

Reliable Node-Based Cyber Resilient Distributed Economic Dispatch for Smart Grids

Research Article


10.65520/erciyesfen.1832165


Imprint:


Volume: 42(1)

Year: 2026

Page: 311-324

 Tolga ŞEN^{a*}

 Mustafa Yasin ERTEN^b

 Hüseyin AYDİLEK^c

^a Res. Asst., Kırıkkale University,
tolgasen@kku.edu.tr

^b Asst. Prof., Kırıkkale University,
mustafaerten@kku.edu.tr

^c Asst. Prof., Kırıkkale University,
huseyinaydilek@kku.edu.tr

* Corresponding Author

Received: 11/28/2025

Accepted: 12/24/2025

Citation:

Tolga ŞEN, Mustafa Yasin ERTEN,
Hüseyin AYDİLEK (2026). Reliable
Node-Based Cyber Resilient
Distributed Economic Dispatch for
Smart Grids. *Erciyes University Journal
of Institute Of Science and Technology*,
42(1), 311-324.

[https://doi.org/10.65520/erciyesfen.
1832165](https://doi.org/10.65520/erciyesfen.1832165)

Abstract

Cybersecurity of distributed economic dispatch (ED) within smart grids is critical for the system's efficiency and reliability. Especially stealth attacks, where an agent secretly manipulates its own cost parameters and turns the system into a non-optimal state, are known to pose a serious threat because of detection difficulty. This study offers a new, architecture-based defense strategy against the mentioned stealthy cost parameter attacks, which is easier to implement. The proposed method is based on an architecture of where trusted nodes are strategically placed in the network and enable normal nodes to proactively filter abnormal data from malicious agents, based on information received from trusted neighbors. The effectiveness of the strategy is tested under three different scenario simulations in MATLAB. The results show that the proposed defense mechanism successfully neutralized the attack, enables healthy nodes to reach optimal consensus, and prevents the system suffering economic losses.

Keywords: Distributed Economic Dispatch, Cyber Attack, Reliable, Consensus Algorithm, Stealthy Attack, Cyber Resilience



Akıllı Şebekeler için Güvenilir Düğüm Tabanlı Siber Dayanıklı Dağıtık Ekonomik Dağıtım

Öz

Akıllı şebekelerde dağıtık ekonomik dağıtımın (ED) siber güvenliği, sistemin verimli ve güvenilir çalışması için kritik bir öneme sahiptir. Özellikle, bir ajanın kendi maliyet parametrelerini manipüle ederek sistemi gizlice optimal olmayan bir duruma getirdiği sinsi saldırılar, tespitinin zorluğu nedeniyle ciddi bir tehdit oluşturduğu bilinmektedir. Bu çalışma, bahsedilen sinsi maliyet parametresi saldırılarına karşı, uygulaması basit ve mimari tabanlı yeni bir savunma stratejisi sunmaktadır. Önerilen yöntem, ağa stratejik olarak yerleştirilmiş güvenilir düğümler mimarisine dayanmakta ve normal düğümlerin, kötü niyetli ajanlardan gelen anormal verileri güvenilir komşularından aldıkları bilgiye göre proaktif olarak filtrelemesini sağlamaktadır. Stratejinin etkinliği, MATLAB ortamında gerçekleştirilen simülasyonlarla üç farklı senaryo altında test edilmiştir. Sonuçlar, önerilen savunma mekanizmasının saldırıyı başarıyla etkisiz hale getirdiğini, sağlıklı düğümlerin optimal konsensüse ulaşmasını sağladığını ve sistemin ekonomik kayıp yaşamasını engellediği görülmüştür.

Anahtar kelimeler: Dağıtık Ekonomik Dağıtım, Siber Saldırı, Güvenilir, Konsensüs Algoritması, Sinsi Saldırı, Siber Dayanıklılık



Screened by



Except where otherwise noted, content
in this article is licensed under a
Creative Commons 4.0 International
license. Icons by Font Awesome.

1. Introduction

Nowadays, power systems have a decentralized and distributed structure because more renewable energy sources and smart devices are being added to the grids. Since the grid is becoming more dynamic, meeting the instantaneous demand with cheaper energy production is needed for both economic efficiency and system reliability. Distributed Economic Dispatch (ED) stands out as the fundamental method for optimizing the power sharing among energy production units. Even without a central controller, distributed ED algorithms provide significant advantages such as scalability and flexibility. By enabling agents to coordinate through local communication, ED can achieve a global optimal goal.

With the dependence on communication networks, the normal operation of the systems has been less studied. ED systems become vulnerable to cyberattacks. If malicious actors infiltrate the communication and spread false data, the entire system's decision-making mechanism can be manipulated. In recent years, new situations such as the decline in network inertia have increased the feasibility of load-shifting attacks [2], and attackers are developing increasingly complex data-driven methods [3]. Various defense strategies have been proposed to address and prevent these attacks. A significant portion of these strategies are based on the "Detect and Isolate" approach. This method is about continuously monitoring abnormal behavior to identify malicious nodes and isolating them from the network [17]. For example, Huang et al. [4] presented a multi-layered detection and isolation strategy that is resilient against both cooperative and non-cooperative attacks. Similarly, Li et al. [5] developed a defense mechanism that operates in a leader-follower architecture for virtual power plants. However, while these studies generally focus on detecting and isolating the attacks, "stealthy attacks" that target only economic efficiency without disrupting the normal operation of the systems have been less studied. In particular, the type of attack analyzed by Zhao et al. [6], which relies on an agent manipulating its own cost parameters, has been found to pose a significant threat due to the difficulty of detection. Ahmed et al. [7] proposed a resilient, distributed and consensus-based energy management algorithm for economic load distribution in microgrids. The method monitors ramp rate constraints and random false data injection (FDI) attacks. Using two Lyapunov functions, they ensured the protocol's convergence even under attack and optimize the system's energy production costs.

Li et al. [8] proposed a resilient and distributed economic load sharing model under carbon emission trading (CET) and false data injection attacks (FDIA). To decrease the impact of FDIA, they developed a two-layer attack detection mechanism with data compensation strategy, representative-level isolation, and reconfiguration-based response. Chen et al. [9] presented a consensus-based algorithm for privacy-protected distributed economic load sharing in smart grids. Using a state-disaggregation based approach, they ensured that only partial data was transmitted, preventing sensitive information from being exposed to network sniffing. Theoretical analyses and simulations show that the proposed algorithm provides seamless transition between operating modes, fast convergence, and high data security.

Liu et al. [10] defined a new type of black-box FDIA that can be used on smart grids with data-driven algorithms, especially through the measurement modules of distributed power sources. In parallel with these studies on cyber-resilient control and dispatch, recent research in deep learning has shown that the choice of optimization algorithm can significantly affect model accuracy and generalization performance, as demonstrated in the comparative analysis of optimization methods on the Fashion MNIST dataset by Saray and Çavdar [11]. The attack was carried out by generating corrupted data that closely resembles real data and is difficult to detect. Using a generative adversarial network (GAN), experiments indicated serious deterioration in system stability and advanced security risks.

In the review article, Zibaeirad et al. [12] comprehensively examined fundamental threats to smart grid security. Attacks carried out, existing defense methods, and future research opportunities investigated. Technological and methodological solutions proposed against cyber-physical threats, data integrity violations, and next-generation attack techniques were evaluated.

Liao et al. [13] summarized secure power monitoring techniques for smart grids. System architectures were examined, cryptographic protocols and anomaly detection methods investigated. Transmission and monitoring processes were discussed. Applications offered integrated approaches for real-time system security.

Oleinikova et al. [14] compiled recent researches about sustainability and resilience of smart grids from a cyber-physical systems. Particular emphasis was placed on network architectures, threat scenarios, and resilient system designs, along with innovative solution methods proposed through simulations.

Zhao et al. [19] developed a two-stage distribution uncertainty-robust optimization (DRO) method. Aim is to reduce power system's cost when load redistribution (LR) type false data injection attacks occur. Performs real-time redistribution after an attack, taking uncertainties of renewable energy production in account, thereby improving system reliability and economic performance. The work is supported by comprehensive performance analysis on a modified IEEE 30-bus system.

Fiuzu et al. [20] presented a distributed consensus control method for nonlinear fractional-order, multi-agent systems exposed to DoS attacks. They used Lyapunov-based stability and reinforcement learning. Study demonstrated that attack effects can be minimized and global convergence of the system can be achieved.

Yang and Du [21] proposed a finite-time dual consensus algorithm for economic power allocation problem in integrated power systems. This algorithm solves the strong power source dependency, enabling rapid attainment of economic optimization in both islanded and grid-connected modes, and its effectiveness has been demonstrated through simulations.

In literature, there is a gap in the development of a simple and preventive defense mechanism against the specified type of stealth attack.

The primary objective of this study is to develop a simple and effective defense strategy against stealthy cost parameter attacks in smart grids that perform distributed economic load distribution. To this end, a robust consensus algorithm has been designed based on the "Trusted Node" architecture proposed in the literature [15], which filters out false information propagated by malicious agents.

The main contributions of this study to literature are as follows:

- (1) The effectiveness of combining cost parameter manipulation, a sophisticated stealth attack type analyzed in the literature, with the trusted node method filtering, a simple and architecture-based defense mechanism also found in the literature, was tested for the first time.
- (2) It has been demonstrated that a preventive filtering mechanism, which is simpler to implement than complex detection and isolation algorithms, can be an effective solution against stealth attacks.
- (3) The success of the proposed strategy has been validated through MATLAB simulations conducted under different scenarios, proving that the system maintains its stability while preventing economic losses.

The original aspect of the study is that it demonstrates its effectiveness by combining a sophisticated attack model found in the literature with a simple, architecture-based defense mechanism also found in the literature. The rest of the article will introduce the ED problem and the attack model, detail the proposed defense strategy, and finally present simulation findings to draw conclusions and provide an evaluation.

Table 1. Nomenclature

Abbreviations	
ED	Economic Dispatch
λ_i	Scalar incremental cost of the i-th generator
λ	the incremental cost vector for the set of generators
P_i	Scalar power generation of i-th generator
P	Vector for all generators totals power generation
a_i, b_i, c_i	Coefficient for i-th generator's cost function
$C(P_i)$	Cost function
W	Weight Matrix
N	Total generator count
V	Node set
V_r, V_n, V_m	Reliable, Normal and Malicious node sets, respectively
δ_i	i-th generator's scalar power deficit
δ	Vector representing all generator's deficit
k	Iteration count
ρ	Feedback gain parameter
$\tilde{\lambda}_i(k)$	Filtered incremental cost of i-th normal node

1.1. Related works

This section reviews previous studies on cyber resilience in the field of distributed economic load distribution (ED). This review covers research conducted between 2018 and 2025 using the keywords “distributed economic dispatch,” “cyber-attack,” and “resilience” in academic databases such as IEEE Xplore and ScienceDirect. The examined studies are grouped according to the approaches used: basic ED algorithms, attack detection and isolation strategies, attack models, and alternative defense mechanisms.

Consensus-based algorithms play a fundamental role in solving the distributed ED problem. These algorithms aim to reach the system's most efficient operating point as quickly as possible, without cybersecurity. For example, in a study by Tang et al. [1], a new consensus-based ED algorithm was presented for a microgrid operating in island mode that does not require a leader unit and provides fast convergence using a fixed step size. Such studies form the basis of the standard ED algorithm used in the project described in this article.

A significant portion of defense strategies in the literature are based on the logic of continuously monitoring abnormal behavior to detect malicious nodes and then isolating them from the network. Li et al. [5] proposed a defense mechanism with a leader-follower architecture that can detect both cooperative and non-cooperative attacks in their work developed for virtual power plants. This mechanism isolates abnormal agents from the system by tracking their “trust level.” Similarly, Zhang and He [16] targeted “stealth attacks” that covertly compromise the system's optimality and proposed a solution that detects and removes attackers from the network by establishing an observation network based on the neighbor monitoring principle. While effective, these approaches require complex observations and decision-making algorithms.

To develop an effective defense, understanding the attacker's methods is essential. Researches indicate these attacks can be dangerous. Ospina et al. [2] analyzed how real-world events such as the COVID-19 pandemic reduced network inertia, making the system more vulnerable to Load Alteration Attacks (LAA). Lakshminarayana et al. [3] showed that attackers, even with limited data, can design difficult-to-detect False Data Injection (FDI) attacks using advanced mathematical methods such as Random Matrix Theory. A study of critical importance to this work is Zhao et al. [6], which details the “stealthy cost parameter attack” model, where an agent can covertly steer the entire system toward a more costly operating point by manipulating only its own cost parameters, without touching the communication messages.

In addition to the above approaches, there are also defense strategies that target more specific problems or are based on a different philosophy. Zhang et al. [17] focused specifically on Denial of Service (DoS) attacks and proposed a restoration process in which the load of the isolated unit after the attack is redistributed to the remaining healthy units in proportion to their capacity. In the study that forms the basis of this work, Ye et al. [15] proposed placing “Trusted Nodes” in the system from the outset, assuming they would not be attacked, rather than using complex detection algorithms. This architecture presents a simple and effective defense mechanism where normal nodes use information received from their trusted neighbors as a “common sense filter” to block abnormal data at the earliest stage.

The literature review reveals that two main approaches emerge as fundamental for cyber-attack resilience in distributed ED systems: the dynamic “Detect and Isolate” approach and the architecture-based “Preventive Filtering” approach. The first approach [5, 16] is reactive, aiming to intervene after an attack, while the second approach [15] creates a proactive defense line by adding specific trusted agents to the system from the outset and generally offers a simpler algorithmic structure.

Current studies generally focus on complex detection algorithms. On the other hand, the effectiveness of a simple, architecture-based defense strategy against difficult-to-detect and cleverly designed attacks, such as the “stealthy cost parameter attack” proposed by Zhao et al. [6], has not been sufficiently investigated. This study aims to fill this gap. By combining this sophisticated attack model [6] from the literature with a simple and effective defense architecture [15] also found in the literature, this study aims to demonstrate that a solution that is both simple and powerful against such stealthy attacks is possible.

2. Material and Method

This section reviews some studies about cyber resilience in distributed economic load dispatch. Simulation environment and test system used in the study are explained in this section. Mathematical foundations and operation of the proposed reliable node-based resilient economic distribution strategy against stealth cost parameter attacks detailed.

2.1. Material

The simulation environment, test system and parameters are introduced.

2.1.1. Simulation environment

The simulations performed in MATLAB R2024b environment, which is the industry standard for scientific and engineering calculations. All tests were run on a personal computer with a standard configuration.

2.1.2. Test system and parameters

To evaluate the performance of the proposed defense strategy, an 8-generator microgrid test system, also used in the literature [15], was modeled. The communication topology of the system was designed as a connected network in which each node can exchange information bidirectionally with its neighbors. The weight matrix (W) representing this topology was constructed according to the Metropolis-Hastings rule.

The production cost of each generator in the system has been modeled using the widely accepted quadratic cost function. The cost function coefficients (a , b , c) and the minimum (P_{\min}) and maximum (P_{\max}) production capacities of the generators used in the test system have been adapted from the test system model presented in Table 1 of Ye et al. [15] and are presented in Table 2.

Table 2. Generator Parameters

Generator No#	Generator Type	a (mu/MW ²)	b (mu/MW)	c (mu)	P_min (MW)	P_max (MW)
1	Coal	0.00142	7.20	510	150	650
2	Petroleum-1	0.00194	7.85	310	100	400
3	Petroleum-1	0.00194	7.85	310	100	400
4	Petroleum-2	0.00482	7.97	78	50	200
5(Malicious)	Petroleum-1	0.00194	7.85	310	100	400
6(Malicious)	Petroleum-2	0.00482	7.97	78	50	200
7	Petroleum-2	0.00482	7.97	78	50	200
8	Coal	0.00142	7.20	510	150	650

2. 2. Methods

2.2.1. Consensus based distributed economic dispatch

The fundamental objective of ED problem is to minimize total production costs while ensuring that total production meets total demand. This optimization problem is defined by the following mathematical expressions [6]. Where a_i, b_i, c_i are fitting parameters of generation unit i .

$$C_i(P_i) = (a_i * P_i^2 + b_i * P_i + c_i) \quad (1)$$

$C_i(P_i)$ represents the cost function of the i -th generator, while P_i represents power generation. This objective function is subject to the following constraints:

$$\sum_{i=1}^N P_i = \sum_{i=1}^N D_i \quad (2)$$

$$P_{i, \min} \leq P_i \leq P_{i, \max} \quad \forall_i \in V \quad (3)$$

Equation (1) here represents the total cost, equation (2) represents the power balance required for total production to meet total demand, and equation (3) represents the requirement that each generator must operate within its own capacity limits [6].

The optimal solution condition for this problem is that the incremental costs (λ) of all generators (the derivative of cost with respect to production dC/dP , is to be equal. To reach this common equilibrium point in a distributed structure, the consensus-based algorithm used in this study employs the following iterative update rules:

Equation (4) Incremental Cost Update (λ): Each generator updates its own incremental cost value by checking on its neighbors' and its own local power deficit. w_{ij} , represents row element of stochastic matrix of W [6].

$$\lambda_i(k+1) = \sum_{j \in V} w_{ij} \lambda_j(k) + \varepsilon \delta_i(k) \quad (4)$$

Equation (5) Power Generation Update (P): Based on the updated new λ value, each generator's new production amount is calculated within its own cost function and limits [6]. α_i and β_i can be derived from a_i and b_i as shown in [6].

$$P_i(k+1) = \begin{cases} P_i^M, & \lambda_i(k+1) \geq \lambda_i^M \\ \beta_i \lambda_i(k+1) + \alpha_i, & \lambda_i^m < \lambda_i(k+1) < \lambda_i^M \\ P_i^m, & \lambda_i(k+1) < \lambda_i^m \end{cases} \quad (5)$$

Equation (6) Updating the Power Gap (δ): Each generator updates its own local power gap based on its neighbors' gaps from the previous step and the amount of change in its own production. q_{ij} represents column element of stochastic matrix of Q [6].

$$\delta_i(k+1) = \sum_{j \in V} q_{ij} \delta_j(k) - (P_i(k+1) - P_i(k)) \quad (6)$$

With this set of equations system converges to the optimal equilibrium point over time. k is the iteration count. i and j represent the communication weight between nodes. ρ represents a feedback gain. Equation (4) represents the filtered value to which our defense mechanism, explained in the next section, is applied.

2.2.2. Stealth cost parameter attack model

In this study, to test the effectiveness of the proposed defense strategy, the “stealthy cost parameter attack,” a complex type of cyber-attack analyzed by Zhao et al. [6], has been modeled. In this attack model, the malicious agent ($i_a \in \mathbf{V}_m$) manipulates its own economic identity to deceive other agents in the system, rather than directly interfering with messages (λ or δ values) flowing through the communication network.

The attacker spreads false information into the system by replacing the cost function coefficients a_{ia} and b_{ia} defined in Equation (1) with the false values \tilde{a}_{ia} and \tilde{b}_{ia} . This manipulation can be expressed as follows:

$$\tilde{a}_{ia} = a_{ia} + \Delta a_{ia} \quad (7)$$

$$\tilde{b}_{ia} = b_{ia} + \Delta b_{ia} \quad (8)$$

Δa_{ia} and Δb_{ia} represents the false data deviations injected into the system by the attacker. As a result of this manipulation, all well-intentioned agents in the network accept the attacker's false parameters as correct during the consensus process and adjust themselves according to this new situation. Consequently, the system converges to an equilibrium point that satisfies the power balance constraint but is suboptimal, meaning the total production cost is higher than it should be. Because the system reaches equilibrium and does not collapse, the attack is difficult to detect immediately by standard monitoring mechanisms, hence it is termed “stealthy.”

2.2.3. Recommended trusted node-based defense strategy

This study proposes a simple, architecture-based defense strategy against stealth attacks. Strategy is based on the “Trusted Node” concept presented by Ye et al. [15]. Instead of detecting an attack after it has occurred, creating a network architecture that is resistant to attacks prevents the effects of the attack from spreading throughout the network.

This strategy is based on the nodes in the network. Nodes are divided into three different security levels: Trusted Nodes (V_t), which are reinforced against attacks; Normal Nodes (V_n), which have standard security and vulnerable to attacks; and Malicious Nodes (V_m), which have been compromised. For the system's resilience, trusted nodes are assumed strategically placed in the network so that each normal node has at least one trusted neighbor.

The proposed defense mechanism relies on a two-step filtering process applied by each normal node in every consensus iteration. A normal node ($i \in V_n$) performs the following steps immediately before performing the consensus update in Equation (4):

Reasonable Range Determination: A normal node i first identifies the reliable nodes (T_i) among its neighbors. It then determines the current minimum ($\lambda_i^m(k)$) and maximum ($\lambda_i^M(k)$) values of the increasing cost (λ) values coming from these reliable nodes. This range is considered the “reasonable range of correct information” for that iteration.

State Correction (Filtering): A normal node compares its current $\lambda_i(k)$ value with this reasonable range. If its value is outside this range (i.e., it has been affected by a malicious neighbor), it discards its own value and instead uses the average of its reliable neighbors' λ values. The filtered $\tilde{\lambda}_i(k)$ value obtained through this correction process is shown in Equation (9).

From the perspective of the consensus dynamics, the filtering rule in Equation (9) preserves convergence because each normal node still updates its state as a convex combination of its trusted neighbors' states. In other words, the update remains an averaging operation over a connected subgraph that contains at least one trusted node for every normal node, which guarantees that all healthy agents' states are driven toward the same invariant consensus value defined by the trusted nodes. A formal convergence proof for a similar trusted-node-based filtering mechanism can be found in Ye et al. [15] and the proposed strategy in this paper follows the same structure.

$$\tilde{\lambda}_i(k) = \begin{cases} \lambda_i(k), & \text{if } \lambda_i^m(k) \leq \lambda_i(k) \leq \lambda_i^M(k) \\ \frac{1}{|T_i|} \sum_{j \in T_i} \lambda_j(k), & \text{else} \end{cases} \quad (9)$$

Thanks to this mechanism, abnormal λ values caused by a malicious agent's lies about its own parameters are filtered out before being included in the consensus calculation of normal agents. Thus, the spread of the attack's effect across the network is proactively prevented, and the entire system converges toward the correct optimal point.

3. Results

This section presents the simulation studies conducted and the results obtained to validate the effectiveness of the proposed reliable node-based defense strategy against the stealthy cost parameter attack introduced in the previous section. The simulations were performed in the MATLAB environment on the 8-agent test system detailed in Section 3.1.

3.1. Simulation scenarios

To comprehensively evaluate the performance of the proposed defense mechanism, three different scenarios were designed and executed:

Scenario 1-Normal performance state

The ideal situation is one where there are no cyber-attacks in the system and all generators behave normally. This scenario has been used as a benchmark to determine the optimal operating point and cost that the system should achieve.

Scenario 2- Vulnerable under attack state

This is a stealth attack scenario in which the 5th and 6th nodes are malicious and manipulate their own cost parameters. In this scenario, the proposed defense mechanism is inactive. The aim is to clearly demonstrate the negative effects of the attack on the system.

Scenario 3- Guarded under attack state

In an attack scenario where malicious nodes are active, the proposed reliable node-based filtering mechanism is also in operation. This scenario is designed to test the effectiveness of the developed defense strategy in preventing the attack.

3.2. Simulation results

The results obtained under three scenarios are presented below for comparison based on increasing cost (λ) convergence, power generation (P) distribution, total production, and total cost metrics.

The distribution of power generation is examined in figure 2. λ in parallel with the change in values, it can be seen in the case of an unprotected attack (Figure 2-b), the power generation of the generators exhibits a suboptimal and unstable distribution. When the proposed defense mechanism is activated (Figure 2-c), it is observed that the power generation levels of healthy generators return to the optimal distribution seen in the normal operating condition (Figure 2-a).

Figure 1 shows the change in agents' increasing cost (λ) values over iterations under three scenarios. Under normal operation (Figure 1-a), all agents' λ values reach a consensus at a common optimal value (8,8), as expected. In the vulnerable attack scenario (Figure 1-b), it is observed that the system fails to reach consensus due to the false information spread by malicious nodes, and the λ values are scattered across different points. This situation indicates that the system has deviated from the optimal point. When the proposed defense strategy is applied (Figure 1-c), it is proven that while the abnormal λ values of the attacking nodes remain isolated, all other healthy nodes (normal and reliable) successfully converge back to the optimal λ value despite the attack. Figure 3 presents the overall performance of the system in terms of total production and total cost metrics. According to figure 3, the attack on the unprotected system caused total production to fail to meet total demand (2600 MW) and led to system instability.

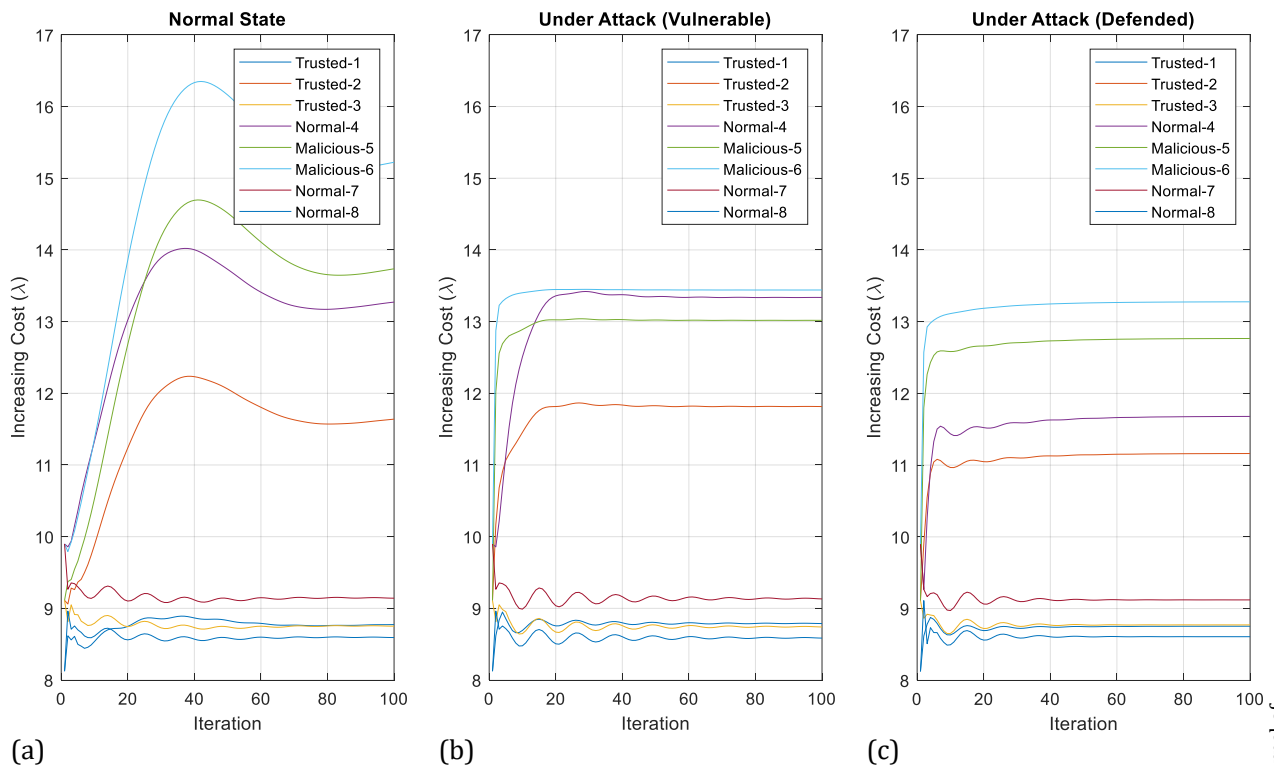


Figure 1. Increasing Cost (λ) Convergence Graphs

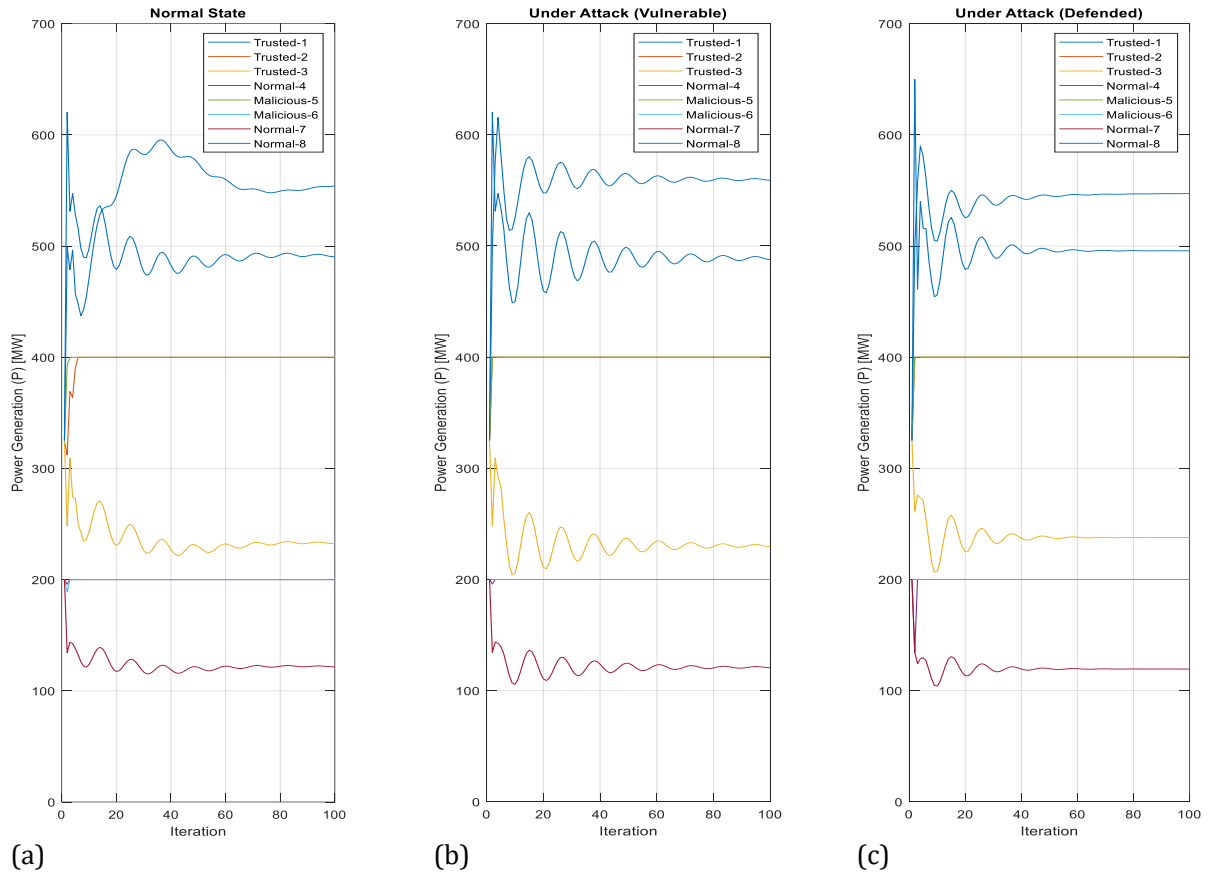


Figure 2. Power Output (P) Convergence Graphs

Simulations indicate that the attack not only causes economic loss but also threatens the system's supply security. The proposed defense strategy succeeds in maintaining supply – demand balance as it does under normal conditions. The cost analysis (figure 3) demonstrates economic success. Attack causes temporary total cost fluctuation on defended (guarded) system, but it recovers. Defended system reaches same level as normal state.

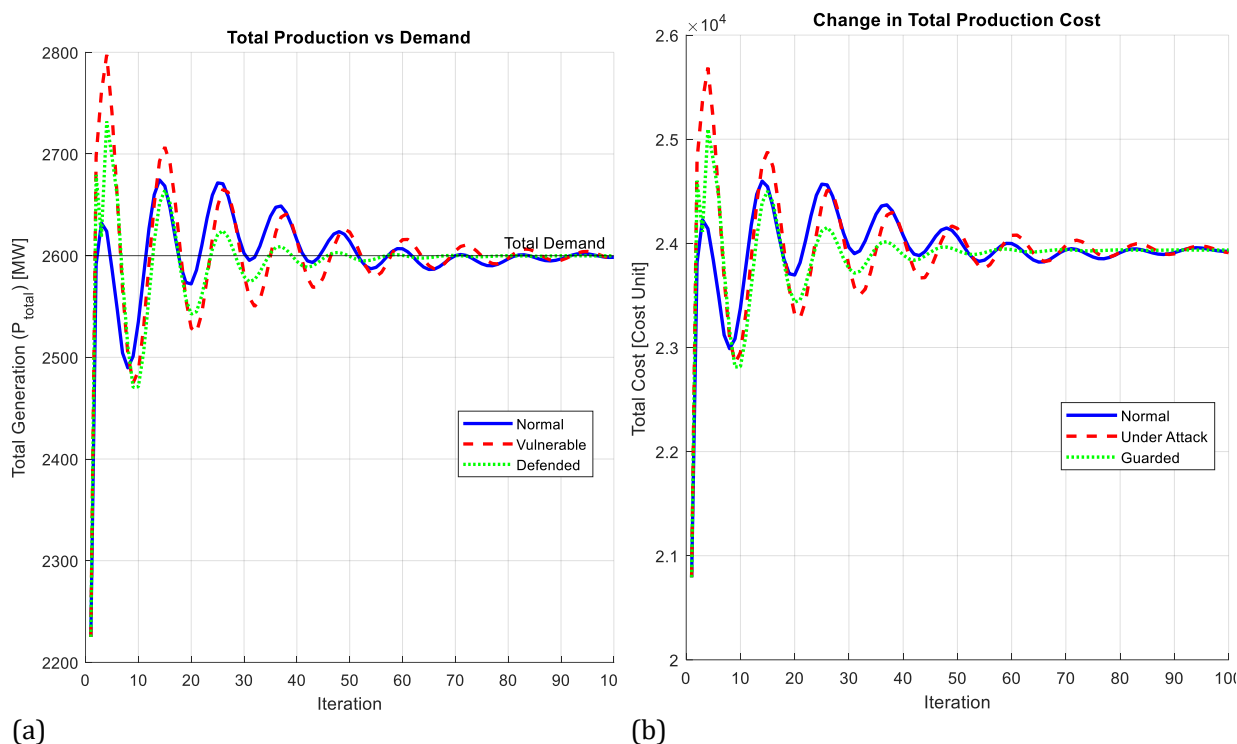


Figure 3. Total Cost and Production Graphs

4. Discussion and Conclusion

Results confirm that stealth cost parameter attacks are a serious threat for distributed ED systems. Under attack, the unprotected system becomes economically inefficient also loses its stability by failing to keep the supply-demand balance.

The proposed reliable node-based defense strategy proven to be highly effective against the threat. Simulation results show that keeping the correct consensus among healthy nodes sustains stability thus system's supply can meet demand. This also helps the system keep at the optimal cost point by preventing the economic loss caused by the attack. With all the benefits and simplicity architecture-based defense mechanisms can be offered as an alternative to complex detection algorithms.

In this study, an effective defense strategy based on reliable node architecture has been proposed and tested to enhance the resilience of smart grids that distribute economic load against stealthy cost parameter attacks. The simulation results obtained clearly demonstrate the success of the proposed method. It has been observed that an unprotected system under such an attack loses its economic efficiency and is driven into instability by failing to maintain the supply-demand balance. In contrast, when the proposed defense mechanism is active, it has been proven that the system successfully converges to its optimal operating point despite the attack and that the total cost is maintained at normal levels.

The most significant implication of the results of this study is that cyber-resilience can be achieved not only through complex detection algorithms but also through simple, architecture-based measures.

A big deal of studies focuses on “detecting and isolating” attacks. To do so incident or the attack must happen at first place [4, 9], but the proactive filtering mechanism presented in this study solves the problem by preventing the spread of false information across the network from the start. This provides a significant advantage, particularly against stealth attacks that are difficult to detect. Therefore, this study contributes to the literature by offering an effective solution that combines a

sophisticated attack model [6] with a simple and preventive defense architecture [15].

Simplicity and proactive protection are the biggest advantages of the offered method. Each normal node performs simple filtering by only using the information received from trusted neighbors (as a reference range). By doing so, complex detection algorithm calculations become unnecessary. The most important assumption underlying the strategy and constraint of the method is the existence of trusted nodes. They must be reinforced against attack within the network, and they must be positioned strategically as neighbors to every normal node.

The results obtained may also have significant implications for practical applications. For microgrid operators, this study demonstrates that physically and cyber-hardening only specific critical nodes (e.g., the system's main controller or largest generators) can provide a significant level of resilience for the entire network, rather than installing complex and expensive cybersecurity software across the entire system. This could offer a cost-effective security strategy, particularly for small-scale networks with limited resources.

Despite the additions this study has certain limitations. The simulations were conducted on an ideal model that lacks real-world factors such as transmission line losses and potential network congestion. Additionally, the test system is limited to 8 agents, and the performance of the proposed method in much larger-scale systems with hundreds of agents remains a topic for future research. Finally, the existence of reliable nodes is assumed, and how these nodes are selected or their optimal placement is beyond the scope of this study. Future work aims to address these limitations and test the method under more realistic network conditions.



Peer-review: External, Independent.

Acknowledgements:

-

Declarations:

1. Statement of Originality:

This manuscript is an original work of the authors. It has not been published previously and is not under consideration for publication elsewhere.

2. Author Contributions:

Concept: TŞ,MYE,HA; **Conceptualization:** TŞ,MYE,HA; **Literature Search:** TŞ,MYE,HA; **Data Collection:** TŞ,MYE,HA; **Data Processing:** TŞ,MYE,HA; **Analysis:** TŞ,MYE,HA; **Writing – original draft:** TŞ,MYE,HA; **Writing – review & editing:** TŞ,MYE,HA.

3. Ethics approval:

Not applicable.

4. Funding/Support:

This work has not received any funding or support.

5. Competing Interests:

The authors declare no competing interests.

6. GenAI Usage Statement:

Generative AI tools were used only for language editing. All outputs were critically reviewed and verified by the authors, and the authors take full responsibility for the final content of manuscript.

7. Sustainable Development Goals:





REFERENCES

- [1] Tang, Z., Hill, D. J., & Liu, T. (2018). A Novel Consensus-Based Economic Dispatch for Microgrids. *IEEE Transactions on Smart Grid*, 9(5), 4535–4546.
- [2] Ospina, J., Liu, X., Konstantinou, C., & Dvorkin, Y. (2021). On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic. *IEEE Access*, 9, 2545–2563
- [3] Lakshminarayana, S., Kammoun, A., Debbah, M., & Poor, H. V. (2021). Data-Driven False Data Injection Attacks Against Power Grids: A Random Matrix Approach. *IEEE Transactions on Smart Grid*, 12(1), 635–646.
- [4] Huang, B., Li, Y., Zhan, F., Sun, Q., & Zhang, H. (2022). A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks. *IEEE Transactions on Industrial Informatics*, 18(2), 880–889.
- [5] Li, P., Liu, Y., Xin, H., & Jiang, X. (2018). A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks. *IEEE Transactions on Industrial Informatics*, 14(10), 4343–4352.
- [6] Zhao, C., He, J., Cheng, P., & Chen, J. (2017). Analysis of Consensus-Based Distributed Economic Dispatch Under Stealthy Attacks. *IEEE Transactions on Industrial Electronics*, 64(6), 5107–5117.
- [7] I. Ahmed, A. Basit, M. Rehan, A. Ali, M. Maaruf, and M. Khalid, “A Resilient Consensus-Based Energy 5.0 Framework for Micro-Grids Under Ramp-Rate Constraints and Stochastic FDI Attacks,” in *2024 IEEE International Conference on Industrial Technology (ICIT)*, pp. 1–7, Mar. 2024, doi: 10.1109/ICIT58233.2024.10540926.
- [8] X. Li, J. Yang, D. Du, Z. Zhou, K. Li, and L. Wu, “Resilient distributed economic dispatch for cyber-physical power systems,” *Energy*, vol. 332, p. 136881, 2025, doi: 10.1016/j.energy.2025.136881.
- [9] W. Chen and G.-P. Liu, “Privacy-Preserving Consensus-Based Distributed Economic Dispatch of Smart Grids via State Decomposition,” *IEEE/CAA Journal of Automatica Sinica*, vol. 11, no. 5, pp. 1250–1263, May 2024, doi: 10.1109/JAS.2023.124122.
- [10] Z. Liu, M. Liu, Q. Wang, and Y. Tang, “False Data Injection Attacks on Data-Driven Algorithms in Smart Grids Utilizing Distributed Power Supplies,” *Engineering*, vol. 51, pp. 62–74, Dec. 2024, doi: 10.1016/j.eng.2024.11.025.
- [11] U. Saray and U. Çavdar, “Comparison of Different Optimization Algorithms in the Fashion MNIST Dataset,” *International Journal of Multidisciplinary Studies and Innovative Technologies*, vol. 8, no. 2, pp. 52–58, 2024, doi: 10.36287/ijmsit.8.2.1.
- [12] A. Zibaeirad, F. Koleini, S. Bi, T. Hou, and T. Wang, “A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities,” *arXiv preprint arXiv:2407.07966*, Jul. 2024.

- [13] T.-L. Liao, C.-P. Lin, and Y.-Y. Hou, "Secure Smart Grid Power Monitoring and Simulations Based on Homomorphic Encryption," *IEEE Access*, vol. 12, pp. 122820–122829, Sept. 2024, doi: 10.1109/ACCESS.2024.3453998.
- [14] I. Oleinikova, D. Mishchenko, and C. Skaga, "Cyber-Physical Studies for Smart Grid Sustainability and Resilience," in *Proc. ESREL-SRA-E 2025: 35th European Safety and Reliability Conference & 33rd Society for Risk Analysis Europe Conference*, pp. 659–665, 2025, doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P7079-cd.
- [15] Ye, T., Zhang, H., & Chen, Z. (2022). Resilient Distributed Optimization Algorithm for Economic Dispatch Against Cyber-Attacks in Smart Grid. In *2022 China Automation Congress (CAC)* (pp. 105-110). IEEE.
- [16] Zhang, W., & He, X. (2018). Stealthy attack detection and solution strategy for consensus-based distributed economic dispatch problem. *Electrical Power and Energy Systems*, 103, 233–246.
- [17] Zhang, Z., Yue, D., Dou, C., Cheng, Z., & Chen, L. (2019). A Robust Consensus-Based Economic Dispatch Strategy Under DoS Attack. In *2019 IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)* (pp. 127-132). IEEE.
- [18] Y. Liu, H. Xin, Z. Qu, ve D. Gan, "An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2923-2932, Nov. 2016.
- [19] P. Zhao, C. Gu, Y. Ding, H. Liu, Y. Bian, ve S. Li, "Cyber-Resilience Enhancement and Protection for Uneconomic Power Dispatch Under Cyber-Attacks," *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 2253-2263, Aug. 2021
- [20] M. Fiuzy ve S. Rass, "Reaching Consensus Under DoS Attacks on the Communication Layer," *2025 Innovations in Intelligent Systems and Applications Conference ASYU*, 2025.
- [21] J. Yang ve J. Du, "Distributed Economic Dispatch Based on Finite-Time Double-Consensus Algorithm of Integrated Energy System," *Frontiers in Energy Research*, vol. 10, Article 907719, Jun. 2022.

