T-IDS: A Thermal-Model-based Intrusion Detection System for Wind Turbines

Ngoc Que Anh Tran
University of Colorado Denver
Denver, CO, USA
ngocqueanh.tran@ucdenver.edu

Liang He
University of Colorado Denver
Denver, CO, USA
liang.he@ucdenver.edu

ABSTRACT

This paper advances the intrusion detection of wind turbines by exploiting the inter-dependent thermal behaviors of individual modules within the turbines. Specifically, we present a novel thermal-model-based intrusion detection system, called T-IDS, to detect intrusions causing abnormal thermal behaviors of the turbines, such as those causing damaged physical modules (and hence heating) or manipulating the temperature readings. T-IDS consists of three key components: a graph model describing the dependencies among thermal variables of wind turbines, a random forest-based method to predict thermal variables in the steering of the thermal graph and a method to detect anomalies by cross-validating the predicted thermal variables with their empirical observations. The optimal configuration of T-IDS is also examined to ensure its robustness. We have evaluated T-IDS using a dataset containing the Supervisory Control And Data Acquisition (SCADA) log of a wind turbine over six months. The results show that T-IDS detects anomalies with an average accuracy of 97.6% while incurring no false detection.

KEYWORDS

wind turbines, intrusion detection, thermal behavior

ACM Reference Format:
Ngoc Que Anh Tran and Liang He. 2024. T-IDS: A Thermal-Model-based Intrusion Detection System for Wind Turbines. In *The 15th ACM International Conference on Future and Sustainable Energy Systems (E-Energy '24), June 04–07, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3632775.3661991

1 INTRODUCTION

Rising greenhouse emissions have dire consequences, with an estimated 8.3 million deaths per year resulting from exposure to toxic air pollution [5]. To combat this alarming trend, wind turbines are proving to be a pivotal player in phasing out traditional energy sources and ushering in a new era of renewable energy. As the largest renewable energy source in the United States, wind power generation has surpassed 650 GW in 2022 and consistently increased by 60 GW annually. Wind turbines serve as the crucial infrastructure that effectively converts kinetic wind power into electrical energy.

E-Energy '24, June 04–07, 2024, Singapore, Singapore

ACM ISBN 979-8-4007-0480-2/24/06
https://doi.org/10.1145/3632775.3661991

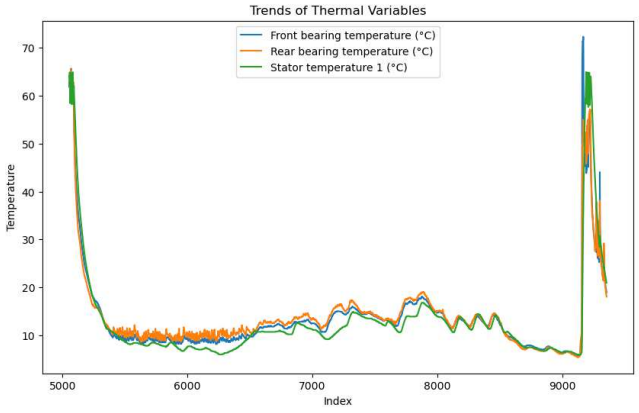

Figure 1: The temperatures of different modules of a wind turbine are highly correlated.

However, the increasing popularity of wind energy has also made it a prime target for attackers because the energy sector has been one of the most targeted sectors since 2014 [4]. Additionally, the growing reliance on wind farms to power the nation's grid is not aligned with the resilience in protecting wind turbine systems and their infrastructure against cyber attacks. The remote locations of wind farms, coupled with the massive size of turbines, make wind turbine facilities vulnerable to various risks, including unauthorized access, control manipulation, operational disruptions, and physical damage to turbines and substations. Furthermore, the broad deployment of Supervisory Control and Data Acquisition (SCADA) systems further escalates the risk of intrusive attacks that can compromise the integrity of onboard fault detection methods [1, 12]. Addressing these security challenges is critical to ensure a secure and reliable energy supply.

To mitigate these critical concerns and enhance the safety of wind turbine systems, this paper presents T-IDS, a thermal-model-based intrusion detection system. T-IDS is inspired by the reliable relationships between the thermal variables of wind turbine components. For instance, Figure 1compares the real-time temperature of three turbine modules: the stator, the front bearing, and the rear bearing, highlighting a clear correlation among the three-time series. Acquiring knowledge of this correlated behavior allows the construction of a comprehensive thermal model for wind turbines, providing a promising opportunity to detect anomalies/intrusions that lead to abnormal temperature readings at various turbine modules.

The innovative system T-IDS consists of three key components: a graph-based thermal model depicting the dependency among the

temperatures of various turbine modules, a random forest-based algorithm to predict the temperature of a target turbine module based on the thermal graph and an anomaly detector that cross-validates the predictions with their empirical observations to detect potential anomalies. T-IDS was evaluated using a real-life dataset consisting of the SCADA log from one wind turbine over six months [2]. The findings reveal that T-IDS detects anomalies in the temperature readings of different turbine modules with an average accuracy of 97.6% while incurring zero false detection.

In summary, this paper makes the following three noteworthy contributions.

- Uncovering and constructing a comprehensive thermal model describing the dependencies among the temperatures of various turbine modules.
- Designing T-IDS, a thermal-model-based intrusion detection system to detect anomalies and intrusions of wind turbines.
- Evaluating T-IDS on a real-world dataset that logs the wind turbine operation for six months.

2 RELATED WORK

While the security of wind turbines is becoming increasingly important, various studies show interest in developing methods to enhance security resilience from physical and cyber-attacks. Staggs et al. provided many mitigations to prevent wind turbines from getting attacked by intruders and increase the physical and cyber resilience of wind turbines and wind farms [8]. However, Staggs's study still has space to develop a comprehensive method to prevent or detect cyber intrusion attacks. Alternatively, Megan Egan proposed recommendations on policies ensuring sustainable communications of wind farms to improve cyber resilience [9]. Nevertheless, the study must address situations where attacks happen while maintaining normal system operations or when intruders manipulate wind turbine sensors to cover their activities.

Many other studies show interest in developing wind turbine component-based methods. Bin Chen et al. studied an acoustical damage detection method based on a Bayesian network [3]. Teng Wei et al. showed interest in fault detection in wind turbines by analyzing vibrational behaviors [10]. Nevertheless, acoustical, vibrational, and oil analysis require additional costs due to the installation of extra sensors for data collecting and background noise cancellation, regardless of their limited performance [11]. Alternatively, developing fault detection of wind turbine component-based methods has recently drawn significant attention from scientists. Yirong Liu et al. provided an efficient early fault detection method by training an extreme gradient-boosting prediction model for gearbox oil temperature [6]. Furthermore, alternative methods using machine learning algorithms, such as k-nearest neighbors and artificial neural networks, were also studied. However, the solutions provided still need to address common limitations. Regardless of the promising results, they need to improve because they rely on a single variable and incompletely analyze the interrelationship among variables of wind turbine components [7].

In response to these limitations, T-IDS lays its foundation on performing insightful analysis of the underlying dynamics of wind turbine components. T-IDS uses a novel anomaly detection method capitalizing on the thermal model graph. By detecting deviations from reference thermal patterns, T-IDS can identify anomalies that indicate potential issues with wind turbine components. This study conducts expansive experiments to evaluate T-IDS's effectiveness in anomaly detection. The results show a high accuracy rate in detecting anomalies in wind turbine components. Another critical contribution of T-IDS is providing comprehensive optimal configurations for the developed system, ensuring robust anomaly detection accuracy across all applications. The development of T-IDS promises to offer a complete anomaly detection framework to reduce the impacts of intrusive attacks on SCADA systems and to increase the general efficiency of the wind turbine system.

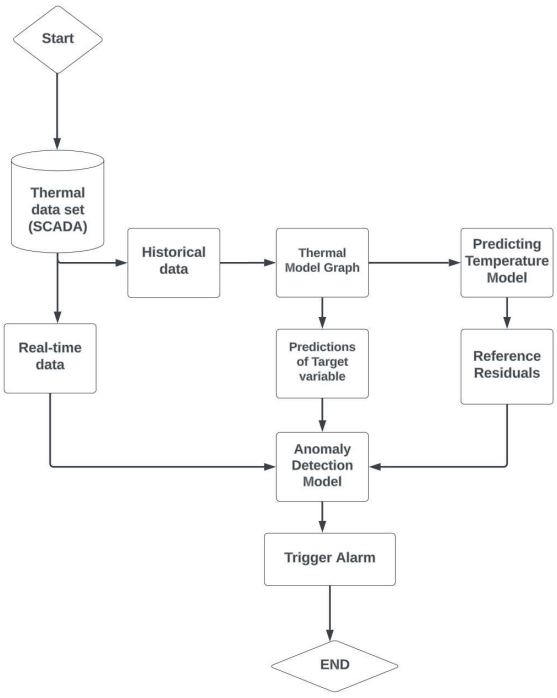

Figure 2: Overview of T-IDS.

3 DESIGN OF T-IDS

Figure 2 shows an overview of T-IDS, which consists of three major components: the thermal graph describing the interdependencies among the temperature of different modules of a wind turbine, a temperature predictor that predicts the temperature of the target module using machine learning algorithms with high accuracy, and an anomaly detector that cross-validates the predictions with their empirical observations to detect anomalies. We will explain each of these components in the next.

3.1 Graph-based Thermal Model

The thermal graph lays the foundation of T-IDS, where each node denotes the temperature of a given turbine module, and the weighted edges quantify the strength of the dependency between the thermal behaviors of associated nodes/modules. Specifically, T-IDS uses the Pearson linear correlation coefficient to quantify the strength of the dependency between two thermal variables. The graph is

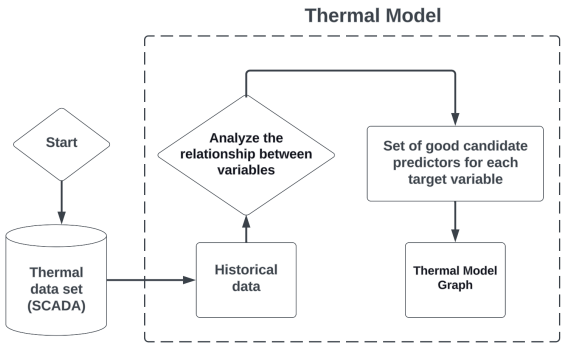

Figure 3: The process to generate the thermal graph.

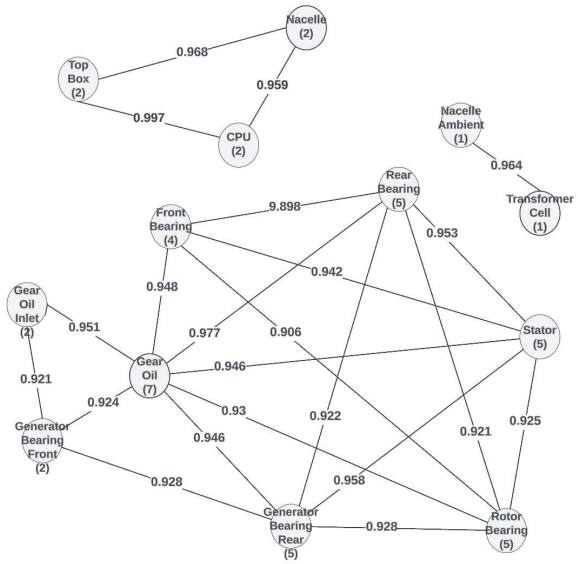

Figure 4: A thermal graph example generated based on the dataset in [2].

constructed based on a given threshold for the correlation strength α, i.e., an edge exists in the graph if its weight is no smaller than α.

The thermal graph serves two purposes for T-IDS. First, it defines T-IDS's capability in anomaly detection, i.e., the thermal variables that T-IDS can diagnose to detect anomalies. Also, the thermal graph guides the prediction of the temperature of the target module by identifying which input variables should be used to complete the prediction — the nodes that connect with the target module in the thermal graph. Figure 3 shows the flowchart for constructing the thermal graph. Figure 4 illustrates an example graph constructed based on the dataset [2].

3.2 Temperature Predictor

The temperature predictor estimates the temperature of a target module. The thermal graph steers this prediction to identify the modules whose temperature strongly depends on the target — they will be the promising input for the prediction. We train the predictor

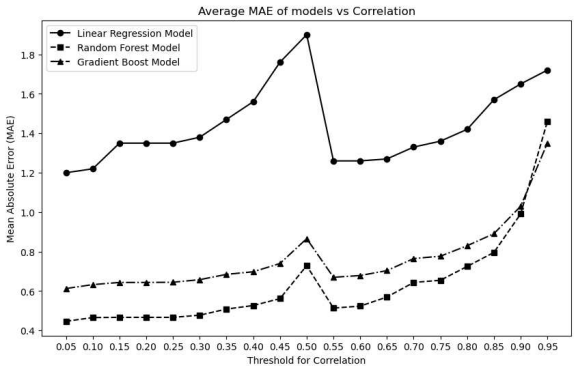

Figure 5: The average MAE when predicting temperature using different methods.

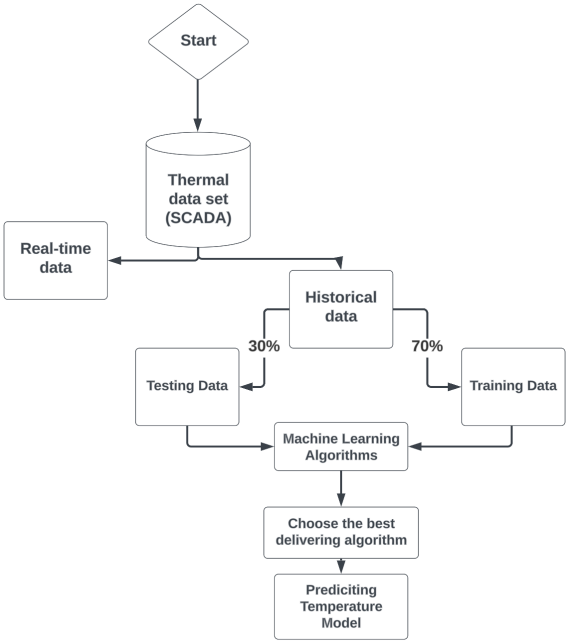

Figure 6: The flow chart of T-IDS's temperature predictor.

using a 7:3 ratio between the training and testing datasets. The following data analytical methods have been examined.

- *Linear Regression:* The linear regression algorithm predicts the target variable based on a linear equation: $y = a \cdot x + b$, where a is the slope of the linear model, and b is the intercept value of a dependent variable.
- *Random Forest:* The random forest algorithm is built based on different decision trees; its output is the mean of all the trees. This algorithm's strength is that it prevents overfitting by randomly selecting samples from the data set.
- *Gradient Boost:* The gradient Boost model produces the target variable by creating multiple weak models and combining previous models to improve the performance of later models. This

method's overall approach is to fit the new learner to the residuals of previous models to enhance the prediction. This machine-learning algorithm avoids overfitting by reducing the learning rate or tree constraints.

We have examined the above methods and chose the best one for T-IDS based on the resulting mean absolute error (MAE) between observed and predicted data. Figure 5 plots the MAEs when predicting temperature variables using different methods, showing that random forest achieves the highest accuracy when compared to others. As a result, random forest is adopted by T-IDS as the temperature predictor. Figure 6 shows the flowchart of T-IDS's temperature predictor.

3.3 Anomaly Detector

After completing the temperature predictor, T-IDS initiates its anomaly detection stage, which is the final step of the whole design. The phrase begins by generating the reference model with 70% of historical data to train the temperature predictor. T-IDS takes its corresponding set of predictors for each target variable to produce the predictions. As this wind turbine component has both observed and predicted values, T-IDS obtains a set of residuals by subtracting the predictions from the historical data.

These residuals' mean and standard deviation set up the upper and lower boundaries for the anomaly detection model. The predetermined safeguard is defined as β times of standard deviations away from the mean of residuals. T-IDS performs anomaly detection by comparing the set of real-time residuals with the established range for residuals. To obtain this real-time residual, T-IDS applies a similar approach of building a reference model with real-time data and predicted values instead. Then, the system treats any value outside this fixed range as an outlier or anomaly and keeps tracking the number of outliers with a counter. As consecutive anomalies exist, the counter increments with each anomaly detected. Otherwise, once a subsequent residual falls within the determined safe bound while its predecessors are anomaly values, the counter halves and retains only the integer part.

With a pre-defined threshold for outlier counter ϵ, once the counter surpasses this threshold, T-IDS triggers an alarm of detected anomaly. The flowchart of T-IDS's anomaly detector is shown in Figure 7.

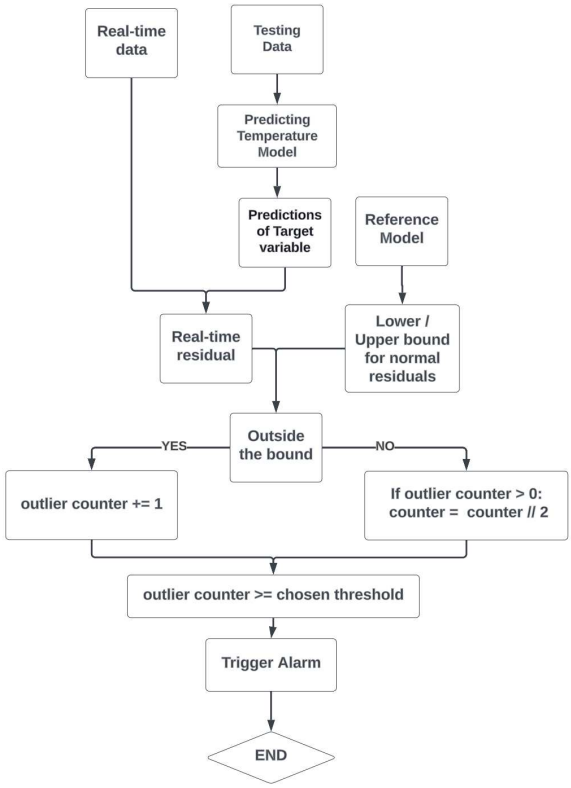

Figure 7: The flow chart of T-IDS's anomaly detector.

4 EVALUATION

Our evaluation of T-IDS was based on four critical factors: (i) the accuracy of its anomaly detection capabilities, (ii) the influence of different system settings on anomaly detector, (iii) its sensitivity to varying degrees of injected anomalies, and (iv) its performance across various anomaly-injected models.

4.1 Testing Methodology

We simulate abnormal/manipulated temperature readings by modifying the original (and normal) dataset based on two anomaly models.

- *Anomaly Model 1 (AM-1).* The first anomaly model is constructed by arbitrarily choosing an anomaly starting point χ within the range of index 0 to the length of the given data set, subtracting from the threshold value for anomaly counter *epsilon* and a random constant δ within the range of minimum and maximum values of the data set. AM-1 simulates anomalies as follows: from the chosen index χ, every variable is set to δ. This model represents the scenario in which the sensors are broken, or when intruders inject anomaly impacts, the observed values are equal to a constant value.
- *Anomaly Model 2 (AM-2).* As with the AM-1, The second anomaly model is initiated by randomly choosing an anomaly starting point. Then, beginning from this index, a random value σ within the range of $[-1, 1]$ is chosen, and the value of the current index fluctuates by multiplying a sum of 1, representing its current value, and σ. Many other sub-models can be constructed from AM-2 based on the range of σ. This study uses the testing methodology by separating the $[-1, 1]$ range into subsets with an interval of 0.1 for each. For instance, starting with a value of -1.0, the bound for choosing the value of σ is $[-1.0, -0.9)$, excluding the upper bound. As mentioned, there are many subcases for the second anomaly model, allowing for the assessment of T-IDS sensitivity in detecting anomalies with different levels of simulated data. These subcases represent scenarios where intruders attempt to inject noise into the SCADA system to uncover their actions.

Besides the two anomaly models introduced above, a positive false alarm model is applied in this study by setting the value of

Table 1: The false alarm rate vs. the bounds of residuals. The false alarm testing model has a correlation threshold value of 0.8, and the anomaly bound is set 3 standard deviations away.

Variable Name \ Outliers Threshold	5	6	7	8	9	10
Gear oil temperature (°C)	928	71	0	0	0	0
Rear bearing temperature (°C)	950	0	0	0	0	0
Stator temperature 1 (°C)	835	0	0	0	0	0
Generator bearing rear temperature (°C)	336	0	0	0	0	0
Rotor bearing temp (°C)	999	999	0	0	0	0
Front bearing temperature (°C)	425	0	0	0	0	0
Generator bearing front temperature (°C)	957	0	0	0	0	0
Nacelle temperature (°C)	0	0	0	0	0	0
Gear oil inlet temperature (°C)	720	0	0	0	0	0
Temp. top box (°C)	958	884	846	0	260	0
CPU temperature (°C)	915	17	0	0	0	0
Nacelle ambient temperature (°C)	958	898	898	682	664	0
Transformer cell temperature (°C)	993	437	0	0	0	0
Hub temperature (°C)	997	954	951	711	0	0

Table 2: The false alarm rate vs. the bounds of residuals. The false alarm testing model has a correlation threshold value of 0.8, and the consecutive outliers threshold is set at 10.

Variable Name \ STD Away	1	2	3
Gear oil temperature (°C)	193	0	0
Rear bearing temperature (°C)	0	0	0
Stator temperature 1 (°C)	0	0	0
Generator bearing rear temperature (°C)	0	0	0
Rotor bearing temp (°C)	0	0	0
Front bearing temperature (°C)	0	0	0
Generator bearing front temperature (°C)	0	0	0
Nacelle temperature (°C)	963	0	0
Gear oil inlet temperature (°C)	0	0	0
Temp. top box (°C)	882	0	0
CPU temperature (°C)	770	0	0
Nacelle ambient temperature (°C)	893	0	0
Transformer cell temperature (°C)	0	0	0
Hub temperature (°C)	963	664	0

σ to 0, illustrating that no anomaly is injected into the observed values.

T-IDS is evaluated against the 2021 Wind Turbine SCADA data set [2]. The set contains fifteen different thermal variables of the wind turbine, which are *CPU temperature*, *Front bearing temperature*, *Gear oil inlet temperature*, *Gear oil temperature*, *Generator bearing front temperature*, *Generator bearing rear temperature*, *Hub temperature*, *Nacelle ambient temperature*, *Nacelle temperature*, *Rear bearing temperature*, *Rotor bearing Temp*, *Stator temperature 1*, *Temp. Top box*, *Transformer cell temperature*, and *Transformer temperature*, with a total of 26,064 records.

To achieve the best observation, T-IDS is evaluated with 1,000 unique cases for each temperature variable.

4.2 Optimal Configuration

As the first step of the evaluation, significant attention is devoted to identifying T-IDS's optimal configuration. This comprises fine-tuning the system's settings to maximize its anomaly detection accuracy. Through evaluations and analysis, T-IDS employs its most effective configuration when the anomaly detection model has its safe range as three standard deviations away from the residuals mean. The anomaly alarm goes off when ten consecutive anomalies are detected, i.e., the setting of β and ϵ is 3 and 10, respectively. These configurations minimize the false detection.

T-IDS performs evaluations with correlation threshold values within the $[0.7, 0.9]$ range in the false alarm testing model. Each correlation value test against distinct test cases with the threshold for anomaly counter between 5 and 10. This testing model expects to produce the minimum number of detected anomaly cases as no anomaly is injected into the observed values. This study observes that T-IDS reduces the positive false detection rate as the value of the anomaly counter increases. Similar trends occur throughout various testing cases with a predetermined range of correlation thresholds. One of the evaluation cases displayed in Table 1 shows T-IDS reducing the false detection rate to 0% when anomaly counter values reach 9 or above.

T-IDS achieves accurate anomaly detection by establishing a range for outlier residual values. This range is defined by upper and lower bounds, which are set based on the standard deviation of the residuals set. As the standard deviation values increase, T-IDS can minimize the number of false positive detections. This approach improves anomaly detection accuracy and reduces the likelihood of false alarms. Table 2 shows the false detection rates of T-IDS, with upper and lower bounds for residuals set as 1,2 and 3 standard deviations away. Compared to the other two settings, once T-IDS's safe bound for residual values is within the range of 3 standard deviations, the false detection rate is reduced to 0. This conclusion is based on the evaluations of false alarm testing models with correlation threshold values in the range of $[0.7, 0.9]$ with 0.1 intervals.

4.3 Performance in Anomaly Detection

Next, we evaluate T-IDS's capability to detect anomalies in wind turbines. T-IDS achieves an almost 100% detection rate for anomalies injected according to the first anomaly model, as shown in Table 3.

T-IDS has demonstrated a remarkable ability to detect significant changes in observed values, as evidenced by its high anomaly detection rate with the first anomaly model. This highlights its robustness and effectiveness in detecting significant deviations from normal operating conditions. Furthermore, T-IDS has performed exceptionally well against the second anomaly model, particularly under conditions where a range of σ represents relatively small simulations, proving its ability to detect subtle anomalies precisely. Despite the challenges in defining minor deviations, T-IDS performs remarkably in recognizing anomalies even though the values of σ are within the range of $[0.01.0.1)$ or $[-0.1, -0.01)$. Table 4 and 5 shows the performance of T-IDS's anomaly detection.

Table 3: Results when evaluating T-IDS against the first anomaly model.

Variable Name \ Correlation Threshold	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95
Gear oil temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	999
Rear bearing temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Stator temperature 1 (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	988
Generator bearing rear temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	914
Rotor bearing temp (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	999	999	999	1000	1000	1000	1000	1000	N/A
Front bearing temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	991
Generator bearing front temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	998	N/A
Nacelle temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	999	999
Gear oil inlet temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	925
Temp. top box (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
CPU temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Nacelle ambient temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	999	999
Transformer cell temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	998	998
Hub temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	999	999	N/A	N/A
Transformer temperature (°C)	1000	1000	1000	1000	1000	1000	1000	999	999	997	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Table 4: Performance of T-IDS in anomaly detection through evaluations with the second anomaly model and range of σ is within $[0.01, 0.1)$.

Variable Name \ Correlation Threshold	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95
Gear oil temperature (°C)	979	979	979	979	979	978	989	989	989	989	988	988	988	988	988	980	981	981	742
Rear bearing temperature (°C)	995	995	995	995	986	983	983	983	973	979	979	979	979	982	975	975	975	934	942
Stator temperature 1 (°C)	917	917	917	917	910	910	906	906	906	902	892	892	892	915	875	875	847	816	358
Generator bearing rear temperature (°C)	789	789	789	789	789	789	789	785	774	774	774	697	697	697	697	630	550	551	0
Rotor bearing temp (°C)	940	940	940	940	940	940	940	940	940	935	861	861	861	727	727	658	524	496	N/A
Front bearing temperature (°C)	946	946	946	943	944	944	944	944	945	942	942	942	927	928	928	928	923	925	143
Generator bearing front temperature (°C)	801	801	810	810	810	810	749	749	749	749	731	731	731	731	731	731	748	219	N/A
Nacelle temperature (°C)	693	668	668	668	668	668	668	668	668	668	668	717	608	608	623	620	386	386	N/A
Gear oil inlet temperature (°C)	607	607	627	627	607	607	607	607	607	607	623	623	623	623	623	623	462	332	0
Temp. top box (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	998	998	997	997	993	966	966	N/A
CPU temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Nacelle ambient temperature (°C)	412	412	412	374	431	452	457	418	418	317	317	317	317	77	77	77	77	0	0
Transformer cell temperature (°C)	862	862	862	862	862	831	802	802	813	622	445	547	0	0	0	0	0	0	0
Hub temperature (°C)	794	794	794	794	794	794	762	762	737	694	659	641	641	406	406	576	0	N/A	N/A
Transformer temperature (°C)	633	328	241	241	241	206	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Moreover, as the range of σ becomes more significant, T-IDS exhibits enhanced anomaly detection capabilities. The system captures anomalies vividly because of the significant deviations from the predetermined normal range of residuals. For instance, as the range of σ shifts to [0.1 and 0.2), the average anomaly detection rate for all thermal variables in the wind turbine system is increased to 96.8%. T-IDS's overall anomaly detection rate with the second anomaly model is 97.6%. This observation underscores T-IDS's ability to adapt to varying magnitudes of anomalies and improve performance as anomaly detection rates become more pronounced. In addition to its outstanding performance, T-IDS also reveals a commendable ability to maintain a low rate of false alarms during the evaluations with the second anomaly model, as the value of σ is fixed to 0. Table 6 shows T-IDS's ability to minimize its false detection rate during evaluations. These observations show that T-IDS can exhibit a 0% false alarm rate with optimal settings. This aspect of T-IDS is crucial in ensuring the reliability and practicality of its anomaly detection framework by reducing the likelihood of unnecessary alerts to maintain a stable workflow.

5 CONCLUSIONS

The wind power industry is grappling with mounting security challenges, as wind turbine and SCADA systems are vulnerable to compromise and manipulation. To enhance intrusion detection in wind turbines, this paper presents T-IDS, a Thermal-Model-based Intrusion Detection System. T-IDS's system comprises three key components: a graph-based thermal model, a temperature predictor, and an anomaly detector. Extensive testing demonstrates T-IDS's remarkable capability of identifying anomalies in the thermal variables of wind turbines while maintaining a low false alarm.

ACKNOWLEDGMENTS

This work is supported by NSF under 2231759, 2245223, and 2245224.

Table 5: Performance of T-IDS in anomaly detection through evaluations with the second anomaly model and range of σ is within $[-0.1, -0.01)$.

Variable Name \ Correlation Threshold	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95
Gear oil temperature (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	980	1000	1000	893
Rear bearing temperature (°C)	999	999	999	999	998	997	997	997	997	997	1000	1000	997	1000	997	975	997	984	988
Stator temperature 1 (°C)	968	968	968	968	968	968	972	972	972	972	947	947	951	947	951	875	939	953	741
Generator bearing rear temperature (°C)	936	936	936	936	936	936	936	903	930	930	930	930	933	933	896	630	861	862	272
Rotor bearing temp (°C)	993	993	993	993	993	993	993	993	993	949	949	869	949	872	658	745	711	N/A	N/A
Front bearing temperature (°C)	991	991	991	991	991	991	991	991	991	990	990	990	987	990	987	928	974	976	582
Generator bearing front temperature (°C)	968	968	952	952	952	952	947	947	947	947	889	889	889	889	889	731	883	693	N/A
Nacelle temperature (°C)	762	784	784	784	784	784	784	784	784	784	784	612	753	670	626	624	531	531	N/A
Gear oil inlet temperature (°C)	712	712	709	709	709	715	715	715	715	715	697	697	697	697	697	623	610	363	0
Temp. top box (°C)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	287
CPU temperature (°C)	1000	748	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Nacelle ambient temperature (°C)	748	748	748	776	689	681	681	681	667	618	618	618	550	796	796	671	550	0	0
Transformer cell temperature (°C)	936	936	936	936	936	932	915	915	909	721	677	705	233	233	233	233	233	85	85
Hub temperature (°C)	960	960	960	960	960	960	906	906	896	892	889	887	891	887	853	576	891	N/A	N/A
Transformer temperature (°C)	809	599	490	490	490	380	317	243	51	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Table 6: The false alarm rate vs. the corresponding value of the outlier counter. False alarm testing model with a correlation threshold value of 0.8 and anomaly bound is set 3 standard deviations away.

Variable Name \ Correlation Threshold	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95
Gear oil temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rear bearing temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Stator temperature 1 (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Generator bearing rear temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rotor bearing temp (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	N/A
Front bearing temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Generator bearing front temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	N/A
Nacelle temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Gear oil inlet temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Temp. top box (°C)	388	388	388	388	388	388	388	388	388	388	388	0	0	0	0	0	0	0	0
CPU temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nacelle ambient temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Transformer cell temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hub temperature (°C)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	652	652	N/A	N/A
Transformer temperature (°C)	0	0	0	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

REFERENCES

[1] Love Allen Chijioke Ahakonye, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, and Dong-Seong Kim. 2023. SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. *Internet of Things* 21 (2023), 100676. https://doi.org/10.1016/j.iot.2022.100676

[2] Charlie Plumley. 2022. Kelmarsh wind farm data. (2022). https://doi.org/10.5281/zenodo.5841834.

[3] Bin Chen, Lei Xie, Yongzhan Li, and Baocheng Gao. 2020. Acoustical damage detection of wind turbine yaw system using Bayesian network. *Renewable Energy* 160 (2020), 1364–1372. https://doi.org/10.1016/j.renene.2020.07.062

[4] Colleen Glenn, Dane Sterbentz, and Aaron Wright. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. (????). https://doi.org/10.2172/1337873

[5] Jos Lelieveld, Andy Haines, Richard Burnett, Cathryn Tonne, Klaus Klingmüller, Thomas Münzel, and Andrea Pozzer. 2023. Air pollution deaths attributable to fossil fuels: observational and modelling study. *BMJ* 383 (11 2023), e077784. https://doi.org/10.1136/bmj-2023-077784

[6] Yirong Liu, Zidong Wu, and Xiaoli Wang. 2020. Research on Fault Diagnosis of Wind Turbine Based on SCADA Data. *IEEE Access* 8 (2020), 185557–185569. https://doi.org/10.1109/ACCESS.2020.3029435

[7] Eddie Yin-Kwee Ng and Jian Tiong Lim. 2022. Machine Learning on Fault Diagnosis in Wind Turbines. *Fluids* 7, 12 (2022). https://doi.org/10.3390/fluids7120371

[8] Jason Staggs, David Ferlemann, and Sujeet Shenoi. 2017. Wind farm security: attack surface, targets, scenarios and mitigation. *International Journal of Critical Infrastructure Protection* 17 (2017), 3–14. https://doi.org/10.1016/j.ijcip.2017.03.001

[9] Jason Staggs, David F. Ferraiolo, and Sujeet Shenoi. 2017. Wind farm security: attack surface, targets, scenarios and mitigation. *Int. J. Crit. Infrastructure Prot.* 17 (2017), 3–14. https://api.semanticscholar.org/CorpusID:4591946

[10] Wei Teng, Xian Ding, Shiyao Tang, Jin Xu, Bingshuai Shi, and Yibing Liu. 2021. Vibration Analysis for Fault Detection of Wind Turbine Drivetrains—A Comprehensive Investigation. *Sensors* 21, 5 (2021). https://doi.org/10.3390/s21051686

[11] Junshuai Yan, Yongqian Liu, and Xiaoying Ren. 2023. An Early Fault Detection Method for Wind Turbine Main Bearings Based on Self-Attention GRU Network and Binary Segmentation Changepoint Detection Algorithm. *Energies* 16, 10 (2023). https://doi.org/10.3390/en16104123

[12] Asal Zabetian-Hosseini, Ali Mehrizi-Sani, and Chen-Ching Liu. 2018. Cyberattack to Cyber-Physical Model of Wind Farm SCADA. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. 4929–4934. https://doi.org/10.1109/IECON.2018.8591200