studies show the challenges of designing an effective IDS–based SCADA system without disclosing their shared data.

• Classic encryption techniques, comprising RSA and AES, are not appropriate because we cannot use the encrypted data for analyzing this data.

• Processing any of SCADA data could be intrusive actions happen; hence it is still a controversial area of research to find methods that provide privacy-preservation for SCADA data.

• Privacy preservation methods are used for reducing number of SCADA features for selecting only important ones without disclosing all information.
Privacy Preservation Methods (cont.)

• The important techniques of privacy preserving Data Mining are:
  – Randomization methods
  – Encryption methods
  – Anonymization methods
Proposed methodology

Privacy preservation IDS framework

1. Collect SCADA data
2. Select portions of important information using PCC
3. Apply EM for clustering normal and abnormal data
4. Assess the performance of proposed privacy IDS technique
The Pearson’s correlation coefficient (PCC) technique is used in order to select the important information of SCADA data, which is considered as one of the simplest linear correlation techniques for approximating the correlation scores of features — Privacy preservation technique.

\[
\rho = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{\sqrt{[n\Sigma x^2 - (\Sigma x)^2][n\Sigma y^2 - (\Sigma y)^2]}}
\]

![Graph showing the Pearson correlation coefficient vs. sample size.](image)
Proposed methodology (cont.)

- **EM clustering for identifying SCADA attacks**

### EM Algorithm

**Initialization:**
The initial parameters of $k$ distributions are selected either randomly or externally.

**Iteration:**

- **E-Step:** Compute the $P(C_i | x)$ for all objects $x$ by using the current parameters of the distributions. Re-label all objects according to the computed probabilities.
- **M-Step:** Re-estimate the parameters of the distributions to maximize the likelihood of the objects’ assuming their current labeling.

**Stopping condition:**
At convergence - when the change in log-likelihood after each iteration becomes small.
Dataset For Evaluation

- The power system datasets [5] for multiclass attacks are used to evaluate the performance of the proposed privacy preservation intrusion detection technique and are compared with three other techniques. The multi-class datasets include 37 scenarios, are encompassed into natural events (8), no events (1) and intrusion events (28).
Evaluation Criteria

• The **accuracy** is defined as the proportion of all normal and attack records properly classified.

• The **Detection Rate (DR)** is the percentage of precisely detected attack records.

• The **False Positive Rate (FPR)** identifies the percentage of incorrectly detected attack records.
## Feature Description and selection

<table>
<thead>
<tr>
<th>Feature Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA1:VH – PA3:VH</td>
<td>Phase A – C Voltage Phase Angle</td>
</tr>
<tr>
<td>PM1:V – PM3:V</td>
<td>Phase A – C Voltage Magnitude</td>
</tr>
<tr>
<td>PA4:IH – PA6:IH</td>
<td>Phase A – C Current Phase Angle</td>
</tr>
<tr>
<td>PM4:I – PM6:I</td>
<td>Phase A – C Current Magnitude</td>
</tr>
<tr>
<td>PA7:VII – PA9:VII</td>
<td>Pos. – Neg. – Zero Voltage Phase Angle</td>
</tr>
<tr>
<td>PM7:V – PM9:V</td>
<td>Pos. – Neg. – Zero Voltage Magnitude</td>
</tr>
<tr>
<td>PM10:V – PM12:V</td>
<td>Pos. – Neg. – Zero Current Magnitude</td>
</tr>
<tr>
<td>F</td>
<td>Frequency for relays</td>
</tr>
<tr>
<td>DF</td>
<td>Frequency Delta (dF/dt) for relays</td>
</tr>
<tr>
<td>PA:Z</td>
<td>Apparent Impedance seen by relays</td>
</tr>
<tr>
<td>PA:ZH</td>
<td>Apparent Impedance Angle seen by relays</td>
</tr>
<tr>
<td>S</td>
<td>Status Flag for relays</td>
</tr>
</tbody>
</table>
## Feature Description and selection

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value1</th>
<th>Value2</th>
<th>Value3</th>
<th>Value4</th>
<th>Value5</th>
<th>Value6</th>
<th>Value7</th>
<th>Value8</th>
<th>Value9</th>
<th>Value10</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1.PA1.VH</td>
<td>0.03</td>
<td>-0.37</td>
<td>0.03</td>
<td>0.94</td>
<td>-0.38</td>
<td>0.03</td>
<td>-0.38</td>
<td>0.03</td>
<td>-0.36</td>
<td>0.03</td>
</tr>
<tr>
<td>R1.PM1.V</td>
<td>1</td>
<td>0.75</td>
<td>0.75</td>
<td>-0.76</td>
<td>0.01</td>
<td>-0.28</td>
<td>-0.31</td>
<td>0.03</td>
<td>0.95</td>
<td>0.34</td>
</tr>
<tr>
<td>R1.PA2.VH</td>
<td>1</td>
<td>0.01</td>
<td>-0.24</td>
<td>-0.36</td>
<td>0.05</td>
<td>0.91</td>
<td>0.06</td>
<td>0.24</td>
<td>0.06</td>
<td>0.37</td>
</tr>
<tr>
<td>R1.PM2.V</td>
<td>1</td>
<td>0.04</td>
<td>0.99</td>
<td>0.04</td>
<td>-0.75</td>
<td>-0.75</td>
<td>-0.61</td>
<td>-0.61</td>
<td>0.92</td>
<td>0.22</td>
</tr>
<tr>
<td>R1.PA3.VH</td>
<td>1</td>
<td>0.00</td>
<td>-0.37</td>
<td>0.00</td>
<td>-0.37</td>
<td>0.00</td>
<td>-0.37</td>
<td>0.00</td>
<td>0.92</td>
<td>0.22</td>
</tr>
<tr>
<td>R1.PM3.V</td>
<td>1</td>
<td>0.04</td>
<td>-0.73</td>
<td>-0.6</td>
<td>-0.64</td>
<td>0.00</td>
<td>0.92</td>
<td>0.24</td>
<td>0.24</td>
<td>0.42</td>
</tr>
<tr>
<td>R1.PA4.IH</td>
<td>1</td>
<td>0.00</td>
<td>-0.38</td>
<td>0.00</td>
<td>-0.36</td>
<td>0.00</td>
<td>0.94</td>
<td>0.02</td>
<td>0.02</td>
<td>0.05</td>
</tr>
<tr>
<td>R1.PM4.I</td>
<td>1</td>
<td>0.00</td>
<td>0.78</td>
<td>0.00</td>
<td>0.80</td>
<td>0.00</td>
<td>-0.81</td>
<td>0.27</td>
<td>0.63</td>
<td>0.29</td>
</tr>
<tr>
<td>R1.PA5.IH</td>
<td>1</td>
<td>0.06</td>
<td>-0.23</td>
<td>0.06</td>
<td>-0.38</td>
<td>0.06</td>
<td>0.94</td>
<td>0.02</td>
<td>0.02</td>
<td>0.05</td>
</tr>
<tr>
<td>R1.PM5.I</td>
<td>1</td>
<td>0.00</td>
<td>0.97</td>
<td>0.00</td>
<td>0.97</td>
<td>0.00</td>
<td>-0.45</td>
<td>0.01</td>
<td>0.01</td>
<td>0.04</td>
</tr>
<tr>
<td>R1.PA6.IH</td>
<td>1</td>
<td>0.00</td>
<td>-0.36</td>
<td>0.00</td>
<td>-0.36</td>
<td>0.00</td>
<td>0.91</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>R1.PM6.I</td>
<td>1</td>
<td>0.00</td>
<td>-0.49</td>
<td>0.00</td>
<td>-0.49</td>
<td>0.00</td>
<td>0.12</td>
<td>0.08</td>
<td>0.09</td>
<td></td>
</tr>
<tr>
<td>R1.PA7.VH</td>
<td>1</td>
<td>0.00</td>
<td>-0.31</td>
<td>0.00</td>
<td>-0.31</td>
<td>0.00</td>
<td>-0.78</td>
<td>0.34</td>
<td>0.73</td>
<td></td>
</tr>
<tr>
<td>R1.PM7.V</td>
<td>1</td>
<td>0.36</td>
<td>0.87</td>
<td>0.24</td>
<td>0.36</td>
<td>0.87</td>
<td>0.24</td>
<td>0.36</td>
<td>0.87</td>
<td>0.24</td>
</tr>
<tr>
<td>R1.PA8.VH</td>
<td>1</td>
<td>0.41</td>
<td>0.96</td>
<td>0.03</td>
<td>0.41</td>
<td>0.96</td>
<td>0.03</td>
<td>0.41</td>
<td>0.96</td>
<td>0.03</td>
</tr>
<tr>
<td>R1.PM8.V</td>
<td>1</td>
<td>0.41</td>
<td>0.96</td>
<td>0.03</td>
<td>0.41</td>
<td>0.96</td>
<td>0.03</td>
<td>0.41</td>
<td>0.96</td>
<td>0.03</td>
</tr>
<tr>
<td>R1.PA9.VH</td>
<td>1</td>
<td>0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R1.PM9.V</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Evaluation using EM technique

<table>
<thead>
<tr>
<th>Feature percentage</th>
<th>DR</th>
<th>Accuracy</th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>25%</td>
<td>66.4%</td>
<td>70.6%</td>
<td>32.5%</td>
</tr>
<tr>
<td>50%</td>
<td>75.6%</td>
<td>76.3%</td>
<td>25.1%</td>
</tr>
<tr>
<td>75%</td>
<td>82.8%</td>
<td>83.5%</td>
<td>17.8%</td>
</tr>
<tr>
<td>100%</td>
<td>88.9%</td>
<td>90.2%</td>
<td>11.7%</td>
</tr>
</tbody>
</table>

ROC Curves of EM technique

Detection Rate %

False Positive Rate %
**Comparison with other techniques and Concluding remarks**

<table>
<thead>
<tr>
<th>Technique</th>
<th>DR</th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nearest Neighbour</td>
<td>55.3%</td>
<td>44.8%</td>
</tr>
<tr>
<td>Naïve Bayes</td>
<td>44.4%</td>
<td>52.6%</td>
</tr>
<tr>
<td>Random Forests</td>
<td>60.5%</td>
<td>38.4%</td>
</tr>
<tr>
<td><strong>Our technique</strong></td>
<td><strong>88.9%</strong></td>
<td><strong>11.7%</strong></td>
</tr>
</tbody>
</table>

- Our technique accomplishes better results than the three other techniques, as it clusters normal and abnormal data based on the exact estimation of mean and standard deviation of normal and attack classes, making a clear difference between them.

- However, the technique is not able to detect the best results with a lower number of features because of the relative similarity between normal and attack data.

- This can be achieved by using hierarchical clustering techniques to use a small number of features, resulting in disclosing sensitive information of SCADA systems.
Reference


Thank you