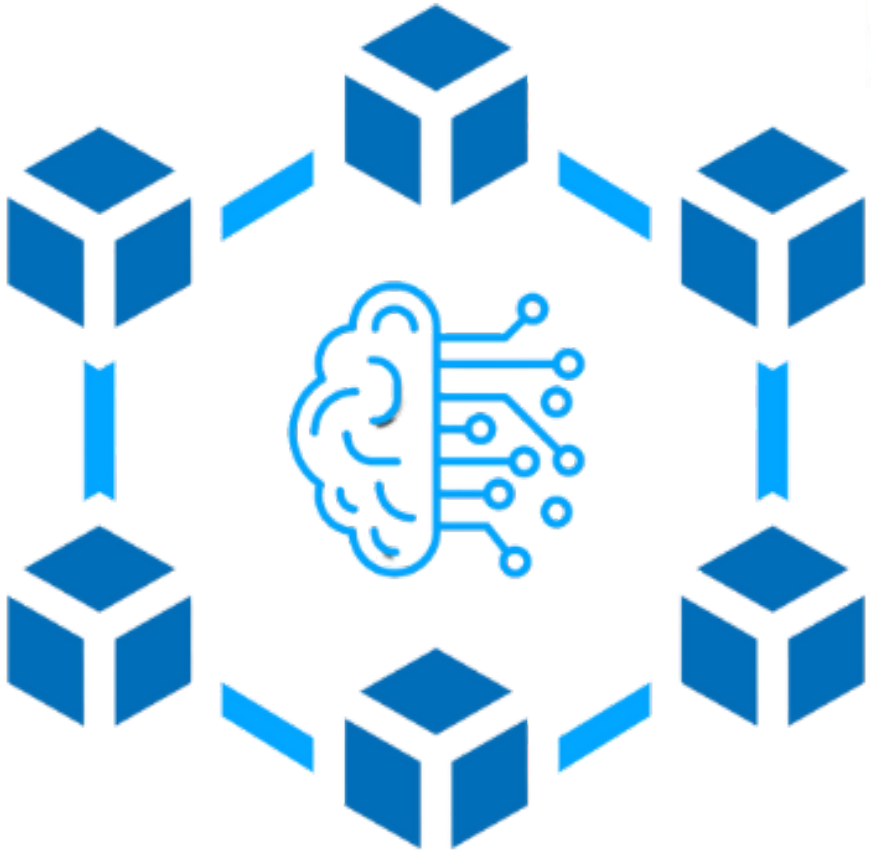
Title: AI-Driven Anomaly and Intrusion Detection in Energy Systems: Current Trends and Future Direction

Conference: IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2024)

Authors: Georgios Andronikidis, Charis Eleftheriadis, Zisis Batzos, Konstantinos Kyranou, Nikolaos Maropoulos, Gohar Sargsyan, Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis

2-4 September 2024
London, UK

Andronikidis Georgios
Research Machine Learning Engineer



This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096456.

Contents

- Introduction
- Methodology
- Challenges in Anomaly and Intrusion Detection
- Future Directions
- Conclusions

Introduction

Advancements and Vulnerabilities in Energy Systems:

- Integration of advanced technologies improves efficiency, reliability, and scalability.
- New vulnerabilities expose systems to complex cyber threats and anomalies.
- Consequences of breaches range from minor disruptions to catastrophic failures.

Role of AI and ML in Enhancing Security:

- AI and ML as pivotal tools in amplifying energy systems' security.
- Advantages of AI-driven approaches: real-time data analysis, pattern identification, high accuracy in threat prediction.
- Superiority of AI-based methods over traditional techniques for detecting cyber-attacks in smart grids.

Historical Cyber Attacks:

- 2015 Ukraine power grid attack (BlackEnergy) left 230,000 consumers without electricity.
- Dragonfly/EnergeticBear campaign targeted Western energy companies, causing espionage and potential disruptions.
- 2023 Denmark cyber attack on 22 energy companies demonstrated advanced preparation and execution, suggesting state actor involvement.

Introduction

Importance of Early Detection and Mitigation:

- Early detection is crucial for safeguarding critical infrastructure.
- Improving resilience fortifies energy systems against disruptions and fosters stakeholder trust.
- Robust cybersecurity measures ensure a stable and reliable energy supply, crucial for modern society.

Purpose of the Survey Paper:

- Provide a comprehensive overview of AI technologies for anomaly and intrusion detection in energy systems.
- Guide researchers and practitioners in developing more secure and resilient energy systems.

Methodology – Anomaly Detection

- Critical role in protecting EPES, SG, and microgrids from cyber threats.
- Techniques address both malicious intrusions and operational irregularities.
- Aim to enhance stability and functionality of energy networks.

Machine Learning and Deep Learning:

- Utilization of unsupervised and supervised learning models.
- Common algorithms include AutoEncoders, LSTM, GRU, Isolation Forest, and Facebook Prophet.
- Focus on handling time-series data and improving detection accuracy.

Time-Series Analysis:

- Techniques to forecast and detect deviations in electrical load data.
- Methods assess alignment with historical patterns to identify anomalies.
- Address class imbalance by focusing on deviations from forecasted patterns rather than relying on labeled data.

Recurrent Models and Autoencoders:

- Recurrent Autoencoders (RAEs) using LSTM, GRU, and ConvLSTM.
- Capture spatiotemporal features and reduce false positives through reconstruction error analysis.
- Deep Autoencoders, including Variational Autoencoders (VAEs) and Attention-based Autoencoders (AEAs), improve anomaly detection performance.

Methodology – Anomaly Detection

Study	Task	Algorithm	Outcome
Ibrahim et. al.	Classification or Regression	AE-LSTM Isolation Forest Facebook-Prophet	AE-LSTM detects anomalies and identifies health signal
Wang et al.	Regression	GRU Bi-LSTM TDG	Eliminates class imbalance problem occurred in anomaly detection
Radaideh et al.	Regression	GRU LSTM ConvLSTM	LSTM demonstrated better performance
Takidin et al.	Regression	SAE VAE AEA	AEA demonstrates significant improvement in detection rates
Morisson et al.	Regression	Isolation Forest GMM KNN LOF	Various algorithms are evaluated with the proposed pre-processing step

Methodology – Intrusion Detection

Optimization-Based Frameworks:

- Techniques such as Binary Grey Wolf Optimization-based Ensemble Classification (BGWO-EC).
- Phases include pre-processing, feature selection, classification, and evaluation.
- Use of Bayesian optimization for hyperparameter tuning to enhance model robustness and efficiency.

Protocol-Specific Detection:

- Intrusion detection tailored for specific protocols like DNP3.
- Use of Dempster-Shafer (DS) theory to reduce false alerts.
- Integration of multi-hypothesis mass function models and fusion frameworks for enhanced situational awareness.

Machine Learning and Deep Learning Models:

- Hyperparameter-optimized Random Forest (RF) classifiers.
- Dimensionality reduction techniques using supervised autoencoders and PCA.
- Cluster-Driven Ensemble Learning (CDEL) combining clustering and ensemble methods for robust classification.
- Enhanced Deep Belief Networks (EDBN) integrating deep learning with rule-based techniques.
- Layered architectures to improve detection accuracy of cyberattacks like False Data Injection (FDIA) and Denial of Service (DoS) attacks.

Methodology – Intrusion Detection

Study	Task	Algorithm	Outcome
Panthi et. al.	Classification	Decision Tree KNN SVM Optimizable Ensemble	The BGWO-EC boost the performance of the detectors
Sahu et al.	Classification	Decision Tree KNN SVM Random Forest	Addresses uncertainty and variability in intrusion detection
Zhu et al.	Classification	Random Forest	A hyperparameter configuration space is constructed, and used to build various Random Forest classifiers
Wang et al.	Classification	Decision Tree KNN AdaBoost Bagging	By using the proposed dimensionality reduction (SupervisedAE and PCA), models demonstrate superior accuracy and F1 score
Roy et al.	Classification	Decision Tree KNN AdaBoost CDEL Logistic Regression Naive Bayes	CDEL algorithm demonstrates better performance over traditional classifiers
Durairaj et al.	Classification	EDBN	EDBN demonstrates higher accuracy and lower false alarm rates

Challenges in Anomaly and Intrusion Detection

Detection of Zero-Day and Complex Attacks:
- Identifying sophisticated threats without prior knowledge.
- Necessity for advanced real-time detection approaches.

High False Alarm Rates:
- Resource wastage due to frequent false positives.
- Importance of enhancing detection accuracy.

Low Detection Rates:
- Risk of threats going unnoticed.
- Need for improving the sensitivity of detection systems.

Unbalanced Datasets:
- Skewed performance of detection algorithms.
- Techniques required to handle class imbalance.

Robustness Against Adversarial Attacks:
- Vulnerability of ML and AI-based detectors to adversarial threats.
- Ongoing research needed to fortify systems.

Challenges in Anomaly and Intrusion Detection

Compatibility with Legacy Systems:

- Ensuring seamless integration with existing infrastructures.
- Addressing interoperability issues.

Regulatory and Compliance Issues:

- Aligning with evolving standards and policies.
- Harmonizing new solutions with existing frameworks for regulatory compliance.

Future Directions

Integration of Large Language Models (LLMs) and Advanced ML Algorithms:

- Training on vast datasets for improved attack pattern identification.
- Assisting security experts with complex attack patterns and mitigation actions.

Sophisticated Adversarial Training Techniques:

- Enhancing robustness of ML and AI-based detectors.
- Utilizing adversarial examples to strengthen defense mechanisms.

Implementation of Transfer Learning:

- Applying models to different, yet related, datasets.
- Overcoming challenges of unbalanced datasets for better generalization.

Federated Learning Technologies:

- Collaborative optimization without compromising data privacy.
- Pooling diverse data sources for comprehensive models.
- Enhanced data security and resilience against targeted attacks.

Cyber-Physical Security Challenges:

- Proactive cyber-defense strategies for integrated IT and OT systems.
- Human-AI collaboration and human-in-the-loop practices for improved adaptability.

Conclusions

Key Findings:

- **Early Detection Mechanisms:** Emphasizing the importance of early detection mechanisms in safeguarding critical infrastructure.
- **Advanced Defense Strategies:** Highlighting the need for robust and proactive defense strategies tailored to the unique characteristics of EPES, smart grids, and microgrids.

Future Directions:

- **Cutting-Edge AI and ML Technologies:** The future of anomaly and intrusion detection lies in the strategic incorporation of advanced AI and ML technologies, coupled with domain-specific enhancements for the energy sector.
- **Interdisciplinary Collaboration:** Continued research and interdisciplinary collaboration will be crucial in realizing these advancements, ultimately leading to more robust and reliable security infrastructures.

Thank you!

SIDROCO

SIDROCO HOLDINGS LTD
KARYATIS 8, Leoforos
Kyriakou Matsi 23, 1082
Nicosia, Cyprus

Email: info@sidroco.com
Tel: +357 22450777

Sidroco Holdings Ltd