



A Multi-Layer False Data Injection Attack on DFIG Wind Turbine Protection and a Wind-Speed Cross-Check Defense

Amirabbas Homayouni
Zanjan Regional Electric Company

ABSTRACT

Wind turbines based on doubly-fed induction generators are increasingly exposed to cyber-physical threats that target their protection systems. This paper investigates a multi-layer false data injection attack that manipulates the measured rotor speed in a DFIG-based wind turbine to prevent overspeed tripping during storm conditions. The attack is designed to remain inactive until the rotor speed approaches the protection threshold, enabling a stealthy and context-aware activation. Beyond the overspeed relay, the attack also suppresses subsequent protection stages, including delay protection and minimum voltage protection, forming a coordinated and adaptive threat. To counter this, a wind-speed cross-check defense is proposed. The defense continuously compares the reported rotor speed with the actual wind speed and issues a trip command when a sustained inconsistency is detected. Simulation results on a standard MATLAB/Simulink DFIG phasor model demonstrate that the attack successfully avoids turbine tripping during a severe wind gust, while the proposed defense detects the abnormal condition and trips the turbine shortly after the storm begins. The study also examines three attack timing strategies and shows that launching the attack before the storm provides the highest likelihood of success. The findings emphasize the importance of independent protection layers and physics-informed monitoring in cyber-physical wind energy systems.

Keywords: False data injection, DFIG wind turbine, overspeed protection, cyber-physical security, trip suppression.

1. INTRODUCTION

Wind energy has become one of the most important sources of renewable electricity in modern power systems. As the number of wind farms continues to grow, their safe and reliable operation is increasingly important. Many modern wind turbines use doubly-fed induction generators because they offer efficient variable-speed operation and require only a partially rated power converter. However, like other digitalized energy systems, wind turbines now depend heavily on sensors, communication links, and automated protection functions. This dependency makes them vulnerable to cyber-physical attacks [1].

A false data injection attack is a serious type of cyber threat. In such an attack, the adversary modifies measurements or internal signals without directly damaging the equipment. The protection system of a wind turbine relies on measured values such as rotor speed, voltage, and current. If one of these values is changed in a careful way, the protection system may fail to act when it is needed. As a result, the turbine can continue operating under dangerous mechanical or electrical conditions. Several studies have highlighted this risk in renewable energy systems and cyber-physical power grids [2].

The present study focuses on a specific protection function: overspeed protection. Under normal conditions, a sudden increase in wind speed causes the rotor speed to rise. If this speed exceeds a safe limit, the turbine should trip. The goal of the proposed attack is to prevent this trip from happening. To do so, the attacker changes the measured rotor speed before it reaches the protection logic. This causes the protection system to believe that the turbine is still operating in a safe region.

A single-layer attack may not be enough in practice, because modern turbines use more than one protection stage. Therefore, this paper presents a multi-layer attack that disables several protection functions in sequence. After bypassing the overspeed relay, the attack also suppresses the delay protection and the minimum voltage protection stages. This coordinated movement through the protection chain makes the attack

more realistic and more difficult to detect. Similar multi-stage attack concepts have been discussed in the context of industrial control systems and cyber-physical energy systems [3].

The paper also proposes a defense mechanism. The defense is based on a simple idea: the reported rotor speed should be consistent with the measured wind speed. If the wind is very strong but the reported rotor speed remains below a safe threshold for a sustained period, this is considered suspicious. The defense uses this inconsistency to issue an independent trip command.

The rest of the paper is organized as follows. Section 2 presents the simulation setup and system model. Section 3 describes the threat model and the proposed attack. Section 4 explains the defense mechanism. Section 5 defines the simulation scenarios and the location of figures and tables. Section 6 presents and discusses the results. Section 7 concludes the paper.

2. RELATED WORK

Cybersecurity of wind energy systems has received increasing attention in recent years. A comprehensive review of cybersecurity issues in inverter-based power systems with high renewable penetration is provided in [1]. Their work highlights the growing attack surface created by power electronic interfaces and communication-based control. In a similar direction, in [2] review attack detection and defense methods in cyber-physical power systems, emphasizing the need for multi-layer solutions.

Several studies have focused specifically on wind farms. The authors in [3] analyze different attack paths against wind farms and discuss how attackers may interfere with monitoring and control functions. In [4] demonstrate cybersecurity resilience evaluation for wind energy sites using co-simulation, showing the importance of realistic test environments.

False data injection attacks have been studied in the context of renewable energy systems from different perspectives. The authors in [5] propose a deep learning-based detection method for false data injection in renewable power systems. Their work shows that data-driven methods can identify abnormal patterns in measurements. In contrast, our study does not rely on learning-based detection, but instead uses a direct physical consistency check between wind speed and rotor speed.

More recent works have also considered specific protection and control challenges in DFIG-based turbines. The authors in [6] investigate detection and mitigation of cyber-attacks in DFIG-based wind energy systems, which is directly related to the simulation environment used in this paper.

Compared with these studies, the present work focuses on a multi-layer attack that moves through several protection stages, and it also evaluates the effect of attack timing. This combination is less common in the existing literature and forms the basis of the proposed study.

3. SYSTEM MODEL

The study is based on the standard MATLAB/Simulink phasor model of a wind farm using DFIG-based wind turbines, which is provided as a built-in example in the MATLAB environment. This model represents a 9 MW wind farm connected to a local grid with conventional generation and loads. The overall structure of the studied system and the location of the attack and defense blocks are illustrated in Fig. 1. Each turbine includes the aerodynamic and mechanical parts of the wind turbine, a doubly-fed induction generator, a back-to-back converter, and local protection functions. The phasor formulation is suitable for studying electromechanical behavior during grid events, including sudden changes in wind speed [6].

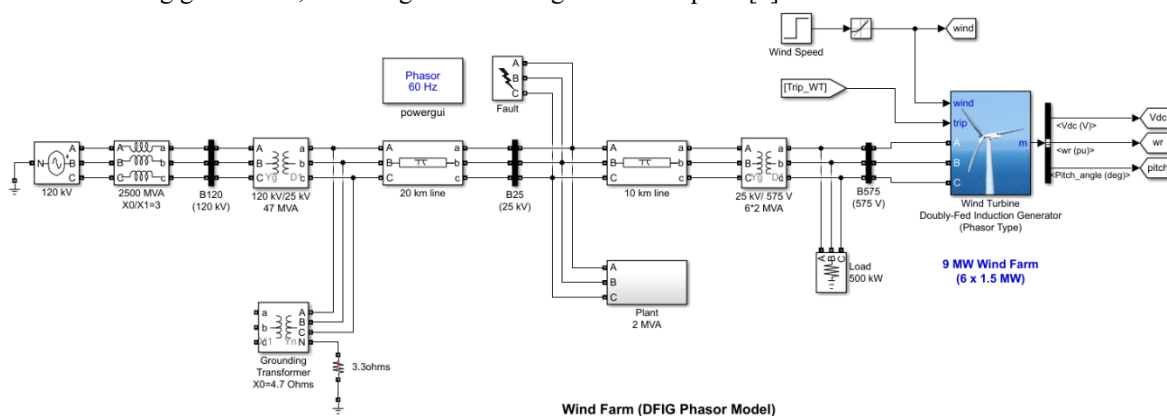


Fig. 1. Overall structure of the studied wind turbine system.

The rotor speed of the turbine is expressed in per-unit with respect to the synchronous speed. Under normal operating conditions, this value remains close to the nominal range. When the wind speed rises rapidly, the rotor accelerates. If the speed exceeds a predefined threshold, the overspeed protection should issue a trip command to disconnect the turbine from the grid. This protection path is the main target of the proposed attack.

The turbine is protected by several complementary stages. The overspeed relay is activated when the measured rotor speed exceeds a set limit. A second protection stage, referred to here as delay protection, acts on similar signals but includes a time delay to avoid unnecessary trips during short transients. A third stage monitors the minimum terminal voltage and issues a trip if the voltage falls below a safe level. In a normal protection sequence, these layers provide a coordinated defense against different abnormal conditions [7].

The measured rotor speed is the most important signal for this study. The attack modifies this signal before it reaches the protection logic, while the physical turbine continues to operate with its own internal dynamics. This separation between the physical speed and the speed seen by the protection system is the central idea of the proposed attack described in the next section.

4. THREAT MODEL AND ATTACK DESIGN

The attacker is assumed to have remote access to the measurement and protection signals of a DFIG wind turbine. The attacker does not physically damage the turbine, but can modify sensor data before it reaches the protection logic. This type of manipulation is consistent with false data injection scenarios discussed in previous studies on wind turbine cybersecurity [8]. Unlike attacks that target the power converter directly, the proposed attack focuses on the protection chain.

The main goal of the attacker is to prevent the turbine from tripping during a severe wind gust. To achieve this, the attacker first injects a negative bias into the measured rotor speed signal. The bias is not applied permanently. It is only activated when the actual rotor speed approaches the overspeed threshold. This design makes the attack context-aware and reduces the chance of being detected during normal operation. Similar conditional attack strategies have been considered in the context of stealthy and multi-stage attacks in cyber-physical systems [9].

The attack is structured in three stages. In the first stage, the rotor speed signal is manipulated so that the overspeed relay does not see the true speed. Previous work has also shown that false data injection can directly affect protection relays in power systems with high renewable penetration [10]. If a third stage, such as the minimum voltage protection, begins to react to the abnormal condition, it is also suppressed. This coordinated movement through the protection chain makes the attack multi-layer. The structure of the attack and the signals involved are illustrated in Fig. 2.

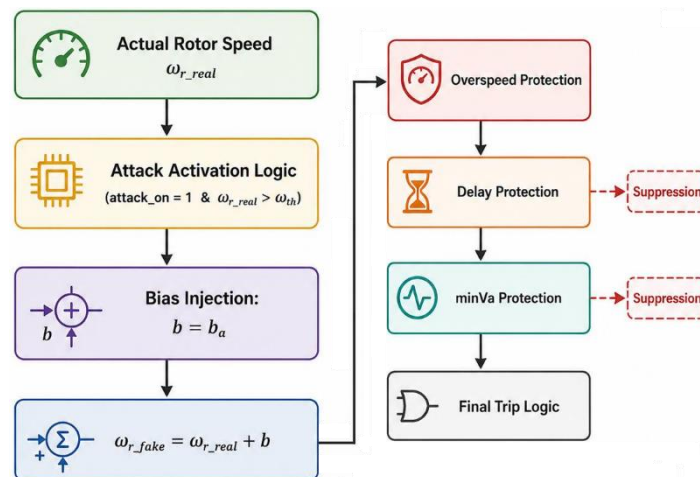


Fig. 2. Structure of the proposed multi-layer false data injection attack, showing the rotor speed measurement path, the bias injection point, and the suppression of backup protection stages.



To implement the attack in simulation, a MATLAB function is used to generate the bias. The fake rotor speed signal is formed as:

$$\omega_{r_fake} = \omega_{r_real} + b \quad (1)$$

where ω_{r_real} is the actual rotor speed, b is the injected bias, and ω_{r_fake} is the speed value received by the protection system.

The injected bias is activated only under a specific condition:

$$b = \begin{cases} b_a & \text{if } attack_on = 1 \text{ and } \omega_{r_real} > \omega_{th} \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

where b_a is the attack bias value and ω_{th} is the rotor speed threshold above which the attack becomes active.

The function compares the measured rotor speed with a predefined activation threshold. If the attack is enabled and the rotor speed is above the threshold, a negative bias of 0.4 per-unit is applied. The resulting signal is referred to as the fake rotor speed. The protection logic receives this fake value while the actual rotor dynamics remain unchanged. This approach is in line with previous works that model false data injection as a manipulation of a specific sensor path rather than a full system compromise [8].

The attack also includes a timing dimension. Three possible attack start times are considered. The attacker can launch the attack before the storm, at the same time as the storm, or after the storm has already begun. Based on the simulation results, the pre-storm scenario is the most reliable because the attack is already active when the rotor begins to accelerate. Delaying the attack may cause the attacker to miss the narrow time window before a protective trip occurs. The importance of timing in coordinated cyber-physical attacks has also been highlighted in recent assessments of wind turbine cyber safety [11].

5. DEFENSE MECHANISM

The proposed defense is based on a simple physical consistency check. Under normal conditions, a strong wind gust should cause a rapid increase in rotor speed. If the measured rotor speed remains below a safe threshold during such an event, this may indicate that the speed signal has been manipulated. The defense uses this relationship between wind speed and rotor speed to detect the attack. The defense compares the reported rotor speed with the actual wind speed. The defense trip condition is defined as:

$$D_{trip} = \begin{cases} 1 & \text{if } (V_{wind} > V_{th}) \text{ and } (\omega_{r_fake} < \omega_{safe}) \text{ for } T_d \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

where V_{wind} is the measured wind speed, V_{th} is the wind speed threshold, ω_{safe} is the safe rotor speed limit, and T_d is the confirmation time.

If the wind speed exceeds a predefined limit and the reported rotor speed is still below a conservative threshold, the defense starts a timer. If this condition remains true for more than two seconds, a trip command is issued. The trip signal from the defense is connected to the turbine protection circuit, independent of the manipulated rotor speed path. This independence is important, because the attacker can modify the rotor speed signal but does not necessarily control the wind speed measurement. This independent protection layer follows the same philosophy as data-driven anomaly detection methods that identify abnormal patterns in wind turbine SCADA systems [12]. The structure of the proposed defense mechanism is illustrated in Fig. 3.

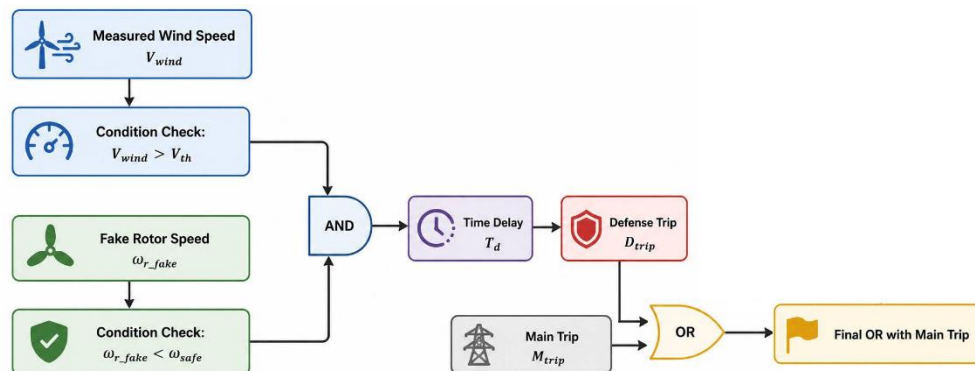


Fig. 3. Block diagram of the wind-speed cross-check defense, showing the comparison logic, the time delay, and the final trip connection.

This approach follows the general principle of physics-informed detection, which uses known relationships between physical quantities to identify abnormal behavior. Similar ideas have been applied in recent studies for cyber-attack detection in wind farms and renewable power systems [13], [14]. The key advantage of this method is that it does not require any information about the attack start time or the attacker's behavior. It only uses measurable signals that are already available in the wind farm monitoring system.

The defense also avoids the use of machine learning or complex models. Instead, it relies on a direct comparison between two signals. This makes the method easy to implement in practice and easier to validate in a simulation environment. It also reduces the risk of false alarms, because the two-second delay filters short transients that may occur during normal operation. Layered and cross-layer defense strategies have also been considered in previous works for cyber-physical wind energy systems, supporting the idea that protection should not rely on a single signal path [15]. This simplicity is important, since more advanced detection methods may not always be practical for field implementation [13].

In the simulation model, the defense is implemented using a set of comparators and a delay block. The output of the comparators is combined using an AND gate, and the result is passed through an on-delay timer. The final trip signal is then merged with the main trip path using an OR gate. This structure allows the defense to act as an additional protection layer without affecting the normal protection logic.

6. SIMULATION SCENARIOS

The performance of the proposed attack and defense is evaluated using three main simulation scenarios. All scenarios use the same wind profile and the same DFIG wind farm model. The only difference between the scenarios is whether the attack or defense is active.

In the first scenario, referred to as the healthy case, no attack is applied. The wind speed is initially set to a moderate value and then increases sharply at a defined time to simulate a storm. In this case, the rotor speed rises quickly and crosses the overspeed threshold. The turbine is expected to trip and disconnect from the grid. This scenario serves as the baseline.

In the second scenario, only the attack is active. The attacker modifies the measured rotor speed using the proposed multi-layer false data injection method. The overspeed relay is therefore not able to see the actual rotor speed. In addition, the delay protection and the minimum voltage protection stages are suppressed. As a result, the turbine continues operating despite the severe wind conditions. This scenario demonstrates the success of the attack.

In the third scenario, both the attack and the proposed defense are active. The attack manipulates the rotor speed signal as in the second scenario. However, the wind-speed cross-check defense monitors the inconsistency between the reported rotor speed and the actual wind speed. Once the condition remains true for more than two seconds, the defense issues an independent trip command. The turbine is then disconnected even though the attacker has bypassed the main protection layers. The wind speed profile used in all scenarios is shown in Fig. 4.

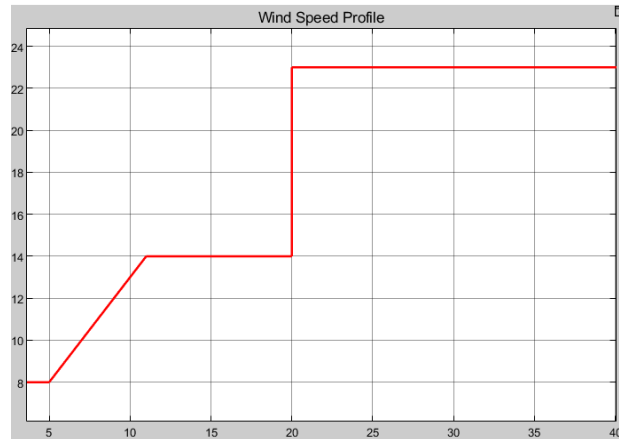


Fig. 4. Wind speed profile used in all simulation scenarios.

The profile includes a stable low-speed period, followed by a gradual increase and then a sudden jump to storm-level wind speed. This shape allows the protection system to be tested under a realistic and repeatable condition. A comparison of Real and fake rotor speed under attack is presented in Fig. 5.

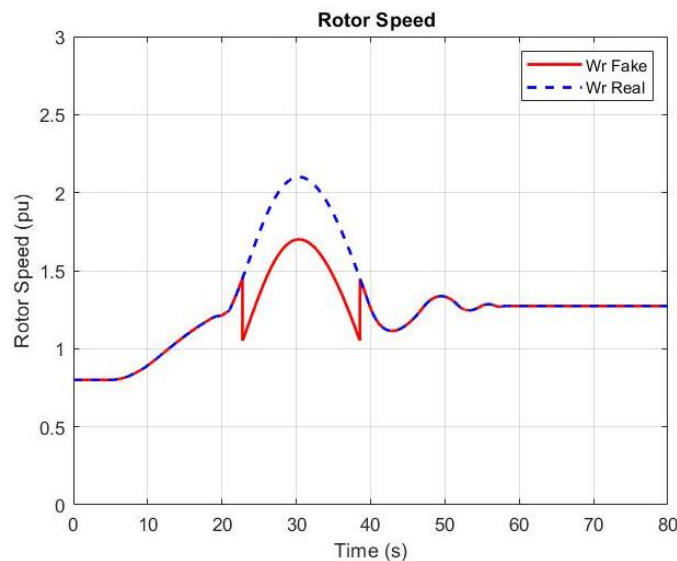


Fig. 5. Real and fake rotor speed under attack.

Fig. 5 shows both the actual and the manipulated rotor speed signals under attack conditions. During the storm, the actual rotor speed increases significantly and exceeds the safe operating range. However, the fake rotor speed received by the protection system remains below the overspeed threshold. This difference allows the attack to remain undetected by the main protection stage and explains why the overspeed relay does not issue a trip command.

Before the defense trip instant, the two curves follow the same path, since the attack logic is identical in both cases. After the defense issues its trip command, the curves are no longer physically meaningful. The trip signals for the attack-only and attack-plus-defense scenarios are shown in Fig. 6.

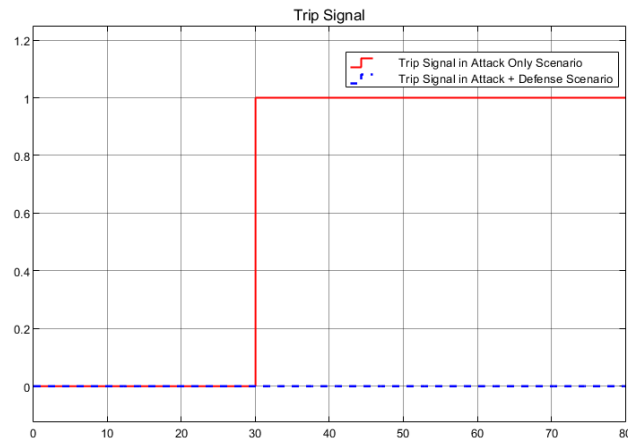
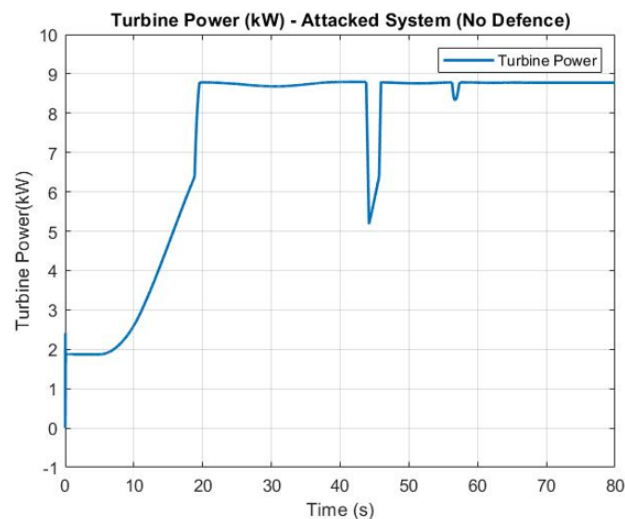


Fig. 6. Trip Signal in Attack-Only and Attack+Defense Scenarios.

In the attack-only scenario, no trip command is generated during the entire storm, which confirms that the multi-layer false data injection attack successfully bypasses the protection chain. In the attack-plus-defense scenario, the defense mechanism detects the sustained inconsistency between the reported rotor speed and the wind speed, and after the confirmation delay, it issues a trip command. The resulting trip signal is shown in Fig. 6.

The healthy case produces a trip shortly after the storm begins. In the attack-only case, no trip is generated. In the attack-plus-defense case, the trip appears after a short delay caused by the two-second confirmation timer. The active power output of the turbine is compared in Fig. 7.



(a)

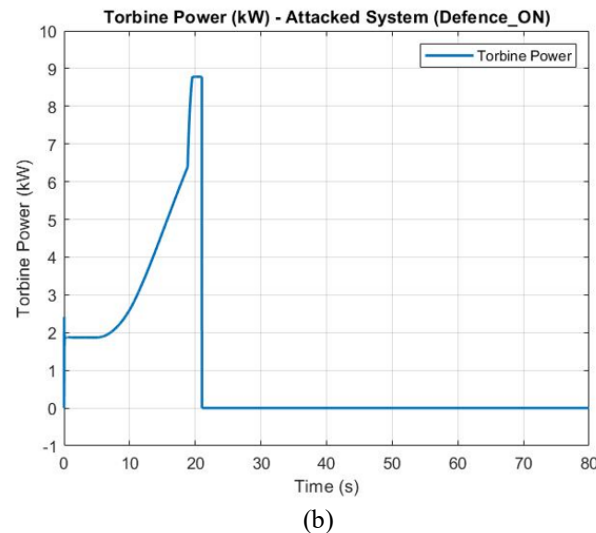


Fig. 7. Active power output: (a) attack-only scenario, (b) attack-plus-defense scenario.

In the attack-only scenario, the protection system does not detect the manipulated rotor speed and therefore no trip signal is generated. The turbine remains connected and continues delivering active power during the storm. In the attack-plus-defense scenario, the proposed defense detects the inconsistency between wind speed and rotor speed, issues an independent trip command, and disconnects the turbine to prevent possible damage. This difference is clearly visible in the active power responses shown in Fig. 7.

In the healthy and defense cases, the output power drops to zero after tripping. In the attack-only case, the turbine remains connected and continues generating power during the storm. Table 1 summarizes the configuration of the three main scenarios.

Table 1. Scenario configuration.

Scenario	Attack	Defense	Expected result
Healthy	Off	Off	Trip occurs
Attack only	On	Off	No trip occurs
Attack + Defense	On	On	Defense trip occurs

In addition to these three scenarios, a separate timing analysis is performed. The attack is launched before the storm, at the same time as the storm, and after the storm has already begun. The objective of this analysis is to determine how the starting time of the attack affects its success. The results of this timing comparison are presented in the next section.

7. RESULTS AND DISCUSSION

The simulation results confirm that the proposed attack can effectively prevent the turbine from tripping under storm conditions. In the healthy scenario, the rotor speed exceeds the overspeed threshold shortly after the sudden increase in wind speed, and the protection system trips the turbine as expected. This result is consistent with the normal operation of the DFIG protection system.

In the attack-only scenario, the behavior of the system is completely different. Although the actual rotor speed increases significantly during the storm, the fake rotor speed received by the overspeed relay remains below the trip threshold. The relay therefore does not issue a trip command. In addition, the delay protection and minimum voltage protection stages are suppressed. As a result, the turbine remains connected and continues generating power during the storm. This outcome confirms that the multi-layer attack is successful.

The proposed defense changes this result. When the defense is active, it observes the inconsistency between the high wind speed and the low reported rotor speed. After the two-second confirmation delay, the



defense issues an independent trip command. The turbine is disconnected even though the attacker has bypassed the main protection layers. This shows that a simple physics-informed cross-check can still detect the attack.

Fig. 5, presented in the previous section, shows that before the defense trip instant, the fake rotor speed in the attack-only and attack-plus-defense scenarios follows the same path. This confirms that the attack behavior is identical in both cases and that the defense does not interfere with the attack before its own activation.

The effect of attack timing is also important. When the attack is launched before the storm, the fake rotor speed is already being manipulated when the rotor begins to accelerate. The overspeed relay is therefore bypassed from the beginning of the dangerous period. When the attack is launched at the same time as the storm, the result is similar. However, when the attack is launched after the storm has already begun, the turbine may trip before the attack becomes active. This shows that the pre-storm strategy is the most reliable for the attacker.

The active power output in Fig. 7 also reflects these differences. In the healthy and defense cases, the output power drops to zero after the trip. In the attack-only case, the output power remains high, which indicates that the turbine is still operating under severe mechanical stress. This is exactly the condition that the protection system is supposed to prevent.

Overall, the results highlight three main points. First, a coordinated false data injection attack can bypass multiple protection stages in a DFIG wind turbine. Second, attack timing plays a key role in the success of the attack. Third, a simple wind-speed cross-check can provide an additional layer of protection without requiring complex models or external information.

It is also worth noting that the proposed detection and defense mechanism remains effective if the false data injection attack is applied gradually, such as in the form of a ramp. In this case, the behavior of the defense is similar to the scenario with a sudden step-like injection, since the final inconsistency between the reported rotor speed and the wind speed still appears and triggers the same protection logic.

8. CONCLUSION

This paper investigated a multi-layer false data injection attack against the overspeed protection of a DFIG-based wind turbine. The attack was designed to manipulate the measured rotor speed before it reached the protection logic, while also suppressing the delay protection and minimum voltage protection stages. The simulation results showed that this coordinated attack could prevent the turbine from tripping during a severe storm.

A wind-speed cross-check defense was proposed to counter this threat. The defense compared the reported rotor speed with the actual wind speed and issued a trip command when an inconsistency continued for more than two seconds. The defense did not require knowledge of the attack timing and operated independently of the manipulated rotor speed path. The results confirmed that this simple defense could detect the attack and disconnect the turbine before severe damage occurred.

The study also examined the effect of attack timing. The results showed that launching the attack before the storm was the most reliable strategy for the attacker. If the attack was delayed until after the storm had already begun, the turbine could trip before the attack became active.

Overall, the findings emphasize that modern wind turbines need independent protection layers that do not rely only on a single sensor path. A simple physics-informed comparison between different measurements can provide effective protection against false data injection attacks. Future work may extend this approach to larger wind farms and consider more complex attack scenarios involving coordinated multiple turbines or communication network delays.

REFERENCES

- [1] Tuyen, Nguyen Duc, Nguyen Sy Quan, Vo Ba Linh, Vu Van Tuyen, and Goro Fujita. "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy." *IEEE Access* 10 (2022): 35846-35875.
- [2] Du, Dajun, Minggao Zhu, Xue Li, Minrui Fei, Siqi Bu, Lei Wu, and Kang Li. "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems." *Journal of Modern Power Systems and Clean Energy* 11, no. 3 (2022): 727-743.

- [3] Ambarita, Evi Elisa, Ivan Kuncara, Augie Widyotriatmo, Anniken Karlsen, Francesco Scibilia, and Agus Hasan. "On cyber-attacks against wind farms." In *IECON 2023-49th Annual Conference of the IEEE Industrial Electronics Society*, pp. 1-6. IEEE, 2023.
- [4] Mccarty, Michael, Jay Johnson, Bryan Richardson, Craig Rieger, Rafer Cooley, Jake Gentle, Bradley Rothwell et al. "Cybersecurity resilience demonstration for wind energy sites in co-simulation environment." *IEEE Access* 11 (2023): 15297-15313.
- [5] Almutairy, Fayha, Lazar Scekic, Ramadan Elmoudi, and Safwan Wshah. "Accurate detection of false data injection attacks in renewable power systems using deep learning." *IEEE Access* 9 (2021): 135774-135789.
- [6] Paul, Sumit, Prakash Kumar, and Kalyan Chatterjee. "Detection and mitigation of cyber attack in DFIG based wind energy systems." *Sustainable Energy, Grids and Networks* (2025): 102057.
- [7] Menezes, Thiago Souza, P. H. A. Barra, F. A. S. Dizioli, V. A. Lacerda, Ricardo Augusto Souza Fernandes, and Denis V. Coury. "A survey on the application of phasor measurement units to the protection of transmission and smart distribution systems." *Electric Power Components and Systems* 52, no. 8 (2024): 1379-1396.
- [8] Zhao, Shiyi, Qinmin Yang, Peng Cheng, Ruilong Deng, and Jinhui Xia. "Adaptive resilient control for variable-speed wind turbines against false data injection attacks." *IEEE Transactions on Sustainable Energy* 13, no. 2 (2022): 971-985.
- [9] Hu, Yan, Yuyan Sun, Youcheng Wang, and Zhiliang Wang. "An enhanced multi-stage semantic attack against industrial control systems." *IEEE Access* 7 (2019): 156871-156882.
- [10] Jafari, Mohamadsaleh, Md Hassan Shahriar, Mohammad Ashiqur Rahman, and Sumit Paudyal. "False relay operation attacks in power systems with high renewables." In *2021 IEEE Power & Energy Society General Meeting (PESGM)*, pp. 01-05. IEEE, 2021.
- [11] Aarsal, Muhammad, Hafizul Asad, Tamer Kamel, and Asiya Khan. "Cyber-safety assessment of wind turbines: A reachability analysis approach against cyber-attacks." In *International Conference on Computer Safety, Reliability, and Security*, pp. 340-354. Cham: Springer Nature Switzerland, 2025.
- [12] Chen, Juntao, and Quanyan Zhu. "A cross-layer design approach to strategic cyber defense and robust switching control of cyber-physical wind energy systems." *IEEE Transactions on Automation Science and Engineering* 20, no. 1 (2022): 624-635.
- [13] Alotibi, Faris, and David Tipper. "Physics-informed cyber-attack detection in wind farms." In *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 1-6. IEEE, 2022.
- [14] Chen, Hansi, Hang Liu, Xuening Chu, Qingxiu Liu, and Deyi Xue. "Anomaly detection and critical SCADA parameters identification for wind turbines based on LSTM-AE neural network." *Renewable Energy* 172 (2021): 829-840.
- [15] Liu, Chensheng, Yongyu Li, Yang Yu, Xiaoming Wu, Ming Yang, Yang Tang, and Jian Long. "Spatiotemporal Stealthy Attacks in Power Systems with High Penetrated Renewable Energy Sources." *IEEE Internet of Things Journal* (2025)..