Qeios

Peer Review

Review of: "On Process Awareness in Detecting Multi-stage Cyberattacks in Smart Grids"

Syed Hasan[1]

1. Information Systems, King Abdul Aziz University, Saudi Arabia

The study presents an innovative approach to enhancing cybersecurity in Smart Grids by leveraging process-aware Intrusion Detection Systems (IDSs). The integration of domain-specific knowledge from IT, OT, and ET layers, combined with machine learning techniques, showcases a forward-thinking methodology that aligns with the complex and evolving nature of cyber threats in smart grid environments. This research effectively highlights the potential of process-aware IDSs in improving detection accuracy for complex, multi-stage cyberattacks, making it a significant contribution to the field of critical infrastructure security.

Strengths of the Study

1. Emphasis on Process Awareness

The focus on process-aware IDS is a standout feature. By moving beyond IT-only approaches, the research demonstrates how incorporating operational and energy-specific data enhances the ability to detect threats that are deeply embedded in the operational processes of Smart Grids. This contextual understanding provides a nuanced approach to intrusion detection, significantly reducing the likelihood of false negatives.

1. Comprehensive Co-Simulation Environment

The use of a co-simulation environment that encapsulates IT, OT, and ET layers is commendable. This layered approach offers a holistic perspective, allowing the simulation of real-world multi-stage cyberattacks and providing a robust platform for evaluating IDS strategies. Such a methodology strengthens the reliability and applicability of the findings.

doi.org/10.32388/H8ZIPB

1. Integration of Machine Learning Techniques

Employing machine learning to enhance IDS capabilities adds a modern and adaptive layer to the research. While challenges like false positives persist, the study makes strides in addressing these issues by correlating ICT and process data, paving the way for more precise and actionable intrusion detection.

1. Domain-Specific Insights

The research makes an important case for leveraging domain knowledge in detecting and mitigating cyber threats. This approach ensures that IDSs are not only more accurate but also more relevant to the unique operational context of Smart Grids, addressing a critical gap in traditional IDS methodologies.

Areas for Improvement

1. High-Level Description of Machine Learning Models

While the study mentions the use of machine learning, it does not delve deeply into the specifics of the algorithms or models employed. A more detailed discussion of the machine learning techniques, their parameters, and their performance metrics would have added depth and clarity to the research.

1. False Positives and Alert Mechanisms

The research acknowledges challenges with false positives and unclear alert mechanisms but does not provide detailed solutions or experimental data addressing these issues. A focused discussion on how the proposed system mitigates these challenges would have strengthened the practical applicability of the findings.

1. Scalability and Real-World Deployment

The study is largely simulation-based, which, while valuable, leaves questions about the scalability and performance of the proposed IDS in real-world deployments. Exploring the potential challenges of implementing such systems in large-scale Smart Grids could enhance the relevance of the research.

1. Comparative Analysis

Although the study claims that process-aware IDSs outperform traditional IT-only IDSs, the absence of a detailed comparative analysis with other state-of-the-art IDS models limits the strength of this

assertion. Including performance benchmarks against existing solutions would provide more compelling evidence of its superiority.

Conclusion

This research provides a solid foundation for advancing intrusion detection in Smart Grids through process-aware methodologies. The integration of domain knowledge and co-simulation environments adds significant value to the field, addressing critical gaps in traditional IDS approaches. However, a deeper exploration of machine learning specifics, real-world scalability, and comparative analysis would further enhance the impact of this work.

Overall, the study is a commendable step forward in the field of Smart Grid cybersecurity. Its innovative approach to leveraging process awareness and multi-domain integration makes it a valuable contribution to the development of more resilient and intelligent IDSs. With further refinement and validation, the proposed framework has the potential to set new benchmarks for securing critical infrastructure.

Declarations

Potential competing interests: No potential competing interests to declare.