Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/NA11.20260262
Published: June 9, 2026

Mathematical Modelling to Facilitate Understanding Constraints Associated with Cyberattacks Mitigation in a P2P-based Energy Trading System

Oluwaseun O. Tooki and Olawale M. Popoola
Centre for Energy and Electric Power (CEEP)
Electrical Engineering Department
Tshwane University of Technology
Pretoria, South Africa
TookiOO@tut.ac.za, PopoolaO@tut.ac.za

Abstract

Peer-to-peer (P2P) energy trading system has the potential to play a transformational role in addressing electricity availability in rural areas and sub-Saharan Africa. P2P is a market-driven energy coordination system that enables communities with/without grid access to generate, trade, and manage electricity locally. Despite P2P enabling prosumers (consumers with the capacity to generate energy) to sell their surplus energy to peers in rural areas, there are still challenges that impede its implementation. Some of the identified impediments include technical issues (Cybersecurity and Data Privacy, Communication and Interoperability, System Stability and Control, and Data Management and Analytics). This article presents a mathematical model that enhances understanding of the technical issues relating to cybersecurity of P2P-based energy trading systems (P2P-ETSs). This research further established the importance of addressing one of the technical constraints, cybersecurity and data privacy, for efficient mapping of bids to allocations and payments in energy trading. A correct understanding of the mathematical formulations of constraints will enhance the advancement of this energy solution with an interest in availability, affordability, and the protection of participants' privacy in a P2P-ETS against adversaries.

Keywords
Cybersecurity, Energy Trading System (ETS), Peer-to-Peer (P2P)

1. Introduction
Energy is a major component of critical infrastructure that supports the provision of various essential services for mankind (Markopoulou, 2023). Peer-to-Peer (P2P) energy markets have surfaced as a path to integrate distributed energy resources (DERs) and prosumer flexibility (Sim et al., 2024). The rise in the penetration of Renewable Energy Resources (RES), as well as breakthroughs in Information and Communication Technologies, permits prosumers to participate in the energy market and trade their surplus energy with peers. For the secure and safe operation of the energy trading system (ETS), the P2P energy trading approach has emerged as a practicable model to provide the essential flexibility and match the energy sharing among prosumers (Zahraoui et al., 2024). The P2P architecture permits energy customers to trade between themselves without the involvement of energy utility companies (Hutty et al., 2024). It minimizes reliance on grid electricity, reduces peak grid load, and is the most effective method in optimizing the usage of Renewable Energy (RE) resources in the distribution network, thereby minimizing losses along transmission and distribution lines (Malik et al., 2023).

The integration of advanced technologies, such as Blockchain, into P2P-ETS has increased the market players' participation in secure transactions and energy trading among prosumers (Shukla et al., 2024). Additionally, researchers have offered insight into the perception of P2P electricity trading within the Power Distribution Network to enhance the understanding of the energy trading market (Almarzooqi et al., 2023). The interconnection of design, high

centralization, and dependence on real-time communication of P2P-ETS makes it susceptible to cyberattacks, thereby increasing the attack surface to adversaries. An insecure P2P-ETS is a bottleneck for prosumers as it impedes them in making optimal real-time decisions. However, there is no substantial information regarding the mathematical modelling of constraints/cyberattacks against the performance of P2P-ETS models.

Scholars have reported several cyberattacks in P2P-ETS lately, including adversarial attacks, where market participants make hidden changes to the input data of other participants to considerably impact operations negatively (Tooki and Popoola, 2024). Other recorded cyberattacks include DDoS, Distributed Denial of Service (attackers overload communication nodes); FDI, False Data Injection (attackers manipulate metre readings and transactions data), and Man-in-the-Middle (where attackers secretly intercept communications between prosumers (Tooki and Popoola, 2024). Our research objective is to facilitate understanding by mathematical modelling of constraints connected to cyberattack mitigation in a P2P-based ETS.

2. Literature Review

2.1 P2P Energy Trading System Existing P2P Energy Trading Models and Algorithms

Researchers have proposed different models for P2P energy trading, such as real-time, hour-ahead market, and game-theoretic approaches. A continuous double auction model was recorded in (Hutty et al., 2024). In the proposed approach, upcoming time slots were concurrently open for trading. The P2P market model was simulated over two weeks using 25 households under varying climate conditions. Although a significant £10/week savings was achieved, the model's forecasting remains imperfect because it is based on a day-ahead structure. In reality, trading must be sustained throughout the day. Four double auction techniques- Average, McAfee, Trade Reduction, and Vickrey-Clarke-Groves (VCG) were proposed to boost the efficiency of P2P energy trading across different MGs (Sim et al., 2024). The results revealed that the average mechanism was the best for a consumer-driven MG, whereas VCG was largely profitable during non-peak hours trading. The limitation of the work is that the network constraints, such as voltage management and power factor, were not taken into cognizance. The authors devised different auction mechanisms to match specific MG configurations.

Reference (Melendez & Matamala, 2025) modelled electricity market dynamics using an equilibrium problem with equilibrium constraints by combining the Fisher–Burmeister function and strong duality theorem. Zhou and Lund comprehensively analyze device degradation costs, transmission losses, equity distribution, and allocation for various participants in the P2P energy pricing model (Zhou & Lund, 2023). A two-stage strategic model was proposed to optimize shared energy storage in a P2P energy trading market (He et al., 2024). In the work, the impact of carbon emissions on the P2P trading process was analyzed. However, the limitation is that the researchers fail to consider uncertainties emanating from the optimization of proposed strategies. In (Shukla et al., 2024), a blockchain-based P2P-ETS network was analyzed using a hybrid technique, Reinforcement Learning and Feed Forward Neural Network. The analytical model was evaluated using trade-offs that affect the delay (throughput and security) as performance metrics.

A no-regret algorithm was proposed to optimize decision-making in energy trading in a day-ahead forward electricity market (Getaneh Abate et al., 2024). The numerical results show that social cost and market-clearing prices can be higher than those matching the classical game-theoretic techniques. A distributed algorithm was presented in (Zahraoui et al., 2024). The framework permits market participants to share information to achieve P2P energy trading consensus while protecting players' privacy. Relatedly, an online distributed algorithm was proposed for a real-time P2P energy market to ensure fast, stable, and safe long-term operation of the system (Liu et al., 2023).

2.2 Cyberattacks and Mitigation on P2P Energy Markets

Various cyberattacks have been reported in the energy system. In some cases, attacks do emanate from demand-side players, where microgrids (MGs) and prosumers engage in malicious activities by targeting other MGs and the independent system operator to compromise demand-side operations (Melendez and Matamala, 2025). A Deep Learning- based Deep Neural Network model was proposed for the detection and mitigation of DDoS attacks in a Software-Defined Network environment (Hnamte et al., 2024). The approach successfully analyzes network traffic data to discern complex structures of DDoS attacks. The performance of the model is limited by the availability of dedicated DDoS datasets. Real-time threat Intelligence and adaptive defense mechanisms were proposed to enhance cyber threat detection (Akinsanya, 2024).

3. Problem Formulations

This problem formulation was carried out to facilitate understanding of challenges associated with the P2P-ETS as it affects prosumers, suppliers, and energy prices.

3.1 P2P Energy Trading System

We modelled P2P-ETS into three major components: Prosumers, Suppliers, and Energy Prices. These are formulated given the equations expressed below.

$$d'_{i,t} = d_{i,t} \cdot \left(1 + \alpha \cdot f\left(d_{i,t}\right)\right)$$

$$f\left(d_{i,t}\right) = \frac{1}{1 + e^{-d_{i,t}}}$$

$$p_t^b = p_t^b \cdot \left(1 - \alpha_p \cdot \frac{\text{Flagged Volume}}{\text{Total Volume}}\right)$$

$$q_t^{\max} = q_t^{\text{total}} \cdot \left(1 - \beta \cdot \frac{\text{Flagged Transactions}}{\text{Total Transactions}}\right)$$

3.2 Objectives

3.2.1 Defender

- Detect and mitigate attacks
- Maintain grid stability and fair pricing.
- Optimize detection accuracy, minimize false positives, and reduce economic disruption.

3.2.2 Attacker:

- Maximize economic gain by creating unfair pricing
- Evade detection to sustain attacks over time
- Disruption of Service to compromise data integrity to steal confidential information

3.2.3 Dynamic Interaction

This interaction is modelled as a **multi-agent RL problem**:

- **Agents**:
  - Attacker (Agent 1): Learns to optimize attack parameters
  - Defender (Agent 2): Learns detection thresholds and mitigation strategies.

4. Mathematical Framework

4.1 State Space $\boldsymbol{S_t}$

At any time t, the system state includes:

$$\boldsymbol{S_t} = \left\{\mathbf{d_{i,t}}, \mathbf{E_{i,t}^g}, \mathbf{p_t^b}, \mathbf{p_t^s}, \text{flagged transactions up to t}\right\}$$

4.2 Action Space $\boldsymbol{A_t}$

4.2.1 Attacker Actions (A_t^{attack})

$$A_t^{attack} = \{\alpha, f(d_{i,t})\}$$

- α: Controls the intensity of the manipulation.
- $f(d_{i,t})$: Determines how demand is manipulated.

4.2.2 Defender Actions ($A_t^{defense}$)

$$A_t^{defense} = \{\text{detection threshold},\ \text{price adjustment factor},\ \text{transaction cap}\}$$

- **Detection Threshold**: Determines the sensitivity of the detection model.
- **Price Adjustment Factor**:

$$p_t^b = p_t^b \cdot \left(1 - \alpha_p \cdot \frac{\text{Flagged Volume}}{\text{Total Volume}}\right)$$

- **Transaction Cap**:

$$q_t^{\max} = q_t^{\text{total}} \cdot \left(1 - \beta \cdot \frac{\text{Flagged Transactions}}{\text{Total Transactions}}\right)$$

4.3 Reward Functions

4.3.1 Attacker Reward

The attacker maximizes:

$$R_t^{\text{attack}} = w_4 \cdot \text{Economic Gain} - w_5 \cdot \text{Detection Penalty}$$

where:

- Economic Gain: Financial benefit from manipulated prices.
- Detection Penalty: Loss incurred when flagged by the detection model.

4.3.2 Defender Reward

The defender maximizes:

$$R_t^{\text{defense}} = w_1 \cdot \text{Detection Accuracy} - w_2 \cdot \text{Instability} - w_3 \cdot \text{Economic Disruption}$$

where:

- **Detection Accuracy**:

$$\text{Detection Accuracy} = \frac{\text{True Positives}}{\text{Total Actual Attacks}}$$

- **Economic Disruption**:

$$\text{Economic Disruption} = \frac{\sum_t |p_t^b - p_t^s|}{T}$$

4.4 Learning Objectives

Attacker's Objective

The attacker learns a policy:

$$\pi^*_{\text{attack}} = \arg\max_{\pi_{\text{attack}}} E\left[\sum_{t=0}^{T} \gamma^t R_t^{\text{attack}}\right]$$

Defender's Objective

The defender learns a policy:

$$\pi^*_{\text{defense}} = \arg\max_{\pi_{\text{defense}}} E\left[\sum_{t=0}^{T} \gamma^t R_t^{\text{defense}}\right]$$

5. Discussion

The summary reported in Table 1 gives a synopsis of the Objectives, Dynamic Interactions, Action Space, and Reward Functions of the Mathematical model of the P2P-based Energy Trading System. The analysis is based on the Defend and Attack scenario. It was observed that the aim of adversaries revolved around creating unfair pricing, compromising data integrity, and evading detection over the period of the attacks. Whereas, the target of the Defender is to optimize detection accuracy, reduce economic disruption to sustained grid stability and fair pricing.

In the proposed approach, the model captures the action space for the attackers which include Controls the intensity of the manipulation (to determines how demand is manipulated) while detection threshold (to determine the sensitivity of the detection model), Price Adjustment Factor and Transaction Cap were considered for the defender.

Additionally, on Reward functions, emphasis was on attackers try to maximize economic gain, that is, financial benefit from manipulated prices and detection penalty associated with Loss incurred when flagged by the detection model. Meanwhile, the defender maximizes Detection Accuracy and Prevention of Economic Interruption towards sustaining grid stability. The stability of grid fosters clean and affordable energy, which aligns to Sustainable Development Goal (SDG) seven.

Table 1. Summary of Objectives, Dynamic Interactions, Action Space, and Reward Functions of the Model

S/N	**Objectives**	
1	**Defender**	**Attacker**
1.1	Detect and mitigate attacks	Maximize economic gain by creating unfair pricing
1.2	Maintain grid stability and fair pricing.	Evade detection to sustain attacks over time
1.3	Optimize detection accuracy, minimize false positives, and reduce economic disruption	Disruption of Service to compromise data integrity to steal confidential information
2	**Agents Dynamic Interaction**	
	Defender Agent: Learns detection thresholds and mitigation strategies	**Attacker Agent**: Learns to optimize attack parameters
3	**Space/Action Space**	
3.1	**Defender Action**	**Attacker Action**
3.1.1	Detection Threshold: Determines the sensitivity of the detection model	Controls the intensity of the manipulation.

3.1.2	Price Adjustment Factor:	Determines how demand is manipulated.
3.1.3	Transaction Cap	
4	**Reward Functions**	
4.1	**Defender Reward**	**Attacker Reward**
4.1.1	Maximizes Detection Accuracy	Maximizes Economic Gain: Financial benefit from manipulated prices
4.1.2	Prevention of Economic Interruption	Detection Penalty: Loss incurred when flagged by the detection model.

6. Conclusion and Future Outlook

Understanding potential limitations can facilitate the development of robust detection algorithms in mitigating cyberattacks on the P2P-ETS. This paper presented mathematical modelling to facilitate understanding of the challenges associated with the cybersecurity of a P2P-based ETS. The mathematical formulations and review of existing models serve as a preliminary evaluation of mitigation of attacks on the P2P-ETS. The authors recommended integrating Blockchain Technology to enhance automation in P2P-based trading systems, thereby minimizing human interactions, increasing transparency, and enabling settlements using Smart Contracts. On the future outlook, the authors planned to use Reinforcement Learning to train the attacker using PPO (Proximal Policy Optimization) and train the defender using MADDPG (Multi-Agent Deep Deterministic Policy Gradient).

References

Akinsanya, A., "Enhancing Cyber Threat Detection through Real-time Threat Intelligence and Adaptive Defense Mechanisms," *International Journal of Computer Applications Technology and Research*, pp. 10–27, July 2024. https://doi.org/10.7753/ijcatr1308.1002.

Almarzooqi, A. H., Osman, A. H., Shabaan, M., and Nassar, M., "An Exploratory Study of the Perception of Peer-to-Peer Energy Trading within the Power Distribution Network in the UAE," *Sustainability (Switzerland)*, vol. 15, no. 6, pp. 1–18, 2023. https://doi.org/10.3390/su15064891.

Getaneh Abate, A., Majdi, D., Kazempour, J., and Kamgarpour, M., "Learning to bid in forward electricity markets using a no-regret algorithm," *Electric Power Systems Research*, vol. 234, p. 110693, April 2024. https://doi.org/10.1016/j.epsr.2024.110693.

He, Y., Wu, H., Wu, A. Y., Li, P., and Ding, M., "Optimized shared energy storage in a peer-to-peer energy trading market: Two-stage strategic model regards bargaining and evolutionary game theory," *Renewable Energy*, vol. 224, February 2024. https://doi.org/10.1016/j.renene.2024.120190.

Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., and Sugali, M. N., "DDoS attack detection and mitigation using deep neural network in SDN environment," *Computers and Security*, vol. 138, November 2024. https://doi.org/10.1016/j.cose.2023.103661.

Hutty, T. D., Brown, S., and Only, G., "P2P trading of heat and power via a continuous double auction," *Applied Energy*, vol. 369, p. 123556, January 2024. https://doi.org/10.1016/j.apenergy.2024.123556.

Liu, J., Long, Q., Liu, R. P., Liu, W., and Hou, Y., "Online distributed optimization for spatio-temporally constrained real-time peer-to-peer energy trading," *Applied Energy*, vol. 331, June 2023. https://doi.org/10.1016/j.apenergy.2022.120216.

Malik, S., Thakur, S., Duffy, M., and Breslin, J. G., "Automating the Procurement of Shared Resources in Multiple Microgrids using a Double Auction Platform," *Smart Grids and Sustainable Energy*, 2023. https://doi.org/10.1007/s40866-023-00178-x.

Markopoulou, D., "Tackling cybersecurity challenges in the energy and water sectors in the context of the cybersecurity and sectoral regulatory frameworks: the case of smart metering systems in the new digitalised environment," *International Review of Law, Computers and Technology*, vol. 37, no. 1, pp. 52–77, 2023. https://doi.org/10.1080/13600869.2022.2094609.

Melendez, K. A., and Matamala, Y., "Adversarial attacks in demand-side electricity markets," *Applied Energy*, vol. 377, p. 124615, 2025. https://doi.org/10.1016/j.apenergy.2024.124615.

Shukla, S., Hussain, S., Irshad, R. R., Alattab, A. A., Thakur, S., Breslin, J. G., Hassan, M. F., Abimannan, S., Husain, S., and Jameel, S. M., "Network analysis in a peer-to-peer energy trading model using blockchain and machine learning," *Computer Standards and Interfaces*, vol. 88, October 2024. https://doi.org/10.1016/j.csi.2023.103799.

Sim, J., Lee, D., and Yoon, K., "Trustful double auction design for Peer-to-Peer energy trading between interconnected micro-grids with supply – demand imbalance," *International Journal of Electrical Power and Energy Systems*, vol. 160, p. 110117, February 2024. https://doi.org/10.1016/j.ijepes.2024.110117.

Tooki, O. O., and Popoola, O. M., "A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems," *Renewable Energy Focus*, vol. 51, August 2024. https://doi.org/10.1016/j.ref.2024.100628.

Tooki, O., and Popoola, O., "Intelligent-Based Techniques for Detection, Identification and Mitigation of Cyberattacks in Cyber-Physical Power Systems: A Review," *2024 IEEE PES/IAS PowerAfrica, PowerAfrica 2024*, pp. 0–4, 2024. https://doi.org/10.1109/PowerAfrica61624.2024.10759370.

Zahraoui, Y., Korõtko, T., Rosin, A., Khalil Zidane, T. E., and Mekhilef, S., "A Real-Time Simulation for P2P Energy Trading Using a Distributed Algorithm," *IEEE Access*, vol. 12, pp. 44135–44146, February 2024. https://doi.org/10.1109/ACCESS.2024.3369899.

Zhou, Y., and Lund, P. D., "Peer-to-peer energy sharing and trading of renewable energy in smart communities ─ trading pricing models, decision-making and agent-based collaboration," *Renewable Energy*, vol. 207, pp. 177–193, November 2023. https://doi.org/10.1016/j.renene.2023.02.125.

Acknowledgements

This work is based on the research supported wholly/in part by the National Research Foundation of South Africa (Grant Numbers: 150574, KIC 250804351170); and Tshwane University of Technology - Faculty of Engineering and Built Environment and Centre for Energy and Electric Power.

Biographies

Oluwaseun Olayinka Tooki has a Ph.D Degree in Electronic and Electrical Engineering (2022), from Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria. Currently, a Postdoctoral Research Fellow at the Centre for Energy and Electric Power, Electrical Engineering Department, Tshwane University of Technology, Pretoria, South Africa. He is a senior member of IEEE and a registered member of the Council for the Regulation of Engineering in Nigeria. His research interests include communication Engineering, Renewable Energy, Artificial Intelligence in Energy, and TES.

Olawale Popoola is a Full Professor and Director Centre for Energy and Electric Power (CEEP) in the Department of Electrical Engineering at Tshwane University of Technology Pretoria, South Africa. He is an Engineer/technologist/lecturer/author with diverse experience in the Electrical and Power industry, Oil and Gas Sector, Shipping Building Industry, Education, Energy and Quality Management field. His love for research and innovation has brought him accolades and achievements. These include a commendation letter from Weatherford Headquarters, Ravenna, Italy at the earliest stage of his career, various institutional awards, a certificate of recognition by the Department of Science and Technology, South Africa in the invention of South African Patent No 2016/04429 as well as grants/project funds. He is a Certified Measurement and Verification Professional (CMVP) with a proven record and extensive knowledge of the energy industry; and a member of the Association of Energy Engineers (AEE). Olawale is an author/co-author of more than 140 scientific publications (articles, chapters in books and author of a book). Prof Popoola currently holds the Sasol/DSI-NRF Research Chair at tier 2 - "Energy Solutions for Inclusive and Sustainable Societies".