Cyber Threat Analysis Framework for the Wind Energy Based Power System

Amarjit Datta and Mohammad Ashiqur Rahman
Department of Computer Science
Tennessee Technological University, USA
adatta42@students.tntech.edu,marahman@tntech.edu

ABSTRACT

Wind energy is one of the major sources of renewable energy. Countries around the world are increasingly deploying large wind farms that can generate a significant amount of clean energy. A wind farm consists of many turbines, often spread across a large geographical area. Modern wind turbines are equipped with meteorological sensors. The wind farm control center monitors the turbine sensors and adjusts the power generation parameters for optimal power production. The turbine sensors are prone to cyberattacks and with the evolving of large wind farms and their share in the power generation, it is crucial to analyze such potential cyber threats. In this paper, we present a formal framework to verify the impact of false data injection attack on the wind farm meteorological sensor measurements. The framework designs this verification as a maximization problem where the adversary's goal is to maximize the wind farm power production loss with its limited attack capability. Moreover, the adversary wants to remain stealthy to the wind farm bad data detection mechanism while it is launching its cyberattack on the turbine sensors. We evaluate the proposed framework for its threat analysis capability as well as its scalability by executing experiments on synthetic test cases.

CCS CONCEPTS

• **Security and privacy → Formal security models**; Distributed systems security; • **Networks** → *Sensor networks*;

KEYWORDS

Cyber-physical Systems; Wind Energy; Security; Formal Analysis.

1 INTRODUCTION

Wind energy is a popular and widely used renewable energy source. Many countries like China, Germany, the United States, the United Kingdom, and India have already deployed a large number of wind farms and are producing a significant amount of energy that feeds into the national grid [1]. In the last decades, we are observing a growing emphasis on green, renewable energy sources, leading to the increasing deployment of wind power infrastructures [2]. Wind energy is currently the second largest form of renewable energy generation source and its installed capacity is increasing more than any other renewable energy [3].

In a typical wind farm, there can be hundreds of wind turbines spread across a large geographical area. These turbines are often equipped with sensors, which measure important meteorological data like wind speed, wind direction, air pressure, and air density [4]. These measurements are important for the operation of the wind farm. The Wind Farm Control Center (WFCC) uses these meteorological data to optimally operate turbines. When the WFCC receives new sensor measurements, it validates the measurements using its Bad Data Detection (BDD) mechanism. Once the measurements are validated, they can be used to determine new power generation setpoints for the turbines.

The wind farm sensors and the data/control command transmission network are vulnerable to cyberattacks. Recent studies in power grids show that an intelligent adversary can alter the power-flow measurements in such a way that it can evade existing BDD algorithms and thus the attack remains undetected to the system operator. These attacks are widely known as Undetected False Data Injection (UFDI) attacks [5]. In a wind farm, an adversary can launch similar UFDI attacks by altering an intelligently selected set of sensor measurements, thus providing false meteorological data to the WFCC while evading the BDD process.

In this work, we propose a formal framework that can model potential UFDI attacks on the wind turbine meteorological sensors and analyze its impact on the wind farm power generation. More specifically, the framework considers an attack model, adversary attributes, and an attack objective and verifies potential UFDI attacks on a wind farm. The attack model mainly considers false data injection attacks on sensor measurements and the attack objective often specifies a maximum reduction in the power production. We also consider the presence of diverse loads and analyze the impact of UFDI attacks on their power consumption information. Our framework models the entire problem in a generic, broad form by considering it through a formal constraint satisfaction and optimization problem. Our framework is built using Satisfiability Modulo Theories (SMT), which is a powerful constraint satisfaction tool and can efficiently solve large complex problems with over thousands of variables [6]. We provide two example case studies to illustrate the execution of the proposed framework. We also evaluate the framework in terms of its threat analysis capability and its scalability.

The rest of this paper is organized as follows: In Section 2, we provide the necessary background. In Section 3, we present the problem definition, research objective, and our attack model. Formalization of the attack model is briefly discussed in Section 4. In

CPS-SPC'17, November 3, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-5394-6/17/11…$15.00
https://doi.org/10.1145/3140241.3140247

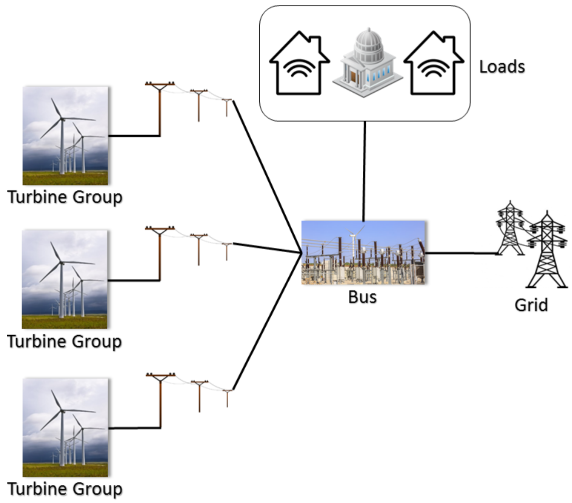


Figure 1: A wind farm in Microgrid environment.

Section 5, we describe two example case studies. The evaluation results are discussed in Section 6. We briefly discuss the related work in Section 7 and conclude in Section 8.

2 BACKGROUND

In this section, we provide the necessary background of the wind energy system. Here, we also discuss common sensors of the wind turbine, their purpose, and the wind farm BDD mechanism.

2.1 Wind Turbine Power Generation

A wind turbine converts kinetic energy of the wind to the mechanical energy by the rotation of the turbine blades and rotors. Then this mechanical energy is converted to electrical energy by the turbine generator. There can be multiple types of wind turbines. In the United States, three-blade, horizontal axis, variable speed, and pitch turbine are more popular. The amount of surface area available for the incoming wind is key to increasing aerodynamic forces on the rotor blades. To optimize the rotation of the blades, the turbine local controller can adjust the angle of the blade according to the direction of the wind. The angle at which the blade is adjusted is referred to as the angle of attack α [7]. The value of α is calculated based on the direction of the wind and the blade chord line. Proper balance between the rotational speed and the velocity of wind are critical for the optimal operation of the wind turbine. The balance between the rotational speed and the wind velocity is referred to as the tip speed ratio λ. The power coefficient of the turbine CP is a function of angle of attack α and the tip speed ratio λ.

We can formulate a three-blade, horizontal axis, variable speed, and pitch turbine power equation as follows [8]:

$$P = (\rho \times A \times v^3 \times CP \times CG \times CE)/2 \tag{1}$$

Here, parameter P represents the power generated by the wind turbine, ρ is the air density, A is the turbine swept area, v is the wind speed, CP is the turbine power coefficient, CG is the gearbox efficiency, and CE is the generator efficiency. From above discussion, it is apparent that the wind turbine power generation is directly related to the direction of the wind, wind velocity, and air density.

2.2 Wind Farm Architecture

Wind energy is a rapidly growing form of renewable energy in the United States. Wind turbines can be on-shore or off-shore. Similarly, they can be industrial (large wind turbines with high capacity) or privately owned. In this work, we only focus on industrial on-shore wind turbines. A wind farm is a collection of wind turbines in a given area. A wind farm can operate as a standalone energy generation source or can be integrated with the conventional power grid as an additional power source. We can observe the location of industrial wind farms, their power generation capability, and the number of turbines in the U.S. as of 2014 in [9]. From this work, we can observe that wind farms operate adjacent to each other in a given area. Within a wind farm, turbines are grouped based on their specification and their power generation capability. In a wind farm, turbines can be manufactured by various manufacturer. As a result, different turbines may have different power generation capability. Based on the specification of the turbines, surrounding area, location, environmental attributes (terrain, elevation), there can be multiple possible architecture of the wind farms. In this section, we present a generic, grid connected wind farm architecture.

Figure 1 presents an architecture of a grid-connected generic wind farm. In this wind farm, all turbines are grouped into multiple arrays, each producing and feeding power to the utility [10]. Wind turbines are connected with the wind farm substations through the collector bus. To control the operation of the wind farm, there are controllers. In a small wind farm, there can be a single controller. However, in a large wind farm, there can be more than one controllers, connected together in an hierarchical structure. In this framework, we consider WFCC as a generic control system of the wind farm that can monitor turbine operations and adjust turbine parameters. It can be a conventional Supervisory Control and Data Acquisition (SCADA) system or can be a customized proprietary controller. Modern wind turbines also have multiple on-board local controllers. These local controllers periodically monitor the turbine sensors and adjust the rotor speed, blade angle of attack according to the requirement established by the main controller (WFCC). Standard communication architecture may not be adequate for the wind farm since a wind farm may operate in a harsh terrain. To address the wind farm communication problem, IEC 61400-25 series of standards for communication technologies have been designed [11]. Different components in a turbine are connected with each other by Ethernet cables. Some wind farm installations also use wireless technologies to connect different components of the wind farm [12].

2.3 Wind Turbine Sensors

Modern wind turbines are equipped with multiple sensors. Sensors play an important role in the operation of a wind farm. WFCC and the turbine local controller use the sensor measurements to monitor turbine properties and identify any component failures. Based on the sensor measurement, the controller makes necessary decisions and configure parameters of the wind turbine for the optimal power generation. It is important to understand that not all the turbines are equipped with all types of sensors. Here we discuss some of the important types of sensors.

- **Wind speed sensors**: Wind speed sensors measure the velocity of the turbine surrounding wind. Generally, there can be more than one wind speed sensors in a turbine, installed at different heights to measure the wind speed from different elevation. In a small wind farm, there may not be any dedicated wind speed sensor. Such wind farms may gather wind speed information from the nearby adjacent wind farms or from some third-party online sources. Ultrasonic Anemometer [13], traditional cup-anemometers, wind vanes, Sodar (Sound Detection And Ranging), and Lidar (Light Detection and Ranging) are commonly used in the turbine/farm wind velocity measurement [14].
- **Temperature sensors**: Turbines may operate in a harsh environment. During the operation of a turbine, there can be mechanical failures which may generate abnormal heat. Sudden temperature change within a wind turbine can indicate major mechanical failure. The temperature sensor is used to detect any unusual temperature in the turbine.
- **Wind direction sensors**: This sensor is used to determine the direction of the wind. Ideally, a wind turbine nacelle and blades should rotate according to the direction of the wind. Direction sensor measurements are very important for WFCC to determine the optimal position of turbine blades and nacelle. Based on wind direction sensor measurement, a wind turbine can adjust its blades to maintain optimal angle-of-attack with the wind.
- **Air density sensor**: Air density sensor measures the air density of the turbine surrounding area. From Equation 1, we can observe that the power generation of the wind turbine is proportional with the air density of the environment. Based on the air density sensor measurement, the WFCC can compute the power generation curve of the wind turbine and adjust turbine parameters.

2.4 Bad Data Detection

In a cyber-physical system, BDD mechanism plays an important role. From previous discussion, we can observe that the operation of the wind farm heavily depends on the accurate measurement of it's sensors. Based on the sensor measurement, the WFCC and turbine's local controller can make important decisions and perform optimal adjustments on the turbine parameters.

Wind turbines operate at harsh environment. Most of the industrial wind turbine sensors are battery operated. Such sensors can malfunction anytime and generate inaccurate information. The wind farm control center collects sensor information from the turbine using cellular or wireless technology. During the transmission of the sensor measurements, sensor data can get corrupted due to network congestion. Finally, there can be cyberattacks, where an intelligent adversary can tap itself in the transmission path, create a communication bridge, and perform false-data-injection attack, denial-of-service, or impersonation attack. Due to all above possibilities, an efficient BDD mechanism is necessary for the reliable data acquisition of the wind farm. In the literature, we can find multiple BDD mechanisms suitable for the wind farm. Here, we discuss some of the generic BDD mechanisms.

- **Redundant sensors**: Wind turbine sensors can malfunction anytime due to its harsh operating condition. If a sensor stalls, it cannot transmit data to the controller. For such situation, modern wind turbines are often equipped with more than one redundant sensors for the measurement of the same parameters. When a sensor malfunction, another sensor can takeover its place. If more than one sensor is operating at the same time, WFCC can collect data from all sensors and validate the measurement.
- **Comparison with adjacent turbines**: In the wind farm, if there are more than one turbines and they are adjacent to each other, WFCC can use their sensor measurements for data validation. If the turbines are adjacent to each other, it is realistic to assume that the turbine will operate at similar meteorological environment (similar wind speed, air density, and wind direction). If the BDD identifies large difference between adjacent turbine meteorological sensor measurement, it can identify that there is a possible error in the data.
- **Data sharing between adjacent wind farms**: Adjacent wind farms can share their meteorological sensor information. Using this shared information, the wind farm controllers can validate the reliability of its sensor data and filter/identify anomalies.
- **Comparison with data from other weather services**: A wind farm control center can collect weather data from various sources. From multiple weather services, a wind farm can collect wind speed, air direction, and air density data and use the data to verify its locally collected sensor measurements. These data may not be 100% accurate, but may act as reference.
- **Historic weather data**: Wind farm can collect previous archived data of the wind farm surrounding area from various third-party or in-house sources and apply the data for verification purpose. If the new sensor data deviates too much from the previous data, it indicates an unusual situation and may raise flag for further investigation.

3 PROBLEM DEFINITION, RESEARCH OBJECTIVE, AND ATTACK MODEL

In this section, we briefly discuss the target problem along with our research objective, and proposed framework.

3.1 Problem Definition

Wind energy is prone to cyberattacks. In a large wind farm, different sensors are manufactured by different organizations. Most of the time, these sensors do not follow any standard security practice and they have limited computation ability. Some sensors may even have very limited embedded security and may use unencrypted passwords for communication [15]. When these sensors share data with the controllers, these transmission can be easily intercepted, and an intelligent attacker can easily modify their packets. If an adversary can intelligently choose its targets and smartly control its attack, it may easily deceive the wind farm's BDD mechanism and create disturbance. Sensor measurements are important for the optimal operation of the wind farm. Corrupted sensor measurements can inflict major damage to the wind farm's power production. However, deceiving the wind farm's BDD mechanism is not straight forward. An attacker cannot attack any turbine it wishes and the wind farm has multiple ways to verify its measurements. If an attacker has sufficient inside knowledge, it can launch this smart stealthy false data injection attack on the wind farm's meteorological sensors and inflict serious damage.

3.2 Research Objective and Challenges

There is great need to explore the possibility of UFDI attack on the wind farm's critical sensor measurements. In this work, we define a comprehensive framework for analyzing the impact of stealthy false data injection attacks on the wind power system. Our objectives are as follows:

- Our objective is to analyze the impact of stealthy false data injection attack on the wind farmâĂŹs critical sensor measurements. For this purpose, we need a comprehensive analysis framework that can model the stealthy attack on the wind farm by taking its parameters, power generation properties, and attack constraints as input and measure the impact.
- The primary objective of an adversary is to create a significant imbalance in the wind farm's power generation and make the system unstable. To remain stealthy throughout the attack, an adversary must intelligently balance the power equations and modify measurements.

In our framework, we consider realistic turbine properties, attack conditions, BDD mechanisms, and attack goals. Launching a UFDI attack on the wind farm is a multi-objective problem, where on one hand the adversary wants to reduce the power generation of the wind farm as much as possible and on the other hand the adversary has limited attack capability and must satisfy all defined constraints to evade the BDD mechanism. Such multi-objective problems are computationally expensive and considered as an NP-Complete.

3.3 Attack Model

Here we define UFDI attacks on the wind turbine in their most generic form, to allow the evaluation of the feasibility of the attacks under various scenarios. The attack attributes that represent the attack model are discussed in the following:

3.3.1 Adversary's Capability. An adversary may not have access to all the wind turbines in the wind farm. Some turbines may be located in a secure location. For some turbines, accessing the physical or remote terminal may be very difficult. For example, in order to launch a false data injection attack on a turbine, an adversary must have access to the turbine's remote terminal unit [16]. For this reason, we assume that an adversary has limited attack capability (can attack a limited number of turbines simultaneously). In our model, we also assume that some turbines are secured. There can be different types of cyberattacks. In this work, we only focus on UFDI attacks on the turbine meteorological sensors.

3.3.2 Group of Turbines. In a large wind farm, there can be many wind turbines scattered across a vast geographical area. From [17], we can observe that most of the wind farms in the U.S. are in central region. In the state of Iowa, South Dakota, Wisconsin, and Minnesota, there are total 260 wind farms. Different wind farms have different number of turbines. For example, the Federated Wind Farm in Minnesota have just one wind turbine. However, the Grant County Wind Farm has ten active wind turbines [17]. Some wind farms can be really big (more than hundreds of turbines). Based on the location of the turbine, their operation, and specification, turbines are grouped into multiple logical groups. The turbines of the same group are generally located close to each other. Within a group, all turbines operate at a similar meteorological condition.

In a large wind farm, we can group the turbines based on their locations. The turbines of the same group are geographically located close to each other. Within a group, all turbines operate at a similar meteorological condition. In the real world, it is reasonable to assume that adjacent locations operate at a very similar meteorological conditions (unless they are in different altitude or there is any severe weather). Let a and b be two turbines of group j. Their distance is $w_{a,b}$. If we measure their wind speed sensor values ($v_{a,j}$ and $v_{b,j}$) and calculate their difference, we can formulate their difference as a function of their distance $w_{a,b}$. We can define this logic using the equation below:

$$v_{a,j} - v_{b,j} \leq f(w_{a,b}) \quad (2)$$

Also in the wind farm, there can be more than one groups. Turbines of adjacent groups may have different meteorological values. However, since their locations are adjacent, if we calculate group average sensor value and compare with the adjacent groups, we can formulate their difference as a function of adjacent group distances. If there are two adjacent groups j and k, their distance is $q_{j,k}$, and their average wind speed sensor values are $\bar{v_j}$ and $\bar{v_k}$, we can define the adjacent group condition using the following equation:

$$\bar{v_j} - \bar{v_k} \leq f(q_{j,k}) \quad (3)$$

3.3.3 Attack on Loads. In a Microgrid environment, there can be loads connected with the bus (Fig 1). There can be different kinds of loads (residential buildings, offices, government buildings, and hospitals). The EMS collects power consumption information from the loads and uses the information to regulate the power generation of its generators (wind farm). Different loads consume a different amount of power. In this framework, we also consider the impact of UFDI attacks on the Microgrid loads [18]. Here, we discuss our load attack model:

- An intelligent attacker can launch UFDI attacks on the power consumption data of the loads.
- Some loads are secured (the communication channel between the load and the EMS is encrypted). An attacker can only attack power consumption data of the vulnerable loads and cannot attack secured loads.
- From the attack, the attacker can alter the power consumption data of the loads. The EMS produces power based on the power consumption data. If the power consumption report is forged, the EMS will set wrong power generation setpoint for the wind farm.
- If the Microgrid is main grid connected, it can get electricity directly from the main grid when the power production of the wind farm is not sufficient. However, the power production cost of the main grid is higher than that of the the wind farm. As a result, Microgrid always prefers to get electricity from its local wind farm than the main grid. In this framework, we do not consider any energy storage.

3.3.4 Bad Data Detection Approach. In any critical system, BDD mechanism plays an important role. BDD mechanism is used to filter unusual data from the input data stream. There are many sophisticated BDD mechanisms available in the literature. For this framework, we consider a comprehensive threshold based BDD mechanism that compares the measurements with predefined thresholds and identify possible anomalies. Here, we discuss two BDD mechanism thresholds that we use in this framework.

- **Turbine sensor measurement (TSM) thresholds**: For each type of sensor measurement, there is a separate measurement threshold. When the BDD mechanism receives new sensor measurements from the turbines, it compares the measurements with the other measurements of the same group (similar to Equation 2). For this comparison, BDD uses TSM threshold, which is a function of the distance between the turbines. If the sensor measurement difference is larger than the TSM threshold, it will indicate anomaly and the BDD will flag the turbine for inspection.
- **Adjacent group measurement (AGM) thresholds**: When the BDD mechanism receives new sensor measurements, it also calculates the group average for each type of sensor (separate average for wind speed, wind direction, and air density sensors). BDD then compares the group average with the group average of the adjacent groups (similar to Equation 3). For each pair of adjacent groups, there is a separate AGM threshold. The average sensor measurement difference of the adjacent groups must be less than this threshold. If the difference is more than the threshold, the BDD mechanism will identify the group measurement as unusual and flag it for further investigation.

3.3.5 Attack Constraints. To launch a successful UFDI attack, an adversary must satisfy the following conditions:

- An attacker cannot alter the sensor measurement values arbitrarily. The new sensor measurement value must satisfy the TSM and AGM thresholds.
- Some turbines can be secured. As a result, an adversary cannot attack every turbine of the wind farm. For each UFDI attack attempt, an adversary can attack a limited number of turbines simultaneously.
- From this attack, an adversary wants to inflict as much power generation change as possible in the wind farm. However, to remain undetected, the power generation change should not be more than a certain limit. If the power generation change is more than this limit, the BDD mechanism will detect the power change and take necessary actions.
- Similarly, an adversary wants to attack the turbines and change the power production of the wind farm to a significant level. For this purpose, we also define an attack margin (minimum target). If the power change is more than this margin, we consider the attack as significant.

3.3.6 Adversary's Target. An adversary wants to launch UFDI attacks on turbine sensors and reduce the wind farm power generation. An adversary's target is to inflict as much damage as possible to the wind farm power generation and remain stealthy.

Table 1: Modeling Parameters

Notation	Definition
n	The total number of turbines in the wind farm.
t	Types of turbines in the wind farm.
g	The total number of groups.
$group_j$	Group j of the wind farm.
$turbine_{i,j}$	Turbine i in group j.
$\bar{v}_j$	Average wind speed value of group j.
$\bar{d}_j$	Average wind direction value of group j.
$\bar{\rho}_j$	Average air density value of group j.
$v_{i,j}$	Wind speed value of $turbine_{i,j}$.
$d_{i,j}$	Wind direction value of $turbine_{i,j}$.
$\rho_{i,j}$	Air density value of $turbine_{i,j}$.

3.4 Contributions

Modern wind farms are equipped with a smart BDD mechanism. However, an intelligent adversary, with sufficient knowledge, can launch UFDI attacks on the wind farm and affect its power generation. Therefore, there is great need to explore the possibility of UFDI attacks on the wind farm meteorological sensors. In this work, we define a comprehensive framework for analyzing the impact of UFDI attacks on the wind energy management system. Our contributions are as follows:

- We present a *formal analysis framework* for analyzing the impacts of UFDI attacks on the wind farm meteorological sensor measurements and loads. In the framework, we consider different attack attributes, adversary's capabilities, and attack constraints. We also consider locations of the turbines and define a generic BDD mechanism.
- The primary objective of an adversary is to reduce the power generation of the wind farm. To remain stealthy, an adversary must deceive the BDD mechanism.

4 FORMAL MODEL OF CYBERATTACK ANALYSIS

In this section, we present the formal model of our proposed framework. In order to present our model, we need a number of parameters to denote the wind farm features, turbine properties, and attack attributes. We present some of the important parameters in Table 1. In this model, no multiplication of two parameters is performed without the multiplication sign.

4.1 Preliminaries

In a wind farm, there can be n turbines of t types. Based on the location of the turbines, we can divide the turbines into g groups. Parameter $group_j$ represents jth group. Parameter $turbine_{i,j}$ represents turbine i in group j. For $group_j$, its average wind speed, wind direction, and air density value can be represented by notation $\bar{v}_j$, $\bar{d}_j$, and $\bar{\rho}_j$, respectively. Parameters $v_{i,j}$, $d_{i,j}$, and $\rho_{i,j}$ represent the wind speed, wind direction, and air density sensor measurements of $turbine_{i,j}$. When the sensor measurements reach WFCC, each measurement is verified by the BDD mechanism. Once they are verified, they are applied to calibrate turbine power generation set points and parameters.

4.2 Turbine and Group Constraints

In a group, all turbines have similar meteorological sensor values. Let $turbine_{i,j}$ and $turbine_{l,j}$ be two turbines in $group_j$. Parameter $v_{i,j}$ and $v_{l,j}$ represent the wind speed sensor measurement value of $turbine_{i,j}$ and $turbine_{l,j}$, respectively. After the UFDI attack, the new wind speed sensor values of the turbines are $\hat{v}_{i,j}$ and $\hat{v}_{l,j}$. Let $\Delta v_{i,j}$ and $\Delta v_{i,j}$ represent the wind speed measurement change of $turbine_{i,j}$ and $turbine_{l,j}$ after a successful attack. Parameter $w_{i,l,j}$ represents the distance between $turbine_{i,j}$ and $turbine_{l,j}$ and parameter $CT_{v,j}$ is a constant that represents the change in wind speed per unit distance. If parameter $mv_{i,j}$ denotes whether the wind speed sensor of $turbine_{i,j}$ is compromised, based on Equation 2, we can represent the attack on wind speed sensor measurements using the following equations:

$$tv_{i,j} \rightarrow (v_{i,j} + \Delta v_{i,j}) - (v_{l,j} + \Delta v_{l,j}) \leq w_{i,l,j} \times CT_{v,j} \quad (4)$$

$$\forall_{1 \leq i,l \leq g_j}\ mv_{i,j} \rightarrow tv_{i,j} \wedge (\Delta v_{i,j} \neq 0) \wedge (\Delta v_{l,j} \neq 0) \quad (5)$$

Similarly, for wind direction sensor, if the parameter $d_{i,j}$ and $d_{l,j}$ represent the original sensor value and parameter $\Delta d_{i,j}$ and $\Delta d_{l,j}$ represent the change in the sensor value due to the UFDI attack then we can represent the turbine wind direction value difference using the equation below:

$$td_{i,j} \rightarrow ((d_{i,j} + \Delta d_{i,j}) - (d_{l,j} + \Delta d_{l,j})) \leq w_{i,l,j} \times CT_{d,j} \quad (6)$$

$$\forall_{1 \leq i,l \leq g_j}\ md_{i,j} \rightarrow td_{i,j} \wedge (\Delta d_{i,j} \neq 0) \wedge (\Delta d_{l,j} \neq 0) \quad (7)$$

Here, $CT_{d,j}$ is a constant that represents the change in the wind direction sensor measurement per unit distance. Parameter $md_{i,j}$ represents whether the wind direction sensor or $turbine_{i,j}$ is successfully attacked.

Finally for air density sensor measurement, if parameter $\rho_{i,j}$ and $\rho_{l,j}$ represent the original air density sensor measurement value of $turbine_{i,j}$ and $turbine_{l,j}$, parameter $\Delta\rho_{i,j}$ and $\Delta\rho_{l,j}$ represent the change in air density measurement due to UFDI attack, parameter $CT_{\rho,j}$ represents the air density change in per unit distance, and parameter $m\rho_{i,j}$ represents whether the air density sensor of $turbine_{i,j}$ is successfully attacked, then we can define the turbine air density value difference using the following equation:

$$t\rho_{i,j} \rightarrow ((\rho_{i,j} + \Delta\rho_{i,j}) - (\rho_{l,j} + \Delta\rho_{l,j})) \leq w_{i,l,j} \times CT_{\rho,j} \quad (8)$$

$$\forall_{1 \leq i \leq g_j}\ m\rho_{i,j} \rightarrow t\rho_{i,j} \wedge (\Delta\rho_{i,j} \neq 0) \wedge (\Delta\rho_{l,j} \neq 0) \quad (9)$$

If any of the condition $mv_{i,j}$, $md_{i,j}$, or $m\rho_{i,j}$ is true, we can consider that the attacker has successfully attacked $turbine_{i,j}$ sensor(s). Let parameter $mt_{i,j}$ represent whether the $turbine_{i,j}$ is successfully attacked. We can combine the turbine sensor measurement conditions and formalize them using following equation:

$$\forall_{1 \leq i \leq g_j}\ mt_{i,j} \rightarrow (mv_{i,j} \vee md_{i,j} \vee m\rho_{i,j}) \quad (10)$$

In our problem model, there is more than one group. The difference between the average sensor measurement values of the adjacent groups can be represented using the Adjacent Group Sensor Measurement threshold. Let us consider that there are two adjacent groups ($group_j$ and $group_k$). For $group_k$, let parameter $\bar{v}_k$, $\bar{d}_k$, and $\bar{\rho}_k$ denote the average wind speed, wind direction, and air density sensor measurement value. After the UFDI attack, let parameter $\Delta\bar{v}_k$, $\Delta\bar{d}_k$, and $\Delta\bar{\rho}_k$ represent the change in average wind speed, wind direction, and air density sensor value of $group_k$. According to the concept of adjacent groups, the difference between the new average sensor measurement values of $group_j$ and $group_k$ must be within the Adjacent Group Measurement Threshold. Let parameter $CG_{v,j,k}$, $CG_{d,j,k}$, and $CG_{\rho,j,k}$ denote the wind speed, wind direction, and air density AGM thresholds for $group_j$ and $group_k$. Parameter $q_{j,k}$ denotes the distance between $group_j$ and $group_k$ and parameter $\mathbb{K}$ denote the set of all turbine groups adjacent to $group_j$. If parameter gv_j, gd_j, and $g\rho_j$ are boolean variables that define whether the group average wind speed, wind direction, and air density values of $group_j$ satisfy the AGM thresholds, then we can formally define the conditions using the following equations:

$$av_{j,k} \rightarrow ((\bar{v}_k + \Delta\bar{v}_k) - (\bar{v}_j + \Delta\bar{v}_j)) \leq q_{j,k} \times CG_{v,j,k} \quad (11)$$

$$gv_j \rightarrow \forall_{k \in \mathbb{K}}\ av_{j,k} \wedge (\Delta\bar{v}_k \neq 0) \wedge (\Delta\bar{v}_j \neq 0) \quad (12)$$

$$ad_{j,k} \rightarrow ((\bar{d}_k + \Delta\bar{d}_k) - (\bar{d}_j + \Delta\bar{d}_j)) \leq q_{j,k} \times CG_{d,j,k} \quad (13)$$

$$gd_j \rightarrow \forall_{k \in \mathbb{K}}\ ad_{j,k} \wedge (\Delta\bar{d}_k \neq 0) \wedge (\Delta\bar{d}_j \neq 0) \quad (14)$$

$$a\rho_{j,k} \rightarrow ((\bar{\rho}_k + \Delta\bar{\rho}_k) - (\bar{\rho}_j + \Delta\bar{\rho}_j)) \leq q_{j,k} \times CG_{\rho,j,k} \quad (15)$$

$$g\rho_j \rightarrow \forall_{k \in \mathbb{K}}\ a\rho_{j,k} \wedge (\Delta\bar{\rho}_k \neq 0) \wedge (\Delta\bar{\rho}_j \neq 0) \quad (16)$$

If $\mathbb{J}$ is the set of all groups and mg_j is the combined condition variable for $group_j$, then we can formalize the combined group condition by combining the conditions in Equation 12, 14, and 16.

$$\forall_{j \in \mathbb{J}}\ mg_j \rightarrow gv_j \wedge gd_j \wedge g\rho_j \quad (17)$$

If Equation 10 and Equation 17 are satisfied, we can conclude that the attacker has successfully launched the UFDI attack on the wind farm.

4.3 Load Constraints

Let parameter sl_r denote whether the $load_r$ is secured. When the load is vulnerable, an attacker may launch UFDI attack on the load to change it's power consumption information. If PC_r is the original power consumption of $load_r$ and ΔPC_r is the change in power consumption due to UFDI attack, then we can formalize the load attack condition using the equation below:

$$yg_r \rightarrow \neg sl_r \wedge (\Delta PC_r \neq 0) \quad (18)$$

4.4 Attack in Power Production

As the wind turbine meteorological sensor values change, the power generation of the wind turbines also change. Let, $P_{i,j}$ be the original power generation value of $turbine_{i,j}$ and $\Delta P_{i,j}$ be the power generation change of the $turbine_{i,j}$ due to the UDFI attack. If the *minimum power generation change* threshold for $turbine_{i,j}$ is $MIN_{i,j}$ then the attacker must alter the sensor measurement values of the turbine in a way that the power generation change is greater than $MIN_{i,j}$. We can formalize this as follows:

$$\forall_{1 \leq i \leq g_j}\ \Delta P_{i,j} \geq MIN_{i,j} \quad (19)$$

If the value of the power generation change $\Delta P_{i,j}$ is less than $MIN_{i,j}$, there will not be any significant power loss on the $turbine_{i,j}$ due to the UFDI attack .

Similarly, the power generation change of the $turbine_{i,j}$ must be less than the *maximum power generation change* threshold $MAX_{i,j}$. If the change is more than the threshold, the WFCC will notice the unusual power difference and take necessary maintenance action.

$$\forall_{1 \leq i \leq g_j}\ \Delta P_{i,j} \leq MAX_{i,j} \quad (20)$$

Let, boolean $pt_{i,j}$ denote whether the power constraint of $turbine_{i,j}$ is met (the power change of the $turbine_{i,j}$ is at least the minimum and the maximum level). We can formalize the minimum and maximum power generation condition using the following equation:

$$\forall_{1 \leq i \leq g_j}\ pt_{i,j} \rightarrow MIN_{i,j} \leq \Delta P_{i,j} \leq MAX_{i,j} \tag{21}$$

Let, P_{total} represent the total generated power of the wind farm. Also, parameter $\hat{P}_{total}$ is the new total generated power of the wind farm due to the UFDI attacks. We can calculate the value of P_{total} and $\hat{P}_{total}$ using the following equations:

$$P_{total} = \sum_{i}^{n}(P_{i,j}) \tag{22}$$

$$\hat{P}_{total} = \sum_{i}^{n}(P_{i,j} + \Delta P_{i,j}) \tag{23}$$

If C_{power} is the wind farm's total *power generation threshold* then the attacker's target is to launch UFDI attacks on wind farm turbines in a way that the difference between $\hat{P}_{total}$ and P_{total} is greater than the threshold C_{power}. This can be represented as follows:

$$\hat{P}_{total} - P_{total} \geq C_{power} \tag{24}$$

If boolean parameter pf bdenotes whether the entire wind farm power generation change threshold is successfully met (the attack is significant enough), then using Equation 24 we can formalize the condition as follows:

$$pf \rightarrow (\hat{P}_{total} - P_{total}) \geq C_{power} \tag{25}$$

If we consider loads in the system, an attacker can launch UFDI attacks on vulnerable loads and alters their power consumption information. Let parameter $\hat{PC}_{total}$ is the new total power consumption requirement of loads in the system after UFDI attacks. Using the concept of power balance, we can formalize the power generation/consumption condition using following equation:

$$bc \rightarrow (\hat{P}_{total} + P_{grid}) - \hat{PC}_{total} = 0 \tag{26}$$

Here, P_{grid} is the power from the main grid and bc is a boolean that represents whether the power balance condition is satisfied.

4.5 Adversary's Capability

Constant $C_{capability}$ denotes the attack capability of the adversary. An adversary can attack $C_{capability}$ number of turbines simultaneously. Let parameter N_{attack} denote the total number of turbines successfully attacked by the adversary during a single UFDI attack attempt on the wind farm. The value of N_{attack} must be less than or equal to the value $C_{capability}$. If the boolean parameter mc denotes whether the capability constraint is met, then we can formalize the capability condition using the following equation:

$$mc \rightarrow (N_{attack} \leq C_{capability}) \tag{27}$$

4.6 Formalization of Attack Goal

Let ΔP_{total} be the total change in the power generation by the wind farm due to the UFDI attack. In our framework, the goal of the adversary is to maximize the value of ΔP^{total} while satisfying all the system constraints. We can define the combined conditions and formalize the attack goal using the following equation:

$$\begin{aligned} m_{goal} \rightarrow\ & MAX(\Delta P_{total}) \wedge \\ & \forall_{j \in \mathbb{J}}\ (\forall_{i \in \mathbb{I}_j}\ (mg_j \wedge mt_{i,j})) \end{aligned} \tag{28}$$

Table 2: Input of example scenario 1

Number of Turbines, Groups, and Types
20 5 3

Group, Air Density (kg/m^3), Wind Speed (m/sec), Wind Direction, Wind Speed Change Threshold(%), Wind Direction Change Threshold(%), and Air Density Change Threshold(%)
1 1.225 16.501 S 22 3 12
2 1.312 15.302 SW 21 4 11
3 1.214 14.432 SW 22 5 12
4 1.234 17.228 SE 23 3 13
5 1.322 12.322 S 21 4 11

Turbine, Group, Type, Swept Area (m^2), Secured, CP, Generator Efficiency, Gearbox Efficiency, Has Wind Speed Sensor?, Has Wind Direction Sensor?, and Has Air Density Sensor?
1 1 1 1256 0 0.35 0.75 0.95 1 1 1
2 2 2 700 1 0.37 0.74 0.91 0 0 0
3 3 3 1018 0 0.36 0.75 0.92 1 1 0
4 3 1 1256 1 0.38 0.73 0.95 1 0 0
5 4 1 1256 0 0.34 0.72 0.97 1 1 1
. . . .

Minimum Power Change(%) and Maximum Power Change(%)
5 10

Adversary's Capability(%)
20

Table 3: Input of example scenario 2

Number of loads ad types of load
20 3

Type, Secure, and Consumption (MW/h)
1 0 0.7
2 1 1
3 1 2

Load, Type
1 1
2 1
3 2
. . . .

Load Attack Capability(%)
20

5 EXAMPLE CASE STUDIES

In this section, we briefly discuss the implementation of the model and illustrate the model's execution with two example.

5.1 Implementation

To execute our model, we use SMT [6] to encode the formalizations presented in the previous section. In both example problems, we define a wind farm with 20 turbines and 5 groups. We analyze the impact of UFDI attacks on the wind farm meteorological sensors and measure power generation loss in Megawatt (MW). For both of the examples, we use realistic synthetic model data. We generated our wind farm model based on United States Geological Survey (USGS) wind farm data [19]. In the first example, we do not consider any load. In the second example, we consider a Microgrid environment. In this example, we consider that the Microgrid is operating in grid-connected mode, and it has local loads. For both of the examples, we consider exactly same wind farm setup (turbine properties and group formations). From Figure 2, we can observe the formation of groups in our synthetic wind farm example. We solved the examples using Microsoft Z3, an efficient SMT solver [20].

5.2 Example: Scenario 1

The complete input regarding the study is shown in Table 2. In this wind farm, there are three different types of wind turbines (manufactured by different manufacturer), each producing a different amount of power. Turbines are divided into groups based on their locations. We also assume that some turbines do not have all the sensors. For example, from Table 2, we can observe that turbine 1

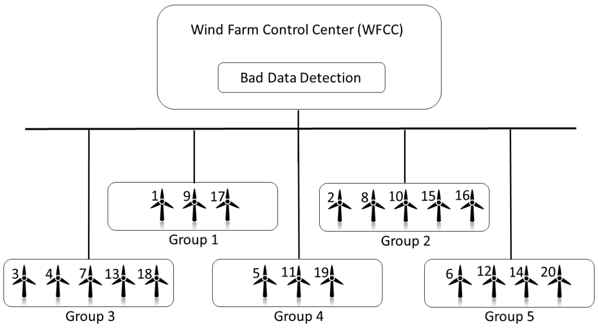


Figure 2: An example wind farm layout with 20 turbines.

has all the sensors and turbine 2 has no sensors. We also assume that some turbines are secured. An adversary cannot launch UFDI attack on a secured turbine. For example, from Table 2, we can observe that the turbine 1 is not secured and turbine 2 is secured. As a result, during cyberattack, an adversary may choose to attack turbine 1, but cannot attack turbine 2.

Our framework can identify many attack vectors of a given problem. However, we are only interested in attacks that generate significant impact. To filter high impact attacks from the low impact attacks, we use two power generation change margin. The first one is the minimum power generation change margin. In this example, the value of this margin is 5%, which means we only consider attacks which change the power generation of the wind farm to at least 5% of its original value. Similarly, the maximum power generation change margin is 10% of the original power generation value. We want to limit our attack within this maximum margin so that the change in power generation does not create suspicion to the grid operators. An adversary can attack a maximum 20% of the turbines simultaneously (except the secure turbines).

An adversary's objective is to launch UFDI attacks on the turbine sensors and reduce the total power generation. In order to remain undetected, an adversary must deceive the wind farm BDD mechanism by limiting the changes within the thresholds. With all above constraints, the execution of the model returns a *SAT* (Satisfiable) result, along with the assignments to different variables of the model. From the assignment, we find that:

- An adversary can launch a successful UFDI attack on the wind farm by attacking the turbines 6, 12, 14, and 20 of group 5. During this attack, the wind speed and the air density sensors of turbine 6 and 12 are attacked. Similarly, the wind speed and the wind direction sensors of turbine 14 and 20 are also attacked.
- The original power generation of the four turbines were 0.42MW, 0.56MW, 0.63MW, and 0.56MW, respectively. After the successful UFDI attack, the new power generation of the four turbines are 0.25MW, 0.47MW, 0.42MW, and 0.41MW.
- The new power generation of the wind farm is 10.615MW. The original power generation of the wind farm was 11.235MW. The total power generation change by the cyberattack is 0.62MW, which is a significant attack (between the minimum and maximum power generation change margin).

As the capability of an adversary increases, its capability to attack multiple turbines simultaneously also increases. In this example, if

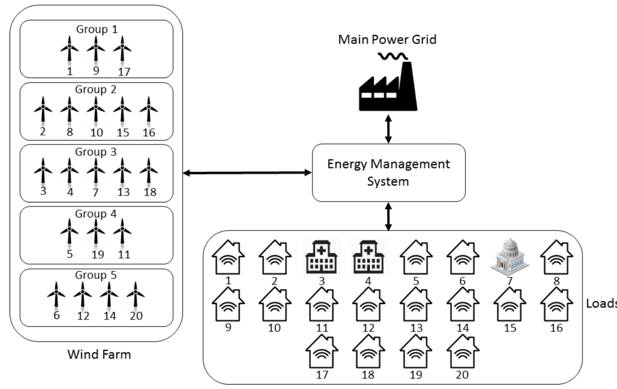


Figure 3: Example scenario 2v– WEMS with loads

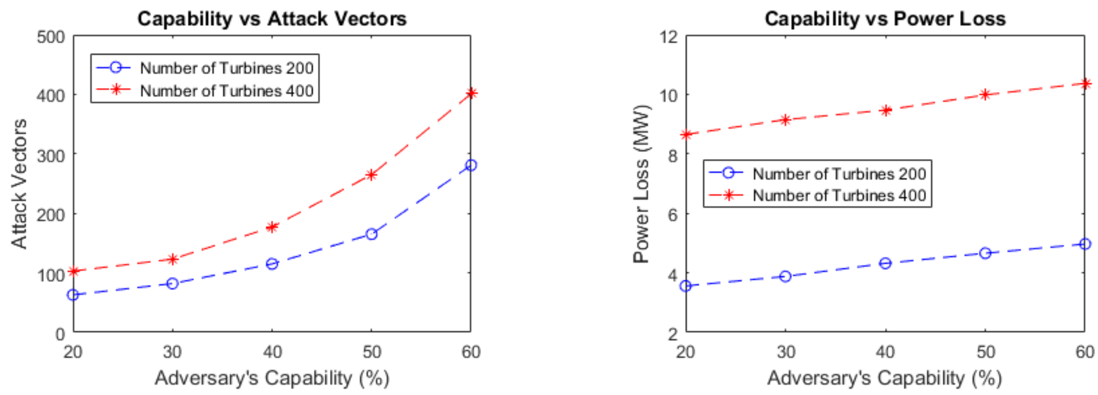
we increase the capability of an adversary to 30%, our framework again returns *SAT* result with the following variable assignments:

- A successful UFDI attack is launched in turbines 1, 5, 9, 11, 17, and 19 of group 1 and group 4. The wind speed and the air density sensors of turbine 1, 5, 11, and 17 are successfully attacked. Turbine 9 and 19 have no sensors.
- The original power generation of the turbines were 0.56MW, 0.63MW, 0.42MW, 0.56MW, 0.56MW, and 0.42MW, respectively. After the successful attack, the new power generation of the 6 turbines are 0.43MW, 0.51MW, 0.29MW, 0.42MW, 0.42MW, and 0.34MW, respectively.
- The new power generation of the wind farm is 10.495MW. The power generation loss of the wind farm due to UFDI attack is 0.74MW, which is more than the minimum margin and less than the maximum allowed limit.

It is interesting to see from this two scenarios that though there are many tight constraints, the adversary has still succeeded to launch a UFDI attack on the wind farm and successfully reduce the power generation. We can also observe that as the capability of an adversary increases, the total number of turbines an attacker can simultaneously attack also increases, and the power generation of the wind farm decreases.

5.3 Example: Scenario 2

In this example, we consider a Microgrid environment where different types of loads connected with the energy management system. Here, we consider a grid-connected Microgrid where the wind farm is the only local power generator. The wind farm turbine arrangement is same as example 1. The complete input of the example is the combination of Table 2 and Table 3. Here, we consider a typical power distribution scenario where the wind farm, loads (consumers), and the main power grid are connected with the Energy Management System (EMS) (Figure 3). We consider three types of load. Type one represents smart homes (average power consumption 700kW/h), type two represents hospitals (average power consumption 1MW/h), and type three represents government building (2MW/h). In this example, we consider that load type two (hospitals) and three (government buildings) are secured. An attacker can only attack load type one (smart homes). An attacker can launch UFDI attacks on the turbines and loads and alter the power generation/consumption measurements.



(a)

(b)

Figure 4: (a) The number of attack vectors with respect to the adversary's capability and (b) the wind farm power loss with respect to the adversary's capability.

To quantify the impact of UFDI attack, in this example, we consider a simple cost model. We make an assumption that the electricity produced by the wind farm is cheaper than the main grid. Based on this cost model, the EMS always prefer to buy electricity from its local wind farm over the main power grid. If the power production of the wind farm less than the consumption requirement (the total power consumption of all loads), the EMS buys the remaining electricity from the main grid. An adversary can simultaneously attack 20% of all turbines and 20% of all loads (except the secure turbines and loads). After formalizing all above constraint in SMT, the execution of the model returns a *SAT* result, along with following assignments to different variables:

- An adversary can launch UFDI attacks on wind turbine 6, 12, 14, and 20 of group 5. In the same attack, an adversary also altered the power consumption measurement of load 1, 2, 5, and 8.
- The original power generation of the four turbines were 0.42MW, 0.56MW, 0.63MW, and 0.56MW, respectively. After successful attack, the new power generation of the turbines are 0.26MW, 0.45MW, 0.43MW, and 0.4MW respectively. The new total power generation of the wind farm is 10.605MW. The total power generation change due to cyberattack is 0.63MW, which is more than the minimum power generation change limit and less than the maximum power generation change limit.
- The original power generation of the wind farm was 11.235MW. The original power requirement of all loads was 10MW. Based on this requirement, before the attack, the Microgrid was capable of producing enough power for its local load. However, after the UFDI attack, the new power requirement of the local loads is 11.2MW, which is more than the new power generation value of the wind farm (10.605MW). As a result, the Microgrid cannot generate enough electricity to support its entire load and force buy additional electricity from the main power grid. The total deficit electricity that the Microgrid buys from the main grid is 0.595MW. In this example, we do not consider any intermediate Energy Storage (ES). However, we can easily extend our case study to incorporate energy storage in the Microgrid system and analyze its impact.

From above analysis, it is visible that, a successful stealthy attack on the turbines and the loads can reduce the power generation of the wind farm and force the Microgrid to purchase electricity from the main grid.

6 EVALUATION

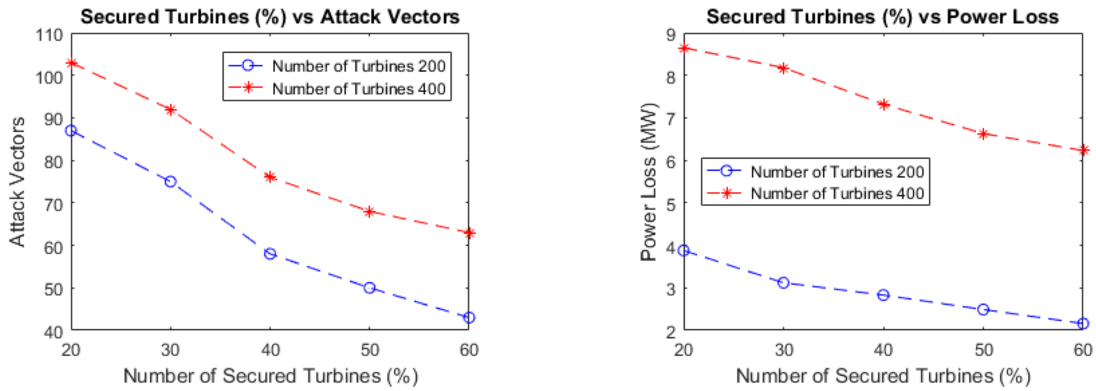
In this section, we conduct necessary experiments to evaluate our proposed framework with respect to different attack attributes and problem sizes.

6.1 Methodology

Here, we analyze the impact of UFDI attacks on the wind farm, with respect to attack capabilities, the number of secure turbines, and the number of turbines. We performed this analysis over two different wind farm sizes: 200 turbines and 400 turbines. In the scalability analysis, we analyze the execution time of our framework with respect to different attack capabilities, number of groups, and the size of the wind farm. We run our experiments on an Intel Core i7 Processor PC with 16 GB memory.

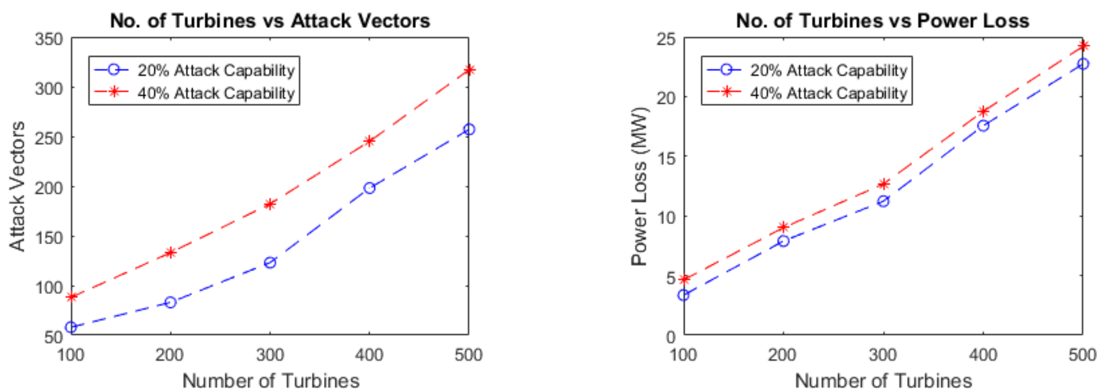
6.2 Threat Analysis

6.2.1 Impact of Adversary's Capability on Threat Analysis. As shown in Figure 4(a) and Figure 4(b), when an adversary's capability increases, the number of attack vectors and the wind farm power loss also increases. An attack vector is a solution found by our framework on the problem model that satisfies all the given constraints. From Figure 4(a), we can observe that the number of attack vectors generated by the wind farm of 400 turbines is significantly higher than that of the wind farm of 200 turbines. Since the wind farm of 400 turbines is a significantly larger problem model, our framework can generate more attack vectors compared to that of the wind farm of 200 turbines. From Figure 4(b), we can observe that as the adversary's capability increases, the power loss of the wind farm also increases. With more capability, an adversary can attack more turbines and further reduce the power generation.



(a) (b)

Figure 5: (a) The number of attack vectors with respect to the number of secured turbines and (b) the wind farm power loss with respect to the number of secured turbines.



(a) (b)

Figure 6: (a) The number of attack vectors with respect to the number of turbines and (b) the wind farm power loss with respect to the number of turbines.

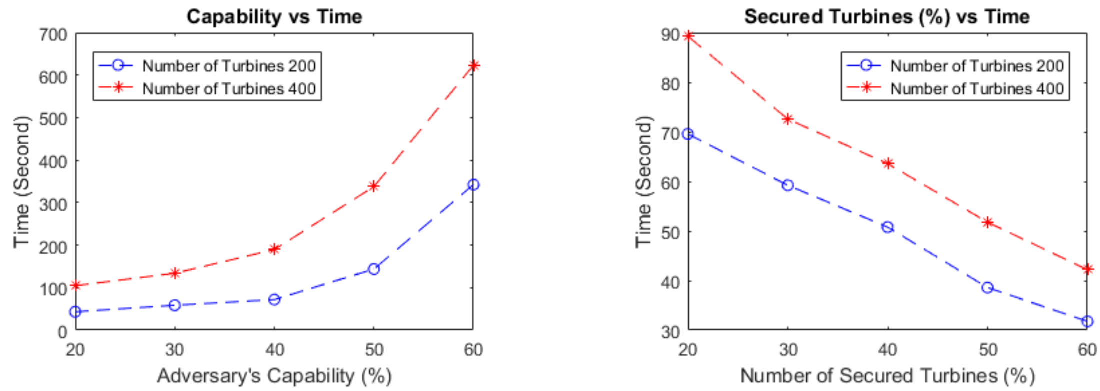
6.2.2 Impact of Security on Threat Analysis. From Figure 5(a), we can observe that as we increase the number of secure turbines (in percentage), the number of attack vectors identified by our framework decreases. When a turbine is secured, the attacker cannot attack the turbine. If the number of secured turbine increases, the attacker would have fewer alternatives to attack, and our framework identifies fewer attack vectors. Similarly from Figure 5(b), we can observe that, when the number of secure turbines increases, the total power loss of the wind farm also decreases. With less capability, the attacker cannot inflict great damage to wind farm's power production.

6.2.3 Impact of Number of Turbines on Threat Analysis. From Figure 6(a) and Figure 6(b), we observe the relationship between the number of attack vectors, the wind farm power loss, and the size of the wind farm. As the number of turbines increases, the size of the framework also increases. As a result, with the increase in number of turbines, our framework can find more attack vectors. Also in the figure, we observe that with higher capability, our framework can identify more attack vectors for the same problem size. Similarly from Figure 6(b), we observe that as the size of the wind farm increases, the total power loss of the wind farm also increases.

6.3 Scalability Analysis

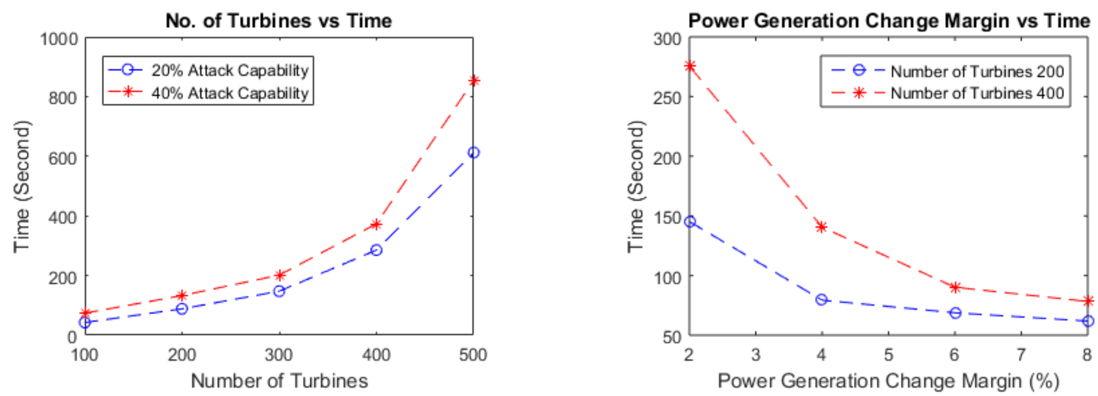
6.3.1 Impact of Adversary's Capability on Execution Time. From Figure 7(a), we can observe the execution time of our framework with respect to different capabilities. As the attackers capability increases, the number of attack vectors generated by our program also increases. As a result, the execution time of the program also increases. Also from the figure, we can observe that, the execution time of the 400 turbine wind farm problem is higher than the 200 turbine wind farm problem. This is logical, as the 400 turbine wind farm model is a significantly larger problem model than the 200 turbine model.

6.3.2 Impact of Number of Secured Turbines on Execution Time. We can observe the relationship between the framework execution time and the number of secured turbines (%) in Figure 7(b). As the percentage of secured turbines increases, the number of attack vectors found by our framework decreases. As a result, our framework requires less time to execute. From the figure, we can also observe that the execution time of the 400 turbine wind farm model is higher than the 200 turbine wind farm model. The 400 turbine wind farm model is a significantly larger problem model



(a) (b)

Figure 7: (a) The execution time with respect to the adversary's capability and (b) the execution time with respect to number of secured turbines.



(a) (b)

Figure 8: (a) The execution time with respect to the number of turbines and (b) execution time with respect to the power generation change margin.

than the 200 turbine model. As a result, our framework requires longer time to execute the 400 turbine model than that of the 200 turbine model.

6.3.3 Impact of Number of Turbines on Execution Time. Figure 8(a) shows the relationship between the execution time of our framework and the size of the wind farm. As the size of the wind farm increases, the problem model of our framework also increases. As a result, our framework requires more time to compute, generates larger number of attack vectors, and require longer time to finish execution. As a result, we can observe that as the number of turbines increases, the execution time of the program also increases. We can also observe that the execution time of the framework with 40% attack capability is larger than the execution time with 20% attack capability. With more attack capability, our framework can generates more attack vectors and requires longer time.

6.3.4 Impact of Power Generation Change Margin on Execution Time. Figure 8(b) shows the relationship between the execution time of our framework and the minimum power generation change margin. In this analysis, the maximum power generation change margin is fixed (always 10%). Also, the adversary has 20% attack capability and 20% of all turbines are secured. From the figure, we can observe that as the minimum power generation margin increases, the execution time of the framework for both 200 turbine problem and 400 turbine problem decreases. When the value of minimum power generation change margin is small, our framework can generate more attack vectors that can inflict significant impact. As a result, our framework requires more time to generate all the attack vectors. However, when the minimum power generation change margin is high, our framework cannot identify too many attack vectors that inflicts significant impact, hence our framework requires less time.

7 RELATED WORK

In a wind farm, monitoring the conditions of the turbines is always very challenging. Yongxiang et al. in [21], presented a remote large-scale, real-time, monitoring and controlling solution. Their proposed solution is applicable for large offshore wind farms. Zhang et al. [22] proposed a unified browser/server based monitoring solution of diverse wind turbines in a wind farm that can monitor the condition of the turbine using a single monitoring interface. Helsen et al. [23] proposed to use a big data analysis solution to monitor the condition of a wind turbine through long term log file monitoring. Monitoring solutions for turbines using power and performance curves are proposed in [24, 25]. Hussain et al. [26] proposed a fault resilient communication network infrastructure for real-time controlling and monitoring of the wind farm turbines and other components.

In [27], Bang et al. proposed a high-speed sensor array for performing shape estimation of the wind turbine at different dynamic loads. Popeanga et al. [12] proposed a wireless sensor network based monitoring solution for the wind farm to monitor the structure, behavior, and response to different components of a wind turbine under dynamic load. Worms et al. [28] proposed a solution to monitor the rotation and position of the wind turbine rotor blade using optically powered sensors. Wind turbines also operate at variable weather conditions and its components can fail anytime. Qiu et al. [29] proposed a model based BDD mechanism for wind turbine gearbox. Agarwal et al. [30] proposed a fuzzy inference system-based fault detection system (FTSFFDS) for structural health monitoring of the wind farm. Godwin et al. [31] presented a data intensive machine learning approach for detecting faults in wind turbine pitch control mechanism. In [32], Butler et al. presented a turbine performance monitoring solution by utilizing wind farm SCADA system data.

None of the above discusses the cyberattacks on the wind turbine meteorological sensors. In this work, we propose a formal framework to analyze the feasibility of UFDI attacks on the meteorological sensors, which is unique to the best of our knowledge. While it appears intuitive that an attack on the wind turbine sensors can compromise the overall wind farm power generation, we provide a systematic modeling framework to analyze such cyberattacks.

8 CONCLUSION

The meteorological sensors of the wind turbines are vulnerable to false data injection attacks. An adversary with sufficient knowledge, accessibility, and resources can successfully perform UFDI attacks on the wind farm, causing non-optimal generation of power. We propose an SMT-based formal framework to systematically investigate potential security threats, particularly the feasibility of UFDI attacks, on WEMS with respect to various attack attributes. We conduct necessary experiments to analyze the threats based on different factors and to evaluate the scalability of the model. In the future, we would like to expand our framework by considering other renewable energy sources.

ACKNOWLEDGEMENT

This work is supported by the National Science Foundation, USA, under Project CNS-1657302.

REFERENCES

[1] A. Koukal and M. H. Breitner. Offshore wind energy in emerging countries: A decision support system for the assessment of projects. In *47th Hawaii International Conference on System Sciences*, Jan 2014.

[2] Z. Chen and E. Spooner. Grid power quality with variable speed wind turbines. *IEEE Transactions on Energy Conversion*, Jun 2001.

[3] U.S. Energy Information Administration. U.s. energy information administration. monthly energy review: November 2014. https://www.eia.gov/totalenergy/data/monthly/index.php.

[4] Y. Wang and X. Ma. Optimal sensor selection for wind turbine condition monitoring using multivariate principal component analysis approach. In *Automation and Computing (ICAC), 2012.*

[5] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. CCS '09. ACM, 2009.

[6] Leonardo De Moura and Nikolaj Bjørner. Satisfiability modulo theories: An appetizer. In *Brazilian Symposium on Formal Methods*, pages 23–36. Springer.

[7] National Instruments. Wind turbine control methods. http://www.ni.com/white-paper/8189/en/.

[8] E. S. Abdin and W. Xu. Control design and dynamic performance analysis of a wind turbine-induction generator unit. *IEEE Transactions on Energy Conversion*, 2000.

[9] Jay E Diffendorfer, Louisa A Kramer, Zach H Ancona, and Christopher P Garrity. Onshore industrial wind turbine locations for the united states up to march 2014. *Scientific data*, 2:150060, 2015.

[10] Tamer A. Kawady and Ahmed M. Nahhas. Modeling issues of grid-integrated wind farms for power system stability studies. http://cdn.intechopen.com/pdfs-wm/43159.pdf.

[11] Qinyin Chen, Y. Hu, J. N. Davies, and P. Excell. Wind farm communication system research based on ethernet. In *Automatic Control and Artificial Intelligence (ACAI 2012), International Conference on*, March.

[12] C. Popeanga, R. Dobrescu, and N. Cristov. Smart monitoring and controlling of wind turbines farms based on wireless sensors networks. In *Systems and Computer Science (ICSCS)*, Aug 2012.

[13] W. Lihua and Y. Dawei. Study of anemometer for wind power generation. In *2014 International Conference on Mechatronics and Control (ICMC)*, pages 657–661, July 2014.

[14] Wind Energy Facts. Wind energy facts. https://www.wind-energy-the-facts.org/best-practice-for-accurate-wind-speed-measurements.html.

[15] Dark Reading. Hacking the wind. http://www.darkreading.com/vulnerabilities---threats/hacking-the-wind/d/d-id/1329453.

[16] O. VukoviÄĞ, K. C. Sou, G. DÃąn, and H. Sandberg. Network-layer protection schemes against stealth attacks on state estimators in power systems. In *Smart Grid Communications (SmartGridComm), 2011 IEEE*, Oct.

[17] OpenEI. Map of wind farms in us. http://en.openei.org/wiki/Map_of_Wind_Farms.

[18] M. A. Rahman, E. A. Shaer, and R. G. Kavasseri. Security threat analytics and countermeasure synthesis for power system state estimation. 2014.

[19] United States Geological Survey. Usgs - wind energy. https://energy.usgs.gov/OtherEnergy/WindEnergy.aspx.

[20] Leonardo De Moura and Nikolaj Bjørner. Z3: An efficient smt solver. Springer-Verlag, 2008.

[21] Y. Bai, Y. Hou, D. Fang, X. He, and C. Zhu. A remote real-time on-line monitoring and control system for large-scale wind farms. In *Electrical and Control Engineering (ICECE), 2010 International Conference on.*

[22] Baofeng Zhang, Zhiwei Li, and Gengxin Ji. Design of large-scale wind farm monitoring system based on b/s mode. In *International Conference on Computer Application and System Modeling (ICCASM 2010).*

[23] J. Helsen, G. D. Sitter, and P. J. Jordaens. Long-term monitoring of wind farms using big data approach. In *2016 IEEE Second International Conference on Big Data Computing Service and Applications.*

[24] E. Papatheou, N. Dervilis, A. E. Maguire, I. Antoniadou, and K. Worden. A performance monitoring approach for the novel lillgrund offshore wind farm. *IEEE Transactions on Industrial Electronics*, 62, 2015.

[25] A. Kusiak and A. Verma. Monitoring wind farms with performance curves. *IEEE Transactions on Sustainable Energy*, Jan 2013.

[26] S. Hussain and Y. C. Kim. Fault resilient communication network architecture for monitoring and control of wind power farms. In *2016 18th International Conference on Advanced Communication Technology.*

[27] H. j. Bang, S. w. Ko, M. s. Jang, and H. i. Kim. Shape estimation and health monitoring of wind turbine tower using a fbg sensor array. In *Instrumentation and Measurement Technology Conference*, May 2012.

[28] K. Worms, C. Klamouris, F. Wegh, and L. Meder. Lightning-safe monitoring of wind turbine rotor blades using optically powered sensors. In *Sensors and Measuring Systems 2014*, June 2014.

[29] Y. Qiu, J. Sun, M. Cao, H. Wang, Y. Feng, W. Yang, and D. Infield. Model based wind turbine gearbox fault detection on scada data. In *Renewable Power Generation Conference (RPG 2014), 3rd.*

[30] D. Agarwal and N. Kishor. A fuzzy inference-based fault detection scheme using adaptive thresholds for health monitoring of offshore wind-farms. *IEEE Sensors Journal*, 14(11):3851–3861, Nov 2014.

[31] Jamie L Godwin and Peter Matthews. Classification and detection of wind turbine pitch faults through scada data analysis. *IJPHM Special Issue on Wind Turbine PHM (Color)*, page 90, 2013.

[32] S. Butler, J. Ringwood, and F. O'Connor. Exploiting scada system data for wind turbine performance monitoring. In *2013 Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 389–394, Oct 2013.