2024 Doctoral Dissertation

Tamper Resistance and Anomaly Detection of Cyber-Physical Systems

Affiliation	Department of Mechanical Systems Engineering
	Graduate School of Engineering
	Nagoya University
Supervisor	Asai Toru Associate Professor
Student Number	482151013
Name	Xu Fangyuan

Abstract

A cyber-physical system (CPS) consists of physical devices and the embedded computer. The physical devices collect the data about the physical processes and send it to the embedded computer. The embedded computer is responsible for analyzing the data, performing computations, controlling the physical processes, and so on. Since CPSs are widely used in critical infrastructures to support the essential services of society, it is critical to ensure the resilience of the system. Here, resilience is the ability to withstand and recover from threats. Two of the most significant threats for CPSs are anomalies of devices and deliberate attacks. In this thesis, we propose a solution to improve the resilience of the CPSs, which consists of an anomaly detection framework and tamper-resistant control for a CPS.

We first propose a generalized anomaly detection framework that iterates sparse reconstruction and sequential measurement. The detection method can detect the anomalies exactly with a small number of measurements, which is expected to be applied to a variety of CPSs. Furthermore, we develop a termination condition for the iterative detection algorithm that allows the algorithm to terminate after a few iterations and locate the anomalies with guaranteed exactness. In this thesis, we present the applications of the detection framework in the case of there is no prior knowledge and there is prior knowledge, using the examples of network systems and demand response of smart grids, respectively. Simulation results demonstrate that the detection method can detect the anomalies exactly and efficiently.

Then, we propose a framework of tamper-resistant control for CPSs, which is resistant to physical attacks on the controller, such as stealing the entity or copying the code of the controller. The tamper-resistant controller stabilizes the system if the state is an element of a finite time-varying set; otherwise, it produces an incorrect value, where the measure of the time-varying set in the set of continuous states is zero. We design the time-varying set elaborately such that the union of the sets over time is a dense set. By using the property of a dense set, the attackers cannot obtain the information of the time-varying set by observing the signals of the system. Furthermore, since the measure of the time-varying set in the set of continuous states

is zero, without the information of the time-varying set, the probability of an attacker obtaining the information of the controller is theoretically zero. The tamper-resistant controller is realized by a neural network and time-varying quantization. Simulation results demonstrate the security and feasibility of the proposed controller.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Cyber-Physical Systems

Over the past decade, propelled by the rapid development of information and communication technologies, a new generation of systems, called *cyber-physical systems* (CPS), have become increasingly popular [1–8]. The term "cyber-physical systems" emerged in 2006, coined by Helen Gill at the National Science Foundation in the United States [9]. A CPS is the integration of computation and physical processes [10], and a typical framework of CPS is shown in Fig. 1-1, composed of physical devices and the embedded computer. The physical devices, such as sensors, collect the data about the physical processes and send it to the embedded computer. The embedded computer is responsible for analyzing the data, performing computations, controlling the physical processes, and so on [11]. Such seamless interaction with networks of physical and computational components is one of the most important properties of a CPS.

Examples of CPSs include industrial control systems, smart grids, healthcare systems, network systems, and intelligent transportation systems [12–21]. Here, two examples, the wireless sensor network system and the smart grid, are introduced.

1. Wireless sensor network system: A typical wireless sensor network system is shown in Fig. 1-2, which consists of a manager and sensor nodes [22]. Sensor nodes connect to others, and then form a network. These nodes collect environmental information, such as temperature and sound, and send their data through the network to other nodes or the network manager, where the data can be observed and analyzed. The manager is responsible for analyzing the data from the network, managing the nodes to maintain the operations of the network, and so on [22, 23]. Wireless sensor network systems can monitor and

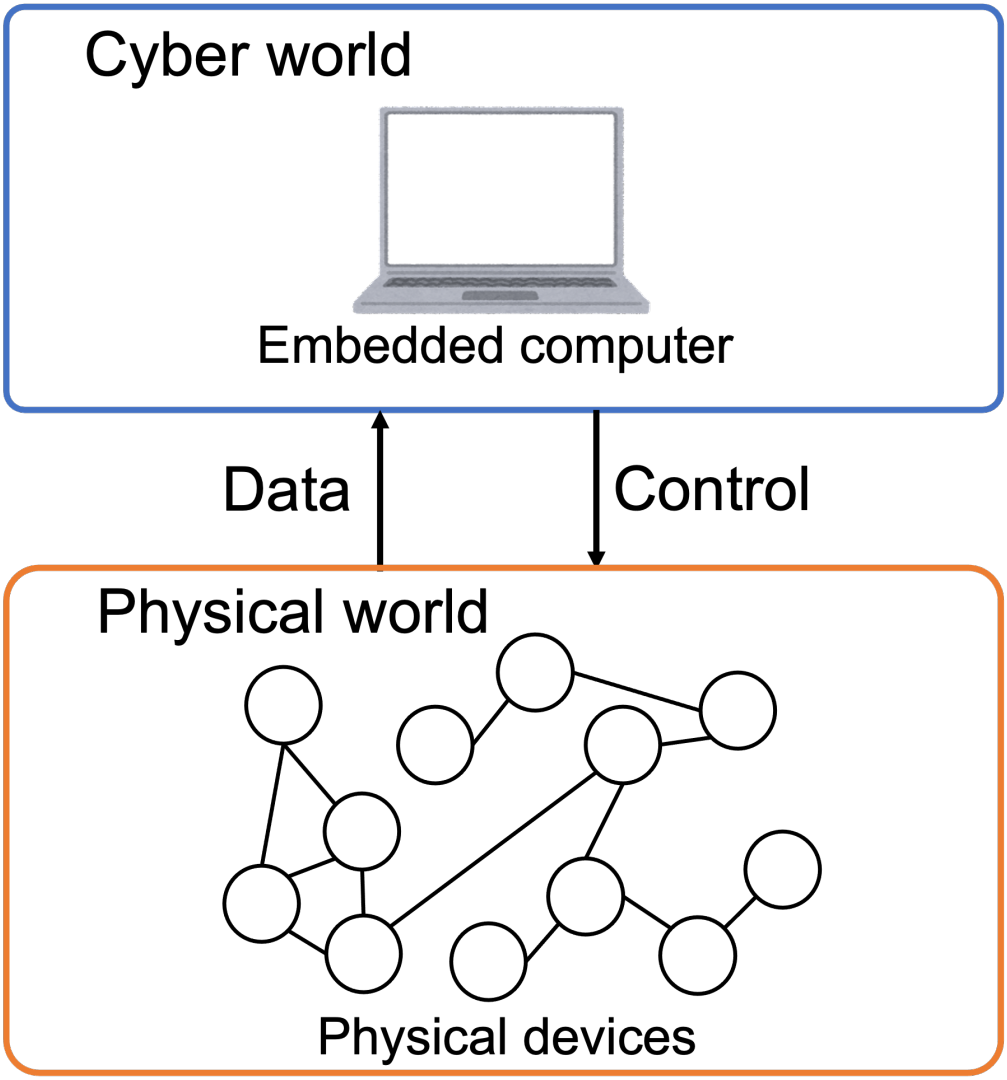


Figure 1-1: A framework of CPS.

control a physical environment and achieve specific goals, which are used in industrial process monitoring and control, agriculture, battlefield surveillance, and so on.

2. Smart grid: The smart grid is a new and improved power grid. It can flexibly adjust the power generation, transmission, and distribution or adjust the power consumption of the customers by collecting the power supply status of the supply side and the power usage status of the customer side. A framework of the smart grid is shown in Fig. 1-3, which incorporates power plants, energy storage and transmission facilities, renewable energy resources such as wind and power plants, customers, and so on. By using two-way flows of electricity

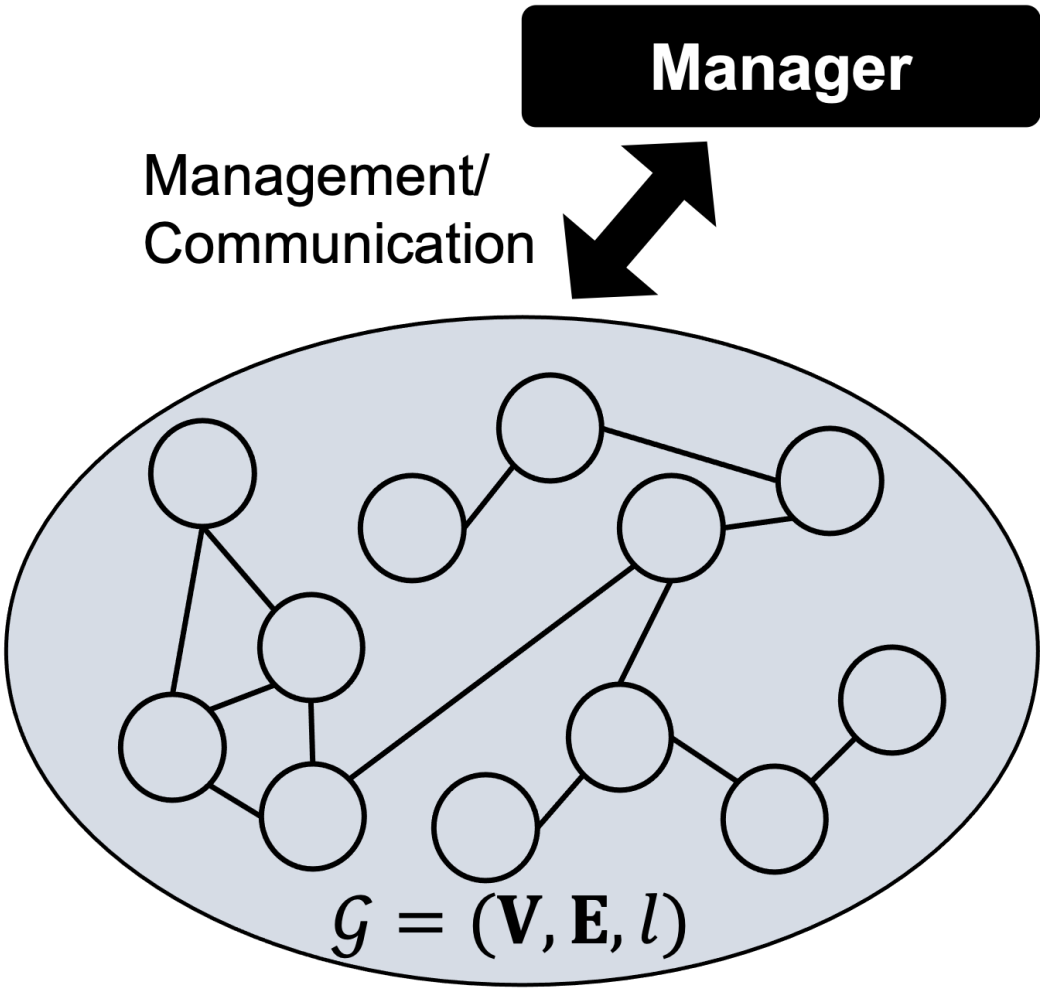


Figure 1-2: A wireless sensor network system.

and information, the smart grid provides better stability and improves energy efficiency than the traditional grid [15, 16].

Since CPS will not only provide the foundation of our critical infrastructure and improve our quality of life but also have the potential to impact various sectors of the world, it has attracted the attention of government, industry, and academia in the United States, Europe, and Japan [16, 24–26]. The National Intelligence Council foresees CPS as one of the six disruptive civil technologies with potential impacts on U.S. interests [24]. The European Commission has launched a research and innovation program in 2013, called Horizon 2020, which covers the research on CPS [25]. The Cabinet of Japan proposed the Society 5.0 strategy, and one of the key technologies to its realization is CPS [26].

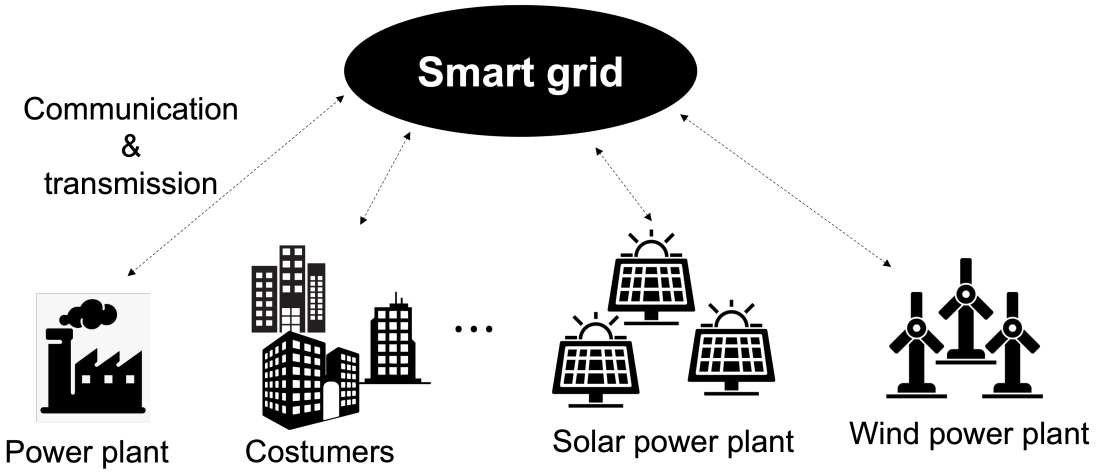


Figure 1-3: A framework of smart grid.

1.2 Resilience of CPSs

Since CPSs are integrated into our everyday lives and used in critical infrastructures to support the essential services of society, there is a greater need for their ability to perform their required functions under expected and unexpected adverse events [27]. This leads to the concept of *resilience*. Resilience is the ability to withstand and recover from threats [27–32]. Two of the most significant threats for CPSs are anomalies of devices and deliberate attacks [27, 33, 34]. Thus, in this thesis, we focus on enhancing the resilience of the CPSs by improving resistance to anomalies and deliberate attacks.

1.2.1 Anomaly Detection of CPSs

Due to the complexity of the physical world, there are inevitably some abnormal physical devices in CPSs [13]. For example, in wireless sensor networks, it is inevitable that some failures occur at the nodes, such as communication delays. Such anomalies may cause the partitioning of the network into various small segments and restrict the communication of the network [37, 38]. To ensure the resilience of the system, the embedded computer has to locate and subsequently repair it as soon as possible [35, 36, 39].

One of the solutions for anomaly detection in CPSs is given by machine learning techniques [36, 39–41]. In [36], an anomaly detection method based on a convolutional neural network is proposed. The method forecasts the behaviors of all devices and utilizes the difference between the predicted and actual behaviors for detection.

In [40], the researchers present an anomaly detection methodology based on semi-supervised machine learning and deep learning. In [41], a detection algorithm based on an echo state network is proposed. These methods can detect anomalies with a high accuracy. However, since these methods need to monitor all devices in real-time, for a large-scale CPS, such methods lead to significant communication and detection costs, which brings a challenge for practical use [42–44].

The technique of *sparse reconstruction* provides a promising solution to the detection problem. Sparse reconstruction is a signal processing technology aimed at recovering a sparse signal, i.e., a signal with only a few nonzero entries, from limited measurements by finding a solution to an underdetermined linear system [45–50]. It is usually applied to compressive sensing and image reconstruction, such as magnetic resonance imaging [51]. Meanwhile, since the anomalies also have sparsity, i.e., it is unlikely that numerous anomalies happen simultaneously, sparse reconstruction can also be applied to anomaly detection [52]. By constructing the measurements properly and using the technique of sparse reconstruction, the anomalies are expected to be located.

Several anomaly detection approaches for CPSs based on a special form of sparse reconstruction, called *group testing*, have been proposed [52–54]. Group testing is a detection method that divides the objects into several groups and identifies anomalies on groups rather than on individual ones [55–59]. It is expected to detect the anomalies without the need to measure all devices. Most existing methods construct the measurements based on some random matrices, such as Gaussian matrices [52–54]. They can not guarantee the exactness of anomaly detection, although the results demonstrate that the method can locate the anomalies with a high probability. On the other hand, a detection approach is proposed in [60]. It iterates sparse reconstruction and individual measurements, which can detect the anomalies with an exactness guarantee. However, there remain several challenges for practical application, such as the excessive number of individual measurements and the inability to handle the majority of realistic cases. Therefore, a generalized detection framework that can detect the anomalies exactly via limited measurements is required.

1.2.2 Tamper Resistance of CPSs

A CPS is vulnerable to attacks on both the physical and cyber sides with the intent of stealing sensitive information, such as the control law [15]. Such attacks could lead to the disclosure of commercial or military secrets, resulting in enormous economic losses and even national security issues. To ensure the resilience of the system, it is important to improve the resistance to attacks [61, 62]. Many studies have focused

on software-defined networking [62–64]. It is an approach that uses software-based controllers or application programming interfaces to communicate with devices and direct traffic on the network, which can prevent unauthorized access to the controller. However, these methods can not handle physical attacks on the controller, such as stealing the entity or copying the code of the controller.

In [65], a tamper-resistant controller is proposed. Here, the tamper resistance is the resistance to unauthorized access to the sensitive information of the controller [66]. The idea is that the tamper-resistant controller produces incorrect values in almost all states except for a predefined limited number of states. Because the measure of the predefined limited number of states in the set of continuous states is zero, without the information of the predefined states, the probability of an attacker obtaining the information of the controller is theoretically zero. The tamper-resistant controller is achieved by a neural network and time-invariant quantization. The controller outputs the correct values only when the states are correctly quantized. However, for a time-invariant quantization system, if the attacker observes the quantized states, the quantization information would be easily obtained since the observed signals are the elements of a finite set. Then, the controller would be vulnerable. Therefore, the tamper resistance of the controller needs to be improved.

1.2.3 Goal

Based on the above observations, we aim to enhance the resilience of the CPSs by improving the resistance to anomalies and deliberate attacks. More specifically, the goal of this thesis is to propose a generalized detection framework that can detect anomalies exactly via a small number of measurements and a framework of tamper-resistant control for CPSs.

1.3 Contribution

This thesis proposes a solution to enhance the resilience of the CPSs, as shown in Fig. 1-4, which consists of an anomaly detection framework and tamper-resistant control for a CPS. The contributions are summarized as follows.

1. Based on the idea of the method in [60], we propose a generalized detection framework that is the *sparse reconstruction based on sequential measurements*. More specifically, we utilize the sparsity of the anomalies and reduce the detection problem to the problem of solving the sparse unknowns from an underdetermined system of linear equations. However, it is well-known that there might

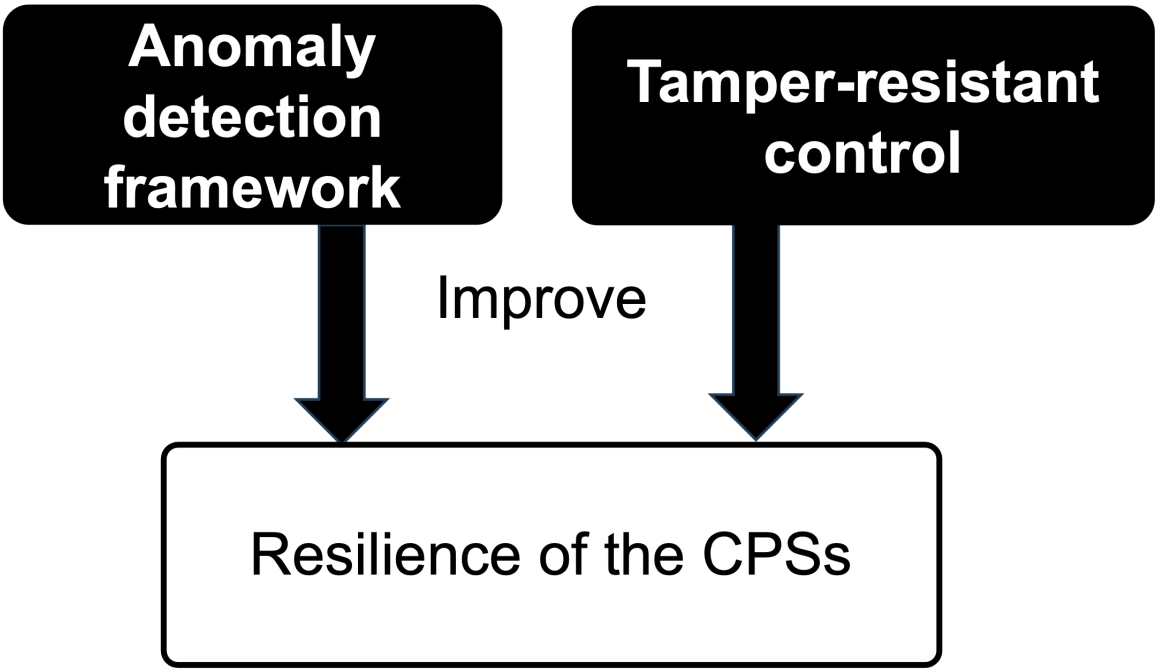


Figure 1-4: The proposed solution to improve the resilience of the CPSs.

be multiple solutions to an underdetermined system of linear equations, even if the sparsity of unknowns is considered. In other words, the information of the linear equations and the sparsity of unknowns is not sufficient for uniquely determining the unknowns. This prevents us from locating the anomalies exactly. Therefore, we incorporate several sequential measurements into the detection to complement the insufficient information and propose the detection framework of sparse reconstruction based on sequential measurements. In this thesis, we present the applications of the detection framework in the case of there is no prior knowledge and there is prior knowledge, using the examples of network systems and demand response of smart grids, respectively. Furthermore, we develop a termination condition for the iterative detection algorithm that allows the algorithm to terminate after a few sequential measurements and locate the anomalies with guaranteed exactness. Simulation results demonstrate that our proposed method can detect the anomalies exactly and efficiently.

2. We propose a framework of tamper-resistant control for CPSs, which can handle physical attacks on the controller, such as stealing the entity or copying the code of the controller. The tamper-resistant controller stabilizes the system if the state is an element of a finite time-varying set; otherwise, it produces an incorrect value, where the measure of the time-varying set in the set of

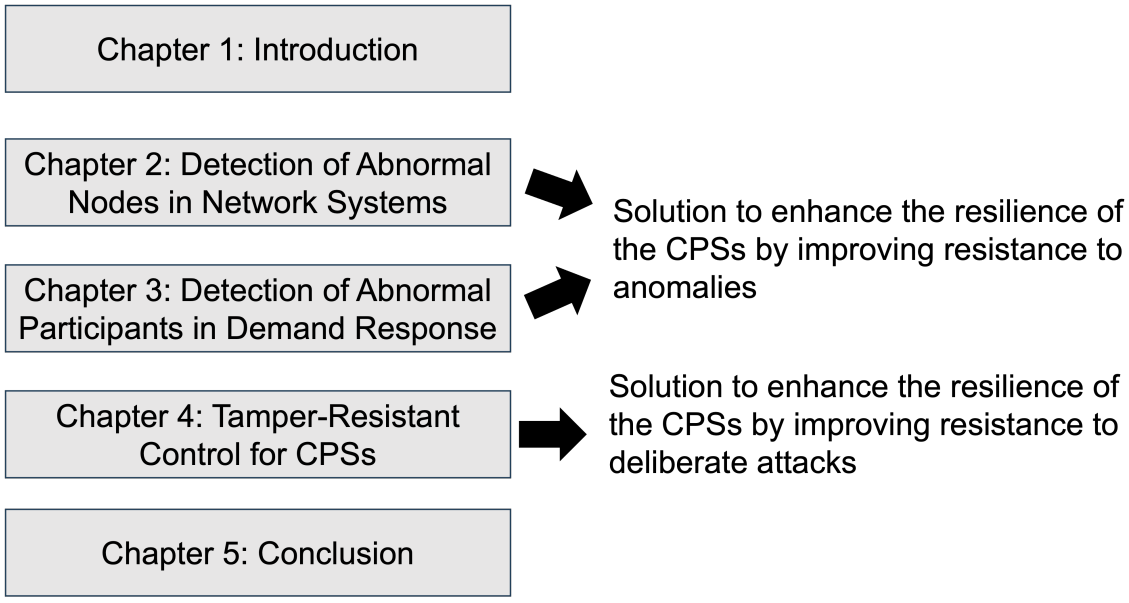


Figure 1-5: Structure of this thesis.

continuous states is zero. We design the time-varying set elaborately such that the union of the sets over time is a dense set. By using the property of a dense set, the attackers cannot obtain the information of the time-varying set by observing the signals of the system. Furthermore, since the measure of the time-varying set in the set of continuous states is zero, without the information of the time-varying set, the probability of an attacker obtaining the information of the controller is theoretically zero. The proposed controller is achieved based on a neural network and time-varying quantization. Our simulation results demonstrate the security and feasibility of the proposed controller.

1.4 Structure of the Thesis

The structure of this thesis is shown in Fig. 1-5. The rest of this thesis is organized as follows: Chapters 2 and 3 present the applications of the detection framework in the case of there is no prior knowledge and there is prior knowledge, using the examples of network systems and demand response of smart grids, respectively. In Chapter 4, we detail the tamper-resistant controller. Finally, the conclusion is presented in Chapter 5.

We next introduce some notations that will be used.

Notation: Let $\mathbf{R}$ be the set of real numbers, and let $\mathbf{R}_+$ denote the set of all positive real numbers. Let $\mathbf{N}$ and $\mathbf{Z}_+$ denote the set of natural numbers and the set of positive

integers, respectively. Let $\|x\|_p$ denote the ℓ_p-norm of the vector x. Note that $\|x\|_0$ is equal to the number of the nonzero elements of x. We use $|\mathbf{P}|$ to denote the cardinality of the set $\mathbf{P}$. Let $\lfloor x \rfloor$ and $\lceil x \rceil$ denote the floor and ceiling of a real number x, respectively. The former is the greatest integer less than or equal to x, and the latter is the least integer greater than or equal to x.

Chapter 2

Detection of Abnormal Nodes in Network Systems

In this chapter, we introduce the detection of abnormal nodes in network systems, which is partially based on our work in [67].

2.1 Introduction

A typical network system is composed of a manager and nodes, as shown in Fig. 1-2. The nodes communicate with others over the links [68]. The network manager is responsible for analyzing the data from the network, managing the nodes to maintain the stable operation of the network, and so on [22, 23].

One of the most common and serious problems in a network is node failure [69]. Once there is an abnormal node, the manager has to locate and recover it as soon as possible to sustain the stable operation of the network [23, 42, 69–72]. For anomaly detection in networks, one might consider that it can be easily achieved by monitoring and measuring the status of all nodes. However, such an approach leads to significant communication and detection costs [43, 44]. Therefore, it is advisable to detect the abnormal nodes with only a few measurements.

Group testing provides a promising solution for the diagnosis of the abnormal nodes in networks. Its idea is to divide the nodes into several groups and identify abnormal nodes on groups rather than on individual ones [55–59]. Group testing is performed by following three steps: (a) The manager specifies several simple paths that are sequences of distinct adjacent nodes in the network. (b) The manager sends the test signals, such as timestamp signals, called probes, along the paths and measures the sum of faults, such as delay, over the paths. (c) The manager locates the

abnormal nodes based on the measurement results of the probes. Several anomaly detection approaches based on the technique of group testing have been proposed, for which the paths of probes are randomly constructed [52–54]. Although the results demonstrate that the manager can locate the abnormal nodes with a high probability by using such probes, it is important to note that they are not guaranteed to achieve an exact detection.

Motivated by the above observations, we aim to propose a method that can detect the abnormal nodes exactly via a small number of measurements for networks. By using the technique of sparse reconstruction, we propose the group testing based on the *binary correlation construction* probes [73–77]. Furthermore, we analyze the performance limitation of the group testing [67]. Our analysis finds that the manager can detect abnormal nodes exactly via a small number of measurements using group testing. However, we also find that the construction approach is not applicable to all networks due to the restriction of network topology. On the other hand, the exactness of detection relies on the assumption that the maximum number of abnormal nodes is known prior. However, it is not realistic. Therefore, based on the idea of incorporating individual measurements into detection in [60], we propose a detection method based on group testing and sequential measurements.

The rest of this chapter is organized as follows: Section 2.2 formulates the anomaly detection problem in networks. Section 2.3 introduces preliminaries on graph theory and group testing. Section 2.4 proposes the group testing based on the binary correlation construction probes and analyzes its performance limitation. Section 2.5 proposes the detection method based on group testing and sequential measurements. Finally, the performance of the proposed method is evaluated by simulation in Section 2.6.

2.2 Anomaly Detection Problem in Networks

Consider a network system as exemplified in Fig. 1-2, composed of a manager and nodes. The network is modeled as an undirected graph $\mathcal{G} = (\mathbf{V}, \mathbf{E}, l)$, where $\mathbf{V} = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes, $\mathbf{E} \subseteq \mathbf{V} \times \mathbf{V}$ is the set of links, and $l : \mathbf{V} \to [0, \infty)$ is a function defining the labels of nodes. We use $l(v_j)$ to denote the label of node v_j, and it represents the *anomaly status* (e.g., delay time and packet losses) at the node. Then, $l(v_j) \neq 0$ means there is an anomaly at node v_j, and $l(v_j) = 0$ means there is no anomaly. A node with a nonzero label is called an *abnormal node*.

To locate abnormal nodes, the network manager can send probes along any several simple paths in the network and measure the anomaly status of the nodes in paths. Assume that the manager specifies m paths and calls them path $1, 2, \ldots, m$. By

letting $\mathbf{P}_i \subseteq \{v_1, v_2, \ldots, v_n\}$ denote the set of the nodes in path i ($i = 1, 2, \ldots, m$), the *measurement* for the probe along path i is defined as

$$y_i = \sum_{v_j \in \mathbf{P}_i} l(v_j). \tag{2.1}$$

In other words, the measurement $y_i \in [0, \infty)$ denotes the sum of the labels of the nodes in path i. If there is at least one abnormal node in path i, we have $y_i > 0$; otherwise, $y_i = 0$. Then, the detection problem is to detect the abnormal node exactly via a small number of probes.

2.3 Preliminaries on Graph Theory and Group Testing

In this section, preliminaries on graph theory and group testing are introduced [56, 78–80].

2.3.1 Graph Theory

Consider an undirected graph $\mathcal{G} = (\mathbf{V}, \mathbf{E})$. The *degree* of a node is the number of links with the node as an end-point. By letting δ_j be the degree of the node $v_j \in \mathbf{V}$, the minimum degree of the nodes in $\mathcal{G}$ is defined as

$$\delta(\mathcal{G}) = \min_{j \in \{1,2,\ldots,n\}} \delta_j.$$

For example, consider the graph $\mathcal{G}$ in Fig. 2-1. The degree of the node v_1 is $\delta_1 = 2$. The minimum degree of the nodes in $\mathcal{G}$ is $\delta(\mathcal{G}) = 1$.

A *simple path* denotes a sequence of distinct adjacent nodes in a graph. A *Hamiltonian path* is defined as a path that visits each node of a graph exactly once. A *random walk* on a graph is a process that begins at a node, and at each time step selects an adjacent node of the present node and moves to the selected node. For example, for the graph in Fig. 2-1, path 1 is a simple path and a Hamiltonian path of $\mathcal{G}$.

Then, we introduce the notion of *induced subgraph*. Consider a set of nodes in $\mathcal{G}$, denoted by $\mathbf{T} \subseteq \mathbf{V}$. The subgraph of $\mathcal{G}$ induced by the set $\mathbf{T}$ is the graph that has $\mathbf{T}$ as its set of nodes and contains all the links of $\mathcal{G}$ that have both endpoints in $\mathbf{T}$. The induced subgraph is denoted by $\mathcal{G}_{\mathbf{T}}$. For example, Fig. 2-2 shows the subgraph of the graph in Fig. 2-1 induced by $\mathbf{T} = \{v_2, v_3, v_4, v_5\}$.

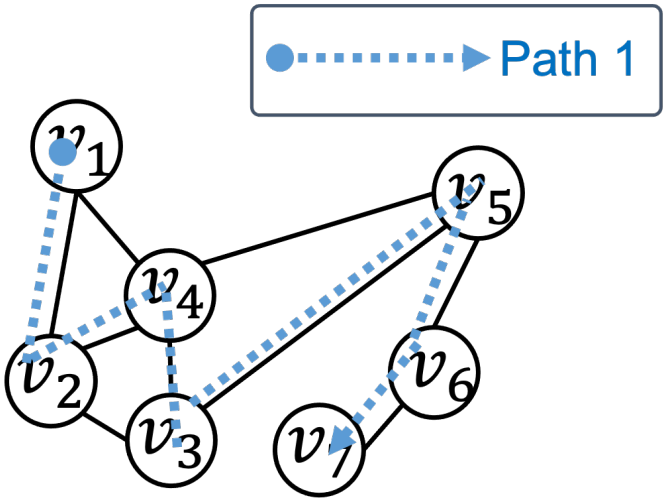


Figure 2-1: Graph $\mathcal{G}$.

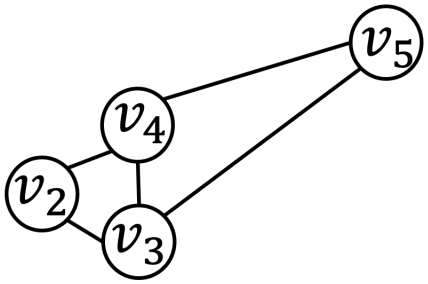


Figure 2-2: An induced subgraph of graph $\mathcal{G}$.

2.3.2 Group Testing

Group testing is a method that is expected to detect abnormal nodes with a small number of probes. Group testing on a network consists of three steps: (a) choosing several simple paths for probes, (b) sending probes along the paths to measure the anomalies over the paths, and (c) locating the abnormal nodes based on the measurement results of probes. The method is described in detail as follows.

Consider a network $\mathcal{G} = (\mathbf{V}, \mathbf{E})$ with n nodes. First, the manager chooses m simple paths in the network. Next, the manager sends probes along each path to measure the anomaly status of the nodes in paths. By sending the m probes, from (2.1), we obtain the measurement results $y_1, y_2, \ldots, y_m$. Then, by letting $y := [\ y_1 \quad y_2 \quad \cdots \quad y_m\ ]^\top \in [0, \infty)^m$, we have

$$y = Cx, \tag{2.2}$$

where $x := [\ l(v_1) \quad l(v_2) \quad \cdots \quad l(v_n)\ ]^\top \in [0, \infty)^n$ is called the *anomaly status vector*,

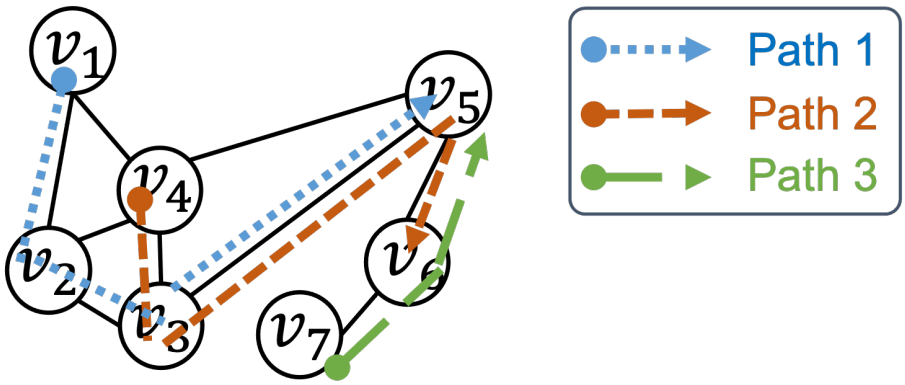


Figure 2-3: Anomaly detection by using group testing.

and $C \in \{0,1\}^{m \times n}$ is called the *measurement matrix*, whose (i,j)-th element c_{ij} represents whether v_j is in path i or not, i.e.,

$$c_{ij} = \begin{cases} 1 & v_j \in \mathbf{P}_i, \\ 0 & v_j \notin \mathbf{P}_i. \end{cases}$$

For example, consider the network in Fig. 2-3, and assume the manager chooses three paths, for which $\mathbf{P}_1 = \{v_1, v_2, v_3, v_5\}$, $\mathbf{P}_2 = \{v_3, v_4, v_5, v_6\}$, and $\mathbf{P}_3 = \{v_5, v_6, v_7\}$. Then, the measurement matrix is given by

$$C = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \tag{2.3}$$

In (2.2), the matrix C and the vector y are known to the manager, and the anomaly status vector x is unknown to the manager. Then, the group testing can find the abnormal nodes by solving the linear equation in (2.2) with respect to the unknown anomaly status vector $x \in [0,\infty)^n$.

2.4 Group Testing Based on the Binary Correlation Matrix and Its Performance Limitation

In this section, we propose the group testing based on the binary correlation matrix and analyze its performance limitation.

2.4.1 Group Testing Based on the Binary Correlation Matrix

As introduced in Section 2.3.2, group testing can detect the abnormal nodes by solving the linear equation in (2.2) with respect to the unknown $x \in [0, \infty)^n$. However, the number of probes is generally less than the number of nodes in group testing, i.e., $m < n$ in (2.2). It implies that there might be an infinite number of solutions of (2.2), preventing the manager from uniquely determining x.

On the other hand, it is reasonable to assume that there are only a few abnormal nodes, i.e., x has a few nonzero elements. Assume that there are at most f abnormal nodes in the network, i.e., x has at most f nonzero elements, then the vector x is called an *f-sparse* vector. By letting $\mathbf{S}(f)$ denote the set of f-sparse vectors in $\mathbf{R}^n$, if the manager can uniquely determine x on $\mathbf{S}(f)$, the abnormal nodes in the network can be located. Then, the notion of f-identifiability for the measurement matrix C gives a solution for exact detection by using group testing:

Definition 1 (f-identifiable matrix) *Consider the linear equation in* (2.2). *The matrix $C \in \mathbf{R}^{m \times n}$ is said to be f-identifiable if* (2.2) *has a unique solution on* $\mathbf{S}(f)$. □

If the manager can construct an f-identifiable measurement matrix C, the abnormal nodes can be detected. A promising method for constructing an f-identifiable matrix is given by the binary correlation matrices [73–77].

Definition 2 (Binary correlation matrix) *Consider a matrix $C \in \{0,1\}^{m \times n}$, let $c_i \in \{0,1\}^m$ denote the i-th column vector of C. The matrix C is called a binary correlation matrix if $c_i^\top c_j \leq 1$ holds for every $(i,j) \in \{1,2,...,n\}^2$ such that $i \neq j$.* □

For example, the following matrix $C \in \{0,1\}^{4 \times 5}$ is a binary correlation matrix:

$$C = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{2.4}$$

There is a sufficient condition for a binary correlation matrix to be f-identifiable [81].

Lemma 1 *Consider a binary correlation matrix $C \in \{0,1\}^{m \times n}$ and an $f \in \mathbf{N}$. Define $d(C) := \min_{i \in \{1,2,...,n\}} \|c_i\|_2$. If*

$$d(C) > f, \tag{2.5}$$

then the matrix C is f-identifiable. □

Then, we propose employing a binary correlation matrix satisfying (2.5) as the measurement matrix of group testing. Such a matrix can be constructed by the progressive edge-growth algorithm in [76, 77].

2.4.2 Performance Limitation of the Group Testing

In this section, we analyze the performance limitation of the group testing based on the binary correlation measurement matrix. The performance of the method corresponds to the number of probes for exact detection. We first define the performance limitation of the group testing and then propose our results.

Definition of Performance Limitation

Let $\mathbf{G}(n)$ denote the set of the networks with n nodes. Consider a network $\mathcal{G} \in \mathbf{G}(n)$. Assume that there are at most f abnormal nodes in $\mathcal{G}$. Let $\mathbf{C}(\mathcal{G}, f)$ denote the set of all feasible binary correlation measurement matrices of $\mathcal{G}$ satisfying (2.5). Let $m(C)$ denote the number of probes when employing the measurement matrix C. In other words, $m(C)$ is the row size of the matrix C. Then, the *performance index* of the group testing is defined as the minimum number of probes required for network $\mathcal{G}$:

$$m(\mathcal{G}, f) := \min_{C \in \mathbf{C}(\mathcal{G}, f)} m(C). \tag{2.6}$$

The *performance limitation* of the group testing is defined as the minimum number of probes required for the networks in $\mathbf{G}(n)$ that is given by

$$m^*(n, f) := \min_{\mathcal{G} \in \mathbf{G}(n)} m(\mathcal{G}, f). \tag{2.7}$$

By letting $\mathcal{G}^*$ be the optimal solution to the minimization problem in (2.7), then $m^*(n, f)$ is the minimum number of probes required for network $\mathcal{G}^*$.

Next, we aim to address the following problem:

Problem 1 *Consider the networks in the set $\mathbf{G}(n)$, and assume that there are at most f abnormal nodes in each network in $\mathbf{G}(n)$.*

1. *Derive $m^*(n, f)$.*
2. *Find $\mathcal{G}^*$.*
3. *Find an f-identifiable measurement matrix $C \in \{0, 1\}^{m^*(n,f) \times n}$ for network $\mathcal{G}^*$.*

□

Analysis Results of the Performance Limitation

A solution to Problem 1 is given as follows.

Theorem 1 *Consider the networks in* $\mathbf{G}(n)$*, and assume that there are at most* f *abnormal nodes in each network in* $\mathbf{G}(n)$*. Let*

$$m^- = \left\lceil \sqrt{(f+1)nf + \frac{1}{4}} + \frac{1}{2} \right\rceil, \tag{2.8}$$

$$m^+ = \left\lceil (f+1)\sqrt{nf + \frac{1}{4}} + \frac{1}{2}(f+1) \right\rceil. \tag{2.9}$$

1. *The relation*

$$m^- \leq m^*(n,f) \leq m^+ \tag{2.10}$$

holds. If there is a binary correlation matrix $C \in \{0,1\}^{m^- \times n}$ *with* $d(C) = f+1$*, then* $m^*(n,f) = m^-$*, i.e.,* m^- *is a solution to 1 of Problem 1.*

2. *Consider a network* $\mathcal{G} \in \mathbf{G}(n)$*. If*

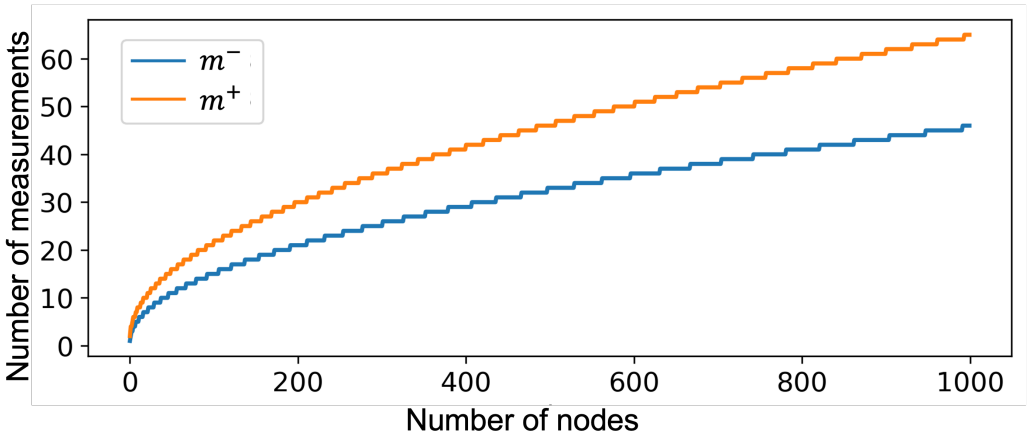
$$\delta(\mathcal{G}) \geq n - \frac{1}{2}\left\lfloor \frac{(f+1)n}{m^+} \right\rfloor, \tag{2.11}$$

then $\mathcal{G}$ *is a solution to 2 of Problem 1.*

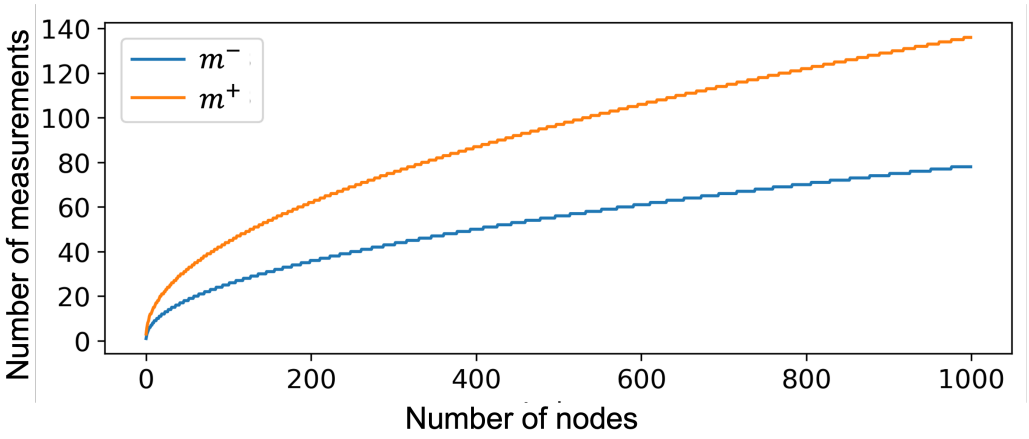
3. *Let* $\mathcal{G}^*$ *be a network satisfying* (2.11)*. A binary correlation measurement matrix* $C \in \{0,1\}^{m^*(n,f)\times n}$ *with* $d(C) = f+1$ *is a solution to 3 of Problem 1.*

Proof of Theorem 1: See Appendix A. ■

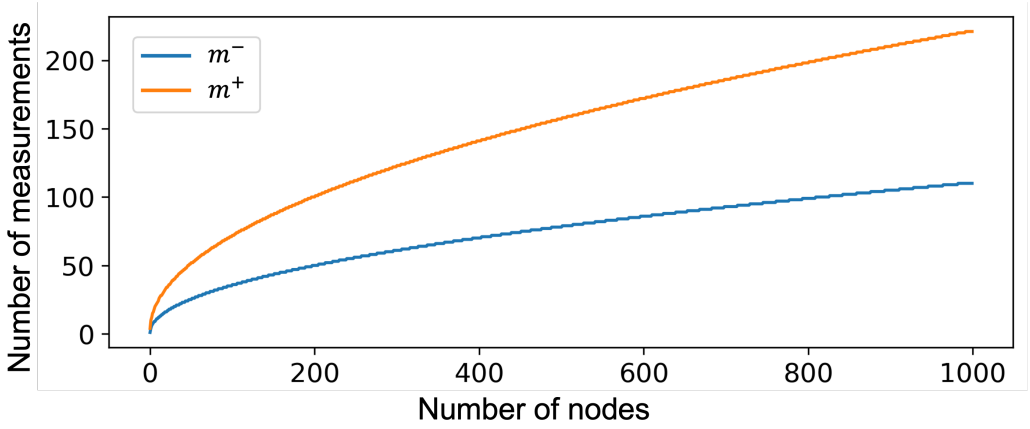
Theorem 1.1 provides the performance limitation of the proposed method and derives the upper and lower bounds of the minimum number of probes required for anomaly detection. Fig. 2-4 shows the upper and lower bounds in the cases of $f \in \{1,2,3\}$. Theorem 1.2 provides a sufficient condition of network topology, under which an f-identifiable measurement matrix with the minimum number of probes can be constructed for the network. For example, consider the case of $n = 30$ and $f = 1$, Fig. 2-5 shows a network $\mathcal{G}$ satisfying (2.11). Theorem 1.3 gives a measurement matrix with the minimum number of probes for the network satisfying (2.11). Fig. 2-6 shows a measurement matrix $C \in \{0,1\}^{9\times 30}$ for the network in Fig. 2-5, where if $c_{ij} = 1$, the cell at the i-th row and j-th column in the grid is colored black, otherwise, it is colored white.



(a) $f = 1$



(b) $f = 2$



(c) $f = 3$

Figure 2-4: Performance limitation of the group testing.

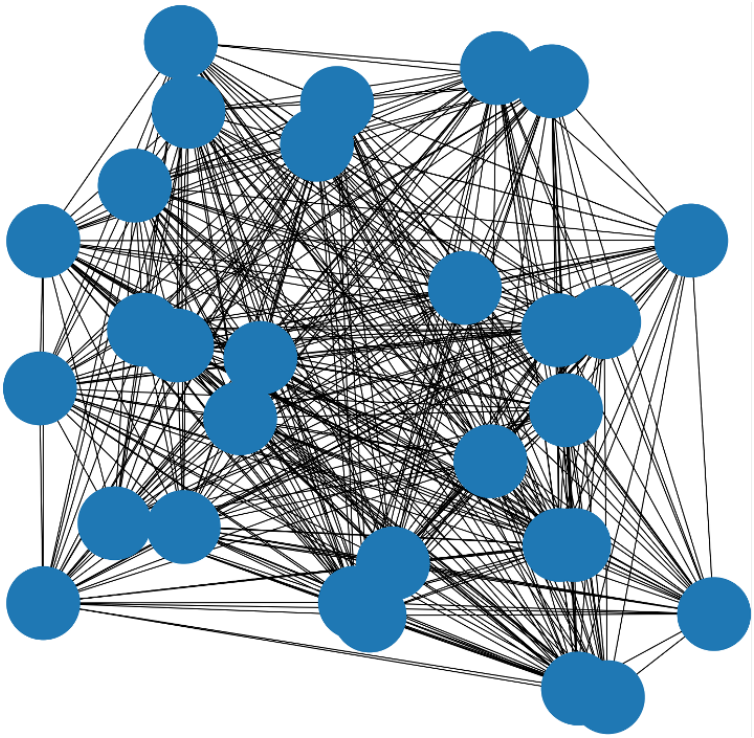


Figure 2-5: Network $\mathcal{G}$ with $n = 30$ and $\delta(\mathcal{G}) = 28$.

2.5 Detection Method Based on Group Testing and Sequential Measurements

Due to the deterministic construction of the measurement matrix, the group testing in Section 2.4 is not applicable to all networks. For example, consider the network with five nodes, as shown in Fig. 2-7. By using the progressive edge-growth algorithm, we have a 4×5 binary correlation matrix in (2.4), for which nodes v_1, v_3, and v_5 will be measured by probe 1, nodes v_1 and v_4 will be measured by probe 2, and nodes v_2, v_4, and v_5 will be measured by probe 4. However, it is clear that there are no simple paths that only consist of the corresponding nodes in the network. It implies that the group testing based on the binary correlation measurement matrix is not applicable to all networks due to the restriction of network topology.

On the other hand, the exactness of detection of the group testing relies on the assumption that the maximum number of abnormal nodes f is known prior. However, it is not realistic.

Based on the above considerations, we propose a detection approach based on group testing and sequential measurements that is applicable to arbitrary network topologies and does not utilize f as prior knowledge. The process of the proposed

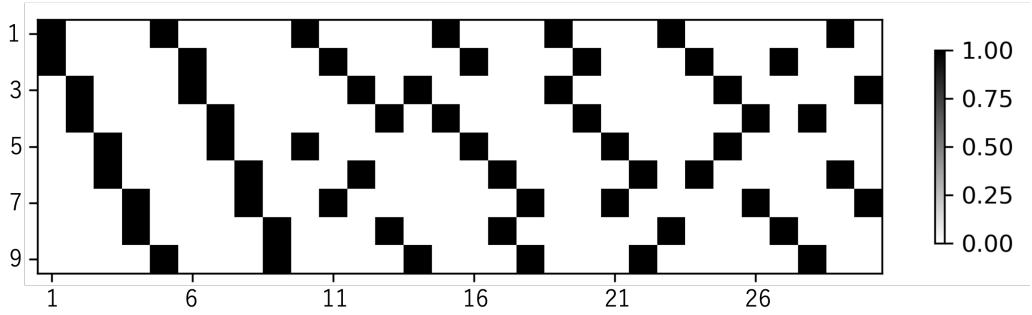


Figure 2-6: A measurement matrix $C \in \{0,1\}^{9\times 30}$ of the network in Fig. 2-5.

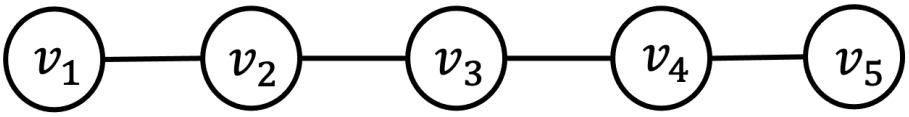


Figure 2-7: A network with a line topology.

method is shown in Fig. 2-8. The method is described in detail in the following subsections.

2.5.1 Group Testing Based on Random Walks

Generate m simple paths based on random walks on network $\mathcal{G} = (\mathbf{V}, \mathbf{E})$ such that

1. $\mathbf{P}_i \neq \mathbf{P}_j$ for every $(i,j) \in \{1,2,\ldots,m\}^2$ such that $i \neq j$,
2. $\bigcup_{i=1}^{m} \mathbf{P}_i = \mathbf{V}$,
3. $\bigcup_{i=1}^{m-1} \mathbf{P}_i \subset \mathbf{V}$.

Here, the first condition is to avoid duplicate measurements, the second one is to ensure that all nodes in the network are measured at least once, and the third condition is to reduce the number of measurements. In addition, in practice, one may prefer to take measurements with short paths to reduce the communication cost and the measurement time [52]. In this case, by setting $|\mathbf{P}_i| \leq d$ for every $i \in \{1,2,\ldots,m\}$, the maximum length of the probes can be limited to d. For example, consider the network in Fig. 2-3, where the manager generates three paths satisfying the above three conditions and $d = 4$.

By sending m probes along the paths, from (2.1), we have (2.2). Then, the group testing is to detect the abnormal nodes by solving (2.2) with respect to x.

However, if $m < n$, the number of scalar equations in (2.2) is less than the number of unknowns. Moreover, the measurement matrix C is constructed randomly.

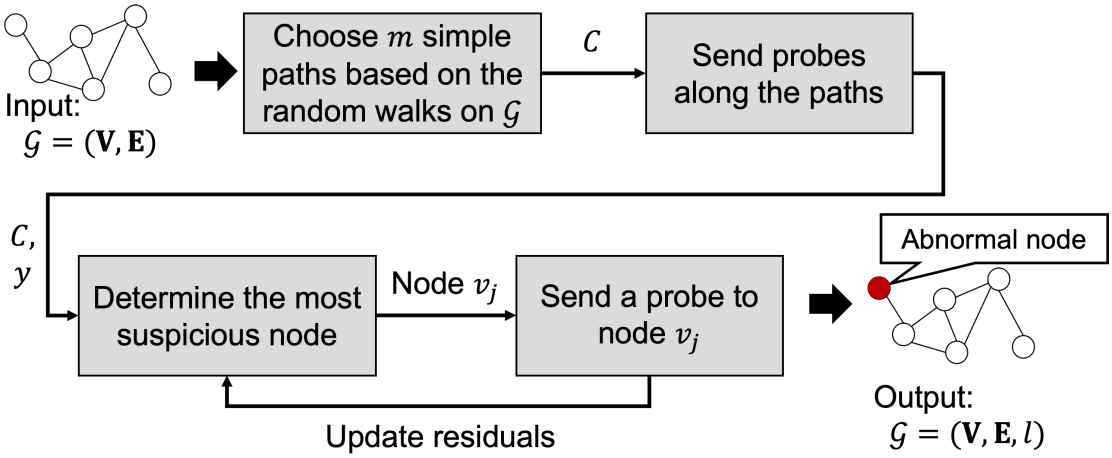


Figure 2-8: Process of the detection method.

They imply that there might be multiple solutions to (2.2). In other words, the information of C and y may not be sufficient for the manager to uniquely determine x. For example, consider the network in Fig. 2-3, the anomaly status vector is $x = [\ 0 \quad 0.8 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0\ ]^\top$, i.e., node v_2 is an abnormal node with $l(v_2) = 0.8$. The manager generates three paths as shown in Fig. 2-3. Then, perform the group testing based on the measurement matrix C in (2.3) and obtain the measurement result $y = [\ 0.8 \quad 0 \quad 0\ ]^\top$. It is clear that there are multiple solutions to (2.2), e.g., $[\ 0.8 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0\ ]^\top$ and $[\ 0 \quad 0.8 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0\ ]^\top$. This motivates us to improve the detection method.

2.5.2 Incorporation of Group Testing and Sequential Measurements

On the one hand, the measurement result y contains information about the abnormal nodes. From C and y, the abnormal nodes can be roughly estimated. On the other hand, the manager can send a probe to any node in the network and measure its anomaly status to complement the insufficient information for the detection. Based on the two considerations, we propose incorporating the individual measurements of the suspicious nodes into the group testing.

Now, how do we select the suspicious node from C and y that will be individually measured? Our idea is given as follows: Consider the linear equation in (2.2), and it can be represented by

$$y = c_1 l(v_1) + c_2 l(v_2) + \cdots + c_n l(v_n), \tag{2.12}$$

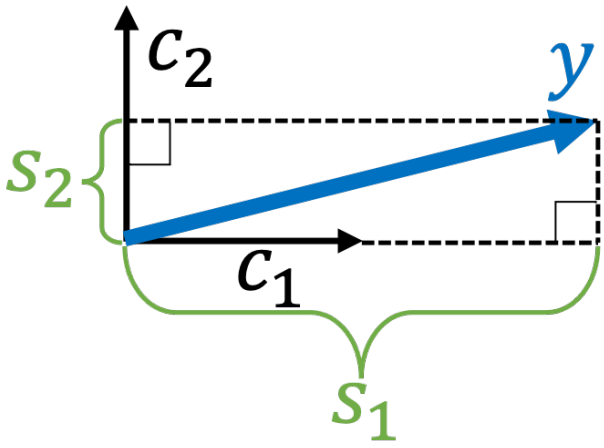


Figure 2-9: An example of the scalar projection.

where $c_j \in \{0,1\}^m$ is the j-th column vector of C. In other words, the vector y is constructed by the components c_j $(j = 1, 2, \ldots n)$ with $l(v_j)$ as coefficients. It is clear that a large value of $l(v_j)$ leads to a large scalar projection of y on c_j, which is given by

$$s_j = \frac{c_j^\top}{\|c_j\|_2} y. \tag{2.13}$$

For example, consider a vector $y = c_1 l(v_1) + c_2 l(v_2)$ with $l(v_1) = 2$ and $l(v_2) = 0.5$ as shown in Fig. 2-9. Since $l(v_1) > l(v_2)$, we have $s_1 > s_2$. Consider it over in reverse, a large scalar projection of y onto the column vectors c_j may mean that $l(v_j)$ has a large value [82, 83]. Therefore, we propose that the most suspicious node is selected by calculating the scalar projection of y onto the column vectors c_j $(j = 1, 2, \ldots, n)$.

Then, the detection method iterates three steps: (a) determining the most suspicious node according to C and y, (b) measuring the anomaly status of the most suspicious node, and (c) updating the estimation of the anomaly status vector and the residual. The method is detailed in Algorithm 1, where the function J_j $(j = 1, 2, \ldots, n)$ is related to the selection of the suspicious node, it is given by

$$J_j(r) = \frac{c_j^\top}{\|c_j\|_2} r. \tag{2.14}$$

In the loop with respect to t, $r(t)$ and $\mathbf{L}(t)$ denote the residual and the index set of nodes which has never been individually measured until the t-th iteration, respectively, $x(t)$ denotes the estimation of the anomaly status vector in the t-th iteration. In Algorithm 1, step (a) is performed in 1 and 2, where the most suspicious node is

Algorithm 1 Detection of Abnormal Nodes in Network $\mathcal{G}$.

Initialization: Let $r(0) = y$, $\mathbf{L}(0) = \{1, 2, \ldots, n\}$, and $x(0) = [\ 0\ \ 0\ \ \cdots\ \ 0\ ]^\top \in \mathbf{R}^n$. Let $J_j : \mathbf{R}^m \to [0, \infty)$ be arbitrarily given for $j \in \{1, 2, \ldots, n\}$.
for $t = 1, 2 \ldots, n$ **do**

1. Calculate $J_j(r(t-1))$ for $j \in \mathbf{L}(t-1)$.
2. Let $j(t)$ denote the index j corresponding to the largest value of $J_j(r(t-1))$ in the list $\mathbf{L}(t-1)$, i.e., $j(t) = \arg\max_{j \in \mathbf{L}(t-1)} J_j(r(t-1))$. If there are multiple maximum values, then $j(t)$ is an arbitrarily selected one of them.
3. Send a probe to the node $v_{j(t)}$ to measure the anomaly status of the node, and obtain its true anomaly status, denoted by $l^*(v_{j(t)})$.
4. Let $x(t) = x(t-1)$. Assign the value of $l^*(v_{j(t)})$ to the $j(t)$-th element of $x(t)$, denoted by $l_{j(t)}(t)$, i.e., let $l_{j(t)}(t) = l^*(v_{j(t)})$.
5. Update $\mathbf{L}(t) = \mathbf{L}(t-1) - \{j(t)\}$ and $r(t) = r(t-1) - c_{j(t)} l^*(v_{j(t)})$.

end for

selected based on the function J_j, step (b) is realized in 3, and step (c) is executed in 4 and 5.

For Algorithm 1, we propose a termination condition that allows the detection algorithm to terminate after a few iterations and output the estimation of the anomaly status vector with guaranteed exactness.

Theorem 2 *Consider Algorithm 1. Let $l^*(v_j)$ denote true label value of the node v_j, and define $x^* := [\ l^*(v_1)\ \ l^*(v_2)\ \ \cdots\ \ l^*(v_n)\ ]^\top \in [0, \infty)^n$. Assume that the measurement matrix C is constructed by the method in Section 2.5.1, and $J_j : \mathbf{R}^m \to [0, \infty)$ is arbitrarily given for $j \in \{1, 2, \ldots, n\}$. If $r(t) = 0$ in 5 of Algorithm 1 for an iteration step t, then $x(t) = x^*$.*

Proof: See Appendix B. ■

Theorem 2 provides a termination condition for the detection algorithm, that is, $r(t) = 0$. Once the condition is satisfied at the t-th iteration, the estimation $x(t)$ is equal to the true anomaly status vector x^*. Then, the algorithm can terminate early and output an exact estimation.

2.6 Performance Evaluation

In this section, we evaluate the performance of the proposed method in Section 2.5 by simulation. The performance of the method corresponds to the number of probes for a given network in a detection.

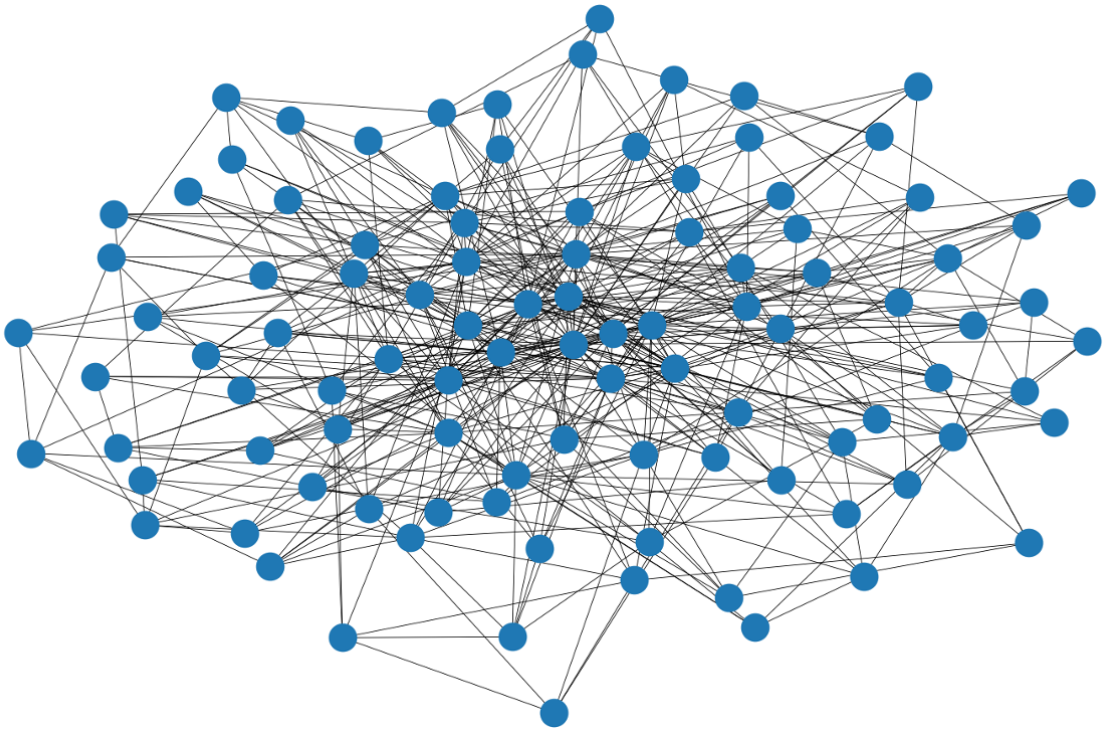


Figure 2-10: Network $\mathcal{G}$ with $n = 100$ nodes.

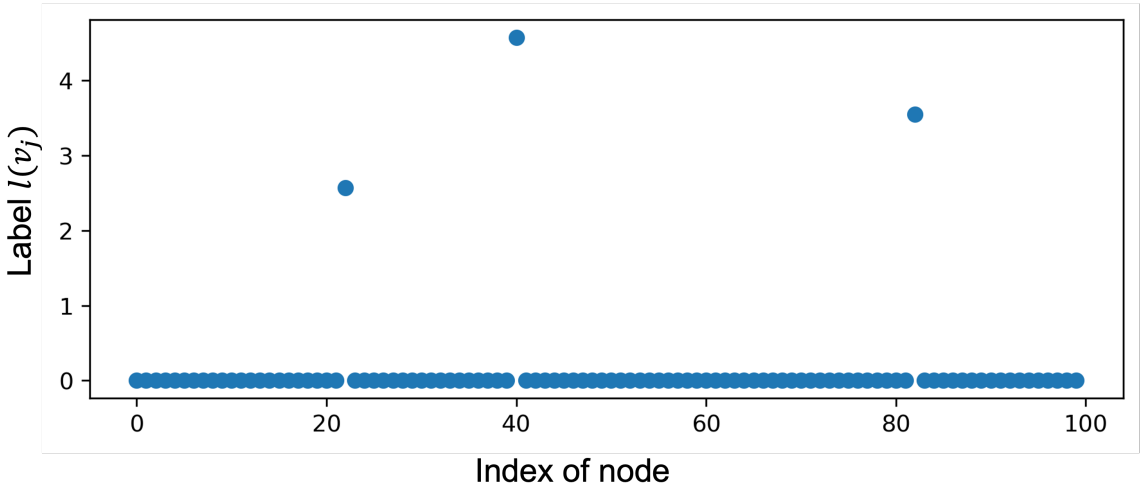


Figure 2-11: Anomaly status vector of network $\mathcal{G}$.

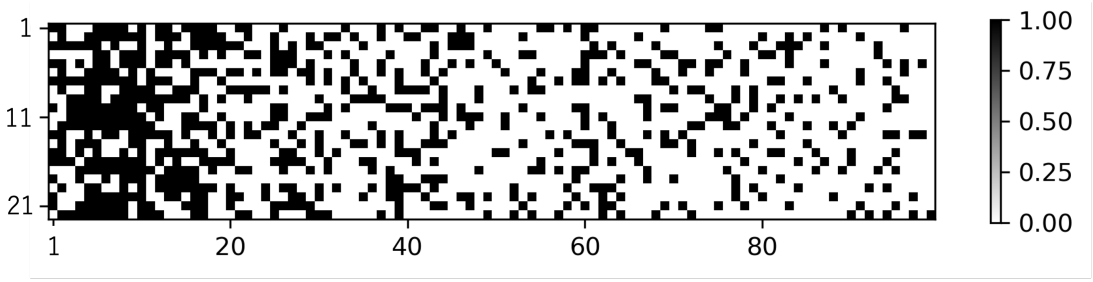


Figure 2-12: Measurement matrix.

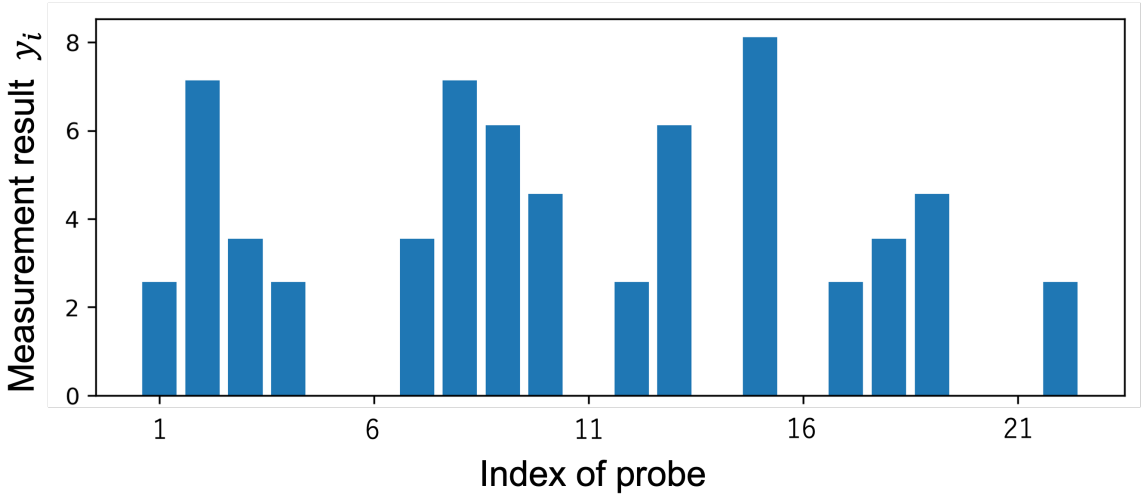


Figure 2-13: Measurement results of the probes.

2.6.1 Simulation Settings

Since the Barabási-Albert (BA) model is capable of generating the networks with real network characteristics [84, 85], we generated a network $\mathcal{G}$ with $n = 100$ nodes from the BA model, as shown in Fig. 2-10.

Assume that $f = 3$, where $l(v_{22}) = 2.57$, $l(v_{40}) = 4.57$, and $l(v_{82}) = 3.55$. The anomaly status vector of network $\mathcal{G}$ is shown in Fig. 2-11, where a dot represents the anomaly status at a node.

Then, perform the proposed method and estimate the anomaly status of nodes.

2.6.2 Detection Result

The constructed measurement matrix $C \in \{0,1\}^{22\times 100}$ with $d = 34$ for network $\mathcal{G}$ as shown in Fig. 2-12, where if $c_{ij} = 1$, the cell at the i-th row and j-th column

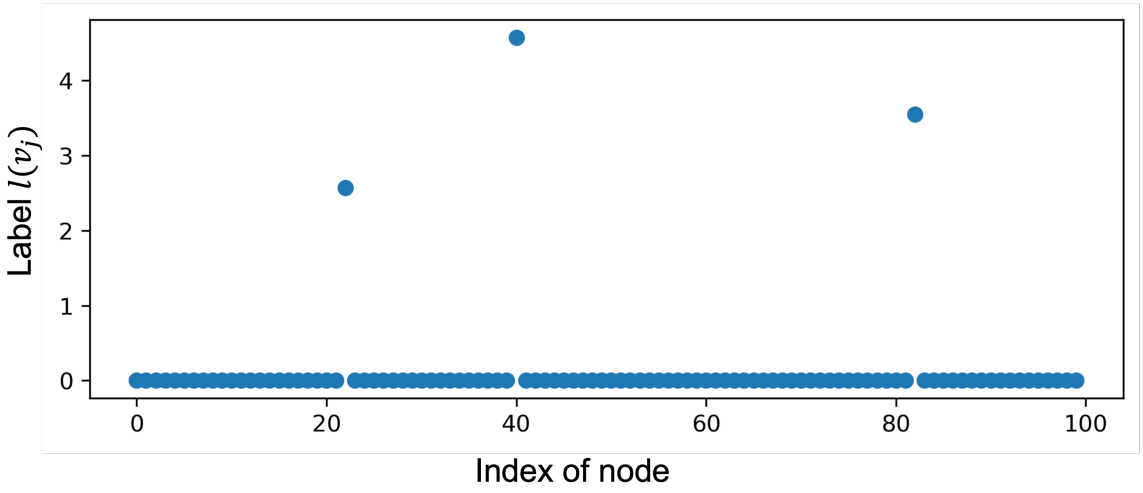


Figure 2-14: Anomaly status vector estimated by the proposed method.

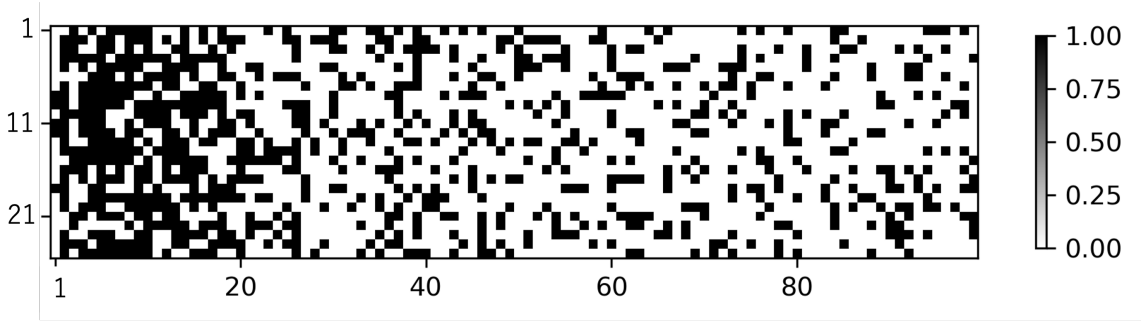


Figure 2-15: Measurement matrix of the previous method.

in the grid is colored black, otherwise, it is colored white. Then, the manager sent probes based on the measurement matrix C and obtained the measurement results, as shown in Fig. 2-13.

We applied Algorithm 1, and the estimated anomaly status vector is shown in Fig. 2-14. The algorithm terminated after three individual measurements. Then, the total number of probes for the detection was $22 + 3 = 25$. The simulation was coded by Python and executed by the personal computer with CPU Intel (R) Core (TM) i7-1065G7, 1.30 [GHz] and memory 16.0 [GB]. The computation time to estimate the anomaly status vector was 0.003 seconds. From this result and Fig. 2-11, we have that the proposed method can exactly and efficiently locate all abnormal nodes with a few probes.

Next, we compare the detection result with that of the group testing in [54], for which the paths of probes are randomly constructed. For fair comparison, we

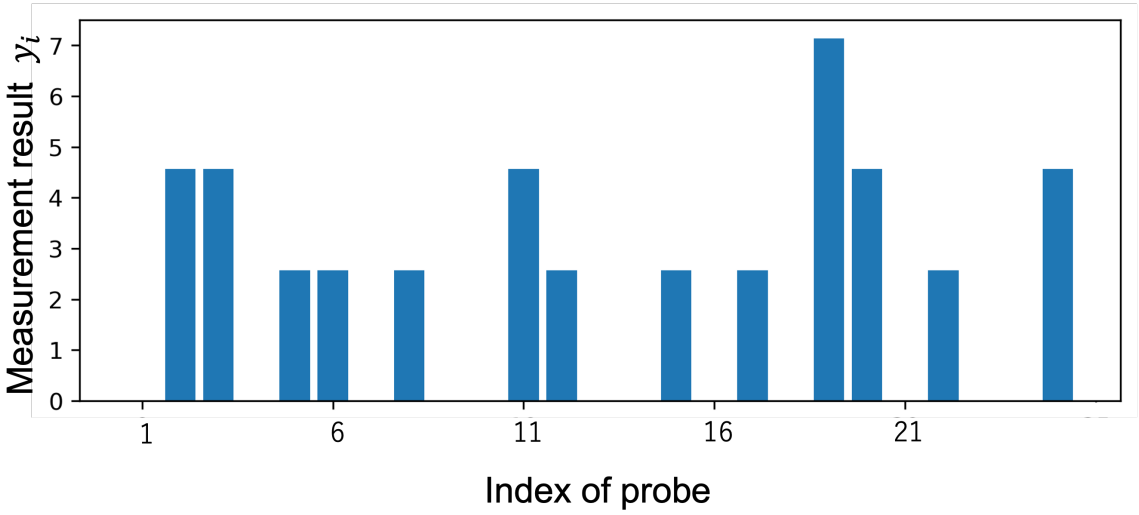


Figure 2-16: Measurement results of the probes of the previous method.

employed the same number of probes as our method, i.e., 25, and the maximum length of the probes was set to $d = 34$. The measurement matrix $C \in \{0,1\}^{25\times 100}$ is shown in Fig. 2-15, by using which the measurement results y are shown in Fig. 2-16. The estimated anomaly status vector of the method in [54] was given by solving the following optimization problem:

$$\min_{x\in\mathbf{R}^n} \|x\|_1 \quad \text{s.t.} \quad (2.2). \tag{2.15}$$

The detection result is shown in Fig. 2-17, we see that the method in [54] can not detect all abnormal nodes exactly.

2.6.3 Statistical Evaluation

We conducted a hundred experiments for each case of $(n, f) \in \{1000, 2000, 5000, 7000, 10000\} \times \{1, 3, 5, 7, 10\}$. Each experiment performed the following steps: (a) generating a network with n nodes from the BA model, (b) generating an anomaly status vector l with f abnormal nodes, and (c) applying the proposed method and estimating the anomaly status vector.

Fig. 2-18 shows the total number of probes in each case, where the triangle marks denote the mean values of the number of probes with the same f. Fig. 2-19 shows the average computation time for the cases of $n \in \{1000, 2000, 5000, 7000, 10000\}$. The results indicate that our proposed detection method requires only a small number of probes and a short computation time for detection.

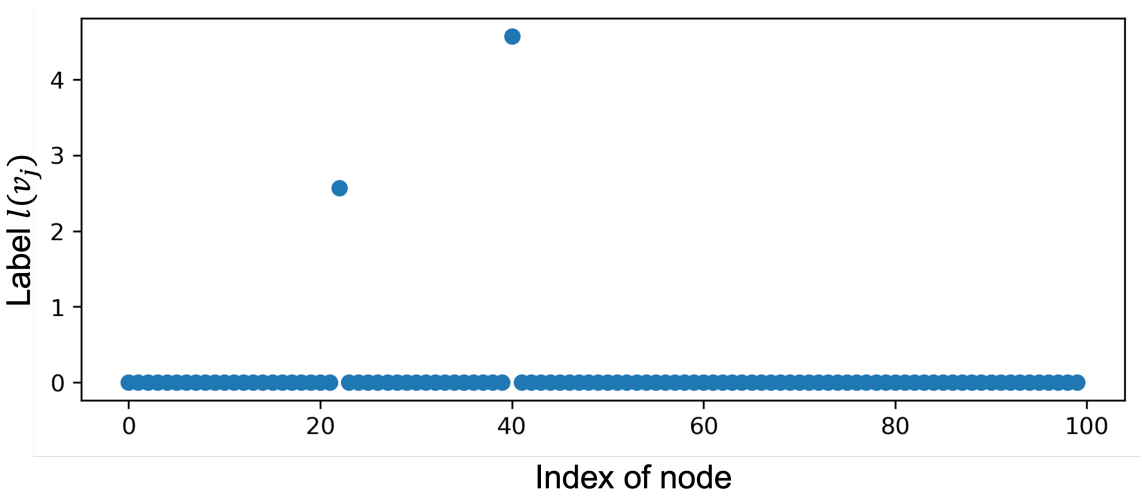


Figure 2-17: Anomaly status vector estimated by the previous method.

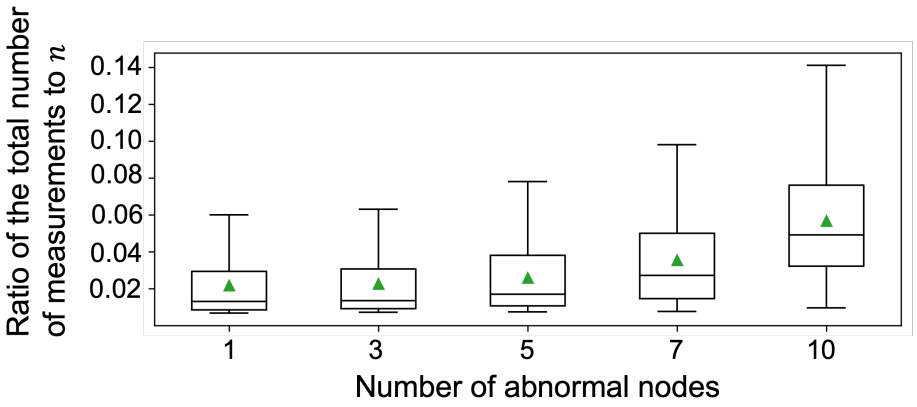


Figure 2-18: Total number of probes of the proposed method.

2.7 Summary

This chapter has investigated the problem of detecting abnormal nodes in the network via a small number of measurements. We proposed the group testing based on the binary correlation matrix and analyzed its performance limitation. Our analysis found that the method can detect abnormal nodes exactly via a small number of measurements. However, we also found that the detection approach is not applicable to all networks due to the restriction of network topology. Therefore, we proposed an iterative detection method based on group testing and sequential measurements. Furthermore, we developed a termination condition for the detection algorithm that allows the algorithm to terminate after a few individual measurements and locate

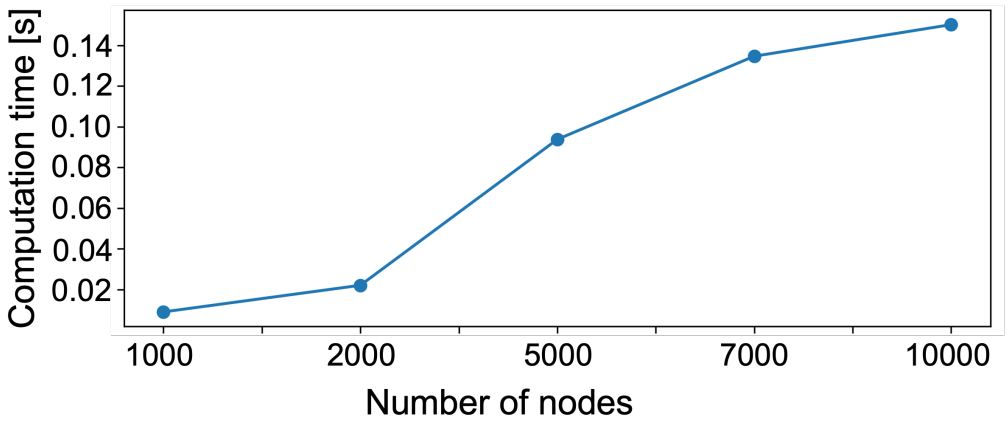


Figure 2-19: Computation time of the proposed method.

the abnormal nodes with guaranteed exactness. Simulation results indicate that our proposed method can locate the abnormal nodes in networks exactly and efficiently.

Chapter 3

Detection of Abnormal Participants in Demand Response

In this chapter, we focus on the detection of abnormal participants in demand response of smart grids.

3.1 Introduction

Demand Response (DR) is the change in electric consumption by prompting consumers to change their normal consumption patterns in response to financial incentives [86–95]. The consumption that is saved through DR is called the *negawatt energy* [96]. DR is a promising solution for managing variable renewables and improving the stability and reliability of smart grids [97–102].

A typical system architecture of DR is shown in Fig. 3-1, where the aggregator is the service provider responsible for collecting negawatt energy, providing monetary incentives to the participants, and then selling the negawatt energy to customers who require it [103–106]. When a shortage of power supply is expected in an area, the utility sends a request to the aggregator to reduce power consumption in the area. Then, the aggregator sends DR requests to the consumers participating in the DR program. In response to the aggregator, the participants reduce consumption by reducing or shifting their electricity usage or by consuming their own energy sources, such as a photovoltaic (PV) generator and batteries.

This research focuses on one of the categories of DR, called *contract-based DR*, in which the aggregator contracts with the participants for their scheduled amounts of negawatt energy, and the participants can receive upfront incentive payments or rate discounts [60]. In practice, it is inevitable that some participants default in

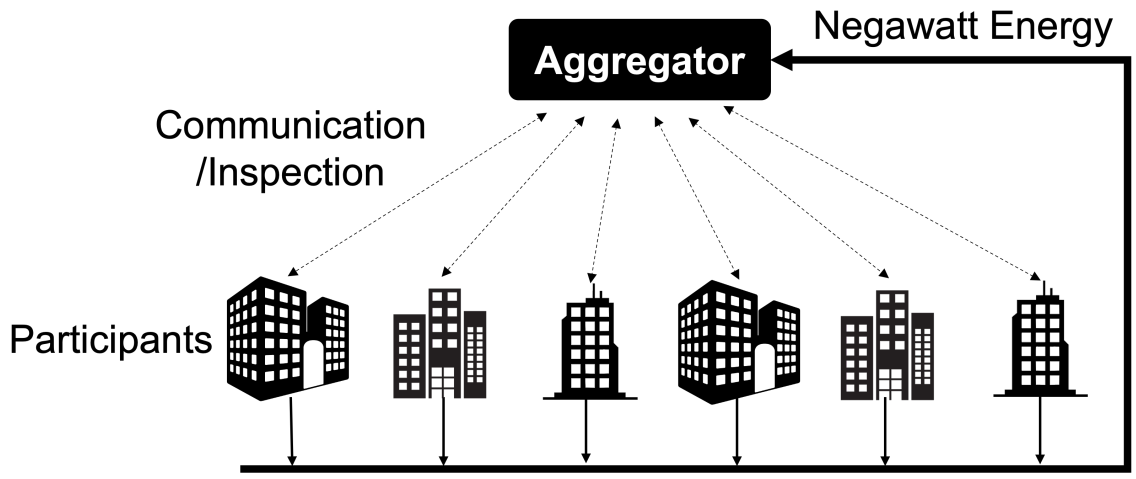


Figure 3-1: Demand response.

providing their scheduled amounts of negawatt energy due to various reasons, such as instrument failures, planned changes, and insufficient PV generation and battery power. Once there is an abnormal participant in DR, the aggregator has to detect and resolve the anomaly as soon as possible to maintain the supply-demand balancing of the power grid.

There is a simple method for the detection of abnormal participants, that is, inspecting the smart meters of all the participants at the moment. However, such brute-force inspection is impractical due to the communication costs [107]. In addition, from the concerns of social acceptance, such a method may cause the participants to feel their privacy is invaded because the smart meters have the electricity consumption data of consumers in near real-time [108–110]. Therefore, it is preferable to detect the abnormal participants with inspections of the smart meters of a few participants.

Recently, a detection approach is proposed in [60]. It iterates the following two steps: (a) estimating the most suspicious participant and (b) inspecting its smart meter, which can detect the abnormal participants exactly without needing 100% exhaustive inspections. However, it remains two challenges for practical application:

1. Unrealistic assumption: The rate of the shortfall to the scheduled negawatt energy, called *anomaly rate*, of a participant is assumed to be time-invariant. It is unrealistic because the anomaly rate is determined by time-varying parameters, such as the scheduled negawatt energy and the actual negawatt energy provided by the participant.

2. Excessive number of inspections: As mentioned in [60], the method requires

inspections for nearly 20 percent of the participants, which may impede practical use since the DR programs have thousands of participants.

This research develops a new method to address the above challenges. We extract four key properties of contract-based DR and incorporate them and the data collected by the aggregator into the anomaly detection. Based on the method in [60], we propose a generalized detection algorithm. It can handle time-varying anomaly rates, incorporate the four properties and data, and significantly reduce the required inspections.

The rest of this chapter is organized as follows: Section 3.2 formulates the anomaly detection problem in DR. Section 3.3 introduces preliminaries on sparse reconstruction. Section 3.4 proposes the detection method. Finally, the performance of the proposed method is evaluated by simulation in Section 3.5.

3.2 Anomaly Detection Problem in DR

3.2.1 Contract-Based DR

A typical framework of the contract-based DR is shown in Fig. 3-1. The aggregator contracts with the participants for their scheduled amounts of negawatt energy. During the DR event, the participants are required to provide the scheduled amount of negawatt energy to the aggregator. The day on which DR is performed is called the *DR event day*. Assume that the contract contains the following clauses:

1. The participant provides a scheduled amount of negawatt energy to the aggregator in response to the DR request from the aggregator. If a participant fulfills it, the participant can receive an incentive from the aggregator; otherwise, the aggregator deducts a certain amount as a penalty from the incentive.

2. The participant declares its address and own power sources, including a photovoltaic (PV) generator and battery.

3. The participant allows the aggregator to inspect its smart meter once a month to collect data and allows the inspection for anomaly detection only when the aggregator detects an anomaly in the DR program.

The first clause is the most fundamental clause in a contract-based DR program. The participants can realize it by installing an energy management system that automatically generates the scheduled negawatt energy during a DR event. The second

Table 3.1: Dataset (a): Profiles of Participants.

Participant 1	
Address	Area 6
PV generation power (kW)	3
Battery capacity (kWh)	6

Table 3.2: Dataset (b): Scheduled Negawatt Energy of Participants.

Participant 1				
Time slot	1	2	$\cdots$	24
Negawatt (kWh)	0.25	0.36	$\cdots$	0.21

clause helps the aggregator estimate the performance of participants in DR. The third clause is related to the data access of smart meters. It limits the real-time inspections for anomaly detection because the smart meter contains private information on the current state of the participant.

3.2.2 Collected Data by the Aggregator

The aggregator collects the data of participants based on the contract. Assume that the aggregator has the following datasets.

(a) Profiles of participants.

(b) Scheduled amount of negawatt energy of participants.

(c) Smart meter data of participants (including the data until the last inspection of the smart meter).

(d) Total negawatt energy that the aggregator obtained (including the data until the last DR event day).

(e) Environmental condition of the prespecified areas (including the data until the last DR event day).

Datasets (a) and (b) are collected when a participant applies to the DR program or updates its profile. Dataset (a) contains the address, PV generation power (kW), and battery capacity (kWh) of the participant, as exemplified in Table 3.1, where the PV generation power or battery capacity is zero if the participant does not have the corresponding device. Dataset (b) includes the scheduled negawatt energy (kWh) at each time slot of the participants, where time slots are prespecified by the aggregator. An example of dataset (b) is shown in Table 3.2. Dataset (c) is collected by inspecting

Table 3.3: Dataset (c): Smart Meter Data of Participants.

Participant 1							
Date	Jan. 1			$\cdots$	Dec. 31		
Time slot	1	$\cdots$	24	$\cdots$	1	$\cdots$	24
Electricity consumption (kWh)	2.3	$\cdots$	2.5	$\cdots$	4.2	$\cdots$	3.9
Actual negawatt (kWh)	0.25	$\cdots$	0.21	$\cdots$	0.1	$\cdots$	0.15
Performance record	0	$\cdots$	0	$\cdots$	0.6	$\cdots$	0.29

Table 3.4: Dataset (d): Total Negawatt Energy Obtaind by the aggregator.

Date	Jan. 1			$\cdots$	Dec. 31		
Time slot	1	$\cdots$	24	$\cdots$	1	$\cdots$	24
Total negawatt (kWh)	1034	$\cdots$	1167	$\cdots$	998	$\cdots$	925

smart meters once a month. As shown in Table 3.3, it includes the electricity consumption (kWh), actual negawatt energy (kWh) provided to the aggregator, and DR performance, which is the rate of the shortfall to the scheduled negawatt energy, at each time slot. Dataset (d) is shown in Table 3.4, which includes the total negawatt energy that the aggregator obtained at each time slot during DR event days. Dataset (e) is illustrated in Table 3.5. It contains the weather data of each area (prespecified by a geographical mesh) at each time slot, i.e., the solar radiation (kWh/m^2), outside temperature (°C), and humidity (%), which are related to the power consumption and PV generation.

3.2.3 Problem Formulation

The anomaly detection problem in a contract-based DR is formulated as follows.

Consider a contract-based DR program, in which participants $1, 2, \ldots, n$ provide the scheduled negawatt energy at time slots $1, 2, \ldots, m$ during a DR event day. Let $c_{ij} \in (0, \infty)$ denote the scheduled negawatt energy (kWh) of participant i at time slot j, and let $x_{ij} \in [0, 1]$ be the *anomaly rate*, i.e., the rate of the shortfall to the scheduled negawatt energy, of participant i at time slot j. If participant i defaults at time slot j, we have $x_{ij} \neq 0$; otherwise, $x_{ij} = 0$. Here, we refer to the participant with $x_{ij} \neq 0$ for any $j \in \{1, 2, \ldots, m\}$ as an *abnormal participant*. Then, the negawatt energy

Table 3.5: Dataset (e): Environmental Conditions of Areas.

Area 1							
Date	Jan. 1			$\cdots$	Dec. 31		
Time slot	1	$\cdots$	24	$\cdots$	1	$\cdots$	24
Solar radiation (kWh/m^2)	0	$\cdots$	0	$\cdots$	0	$\cdots$	0
Temperature (°C)	5	$\cdots$	4	$\cdots$	6	$\cdots$	2
Humidity(%)	52	$\cdots$	45	$\cdots$	43	$\cdots$	47

(kWh) actually provided by participant i at time slot j is given by $c_{ij}(1 - x_{ij})$. Let $s_j \in [0, \infty)$ denote the total amount of negawatt energy (kWh) that the aggregator obtained at time slot j. Since the total negawatt energy provided by the participants is equal to that collected by the aggregator at each time slot, we have

$$\sum_{i=1}^{n} c_{ij}(1 - x_{ij}) = s_j \quad (j = 1, 2, \ldots, m). \tag{3.1}$$

From datasets (b) and (d), the aggregator has the information on c_{ij} $(i = 1, 2, \ldots, n,$ $j = 1, 2, \ldots, m)$ and s_j $(j = 1, 2, \ldots, m)$ in (3.1), and x_{ij} $(i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m)$ are unknown to the aggregator. Then, by solving the linear equations in (3.1) with respect to the unknowns x_{ij} $(i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m)$, the aggregator can detect the abnormal participants in the DR.

However, in (3.1), the number of scalar equations, i.e., m, is less than the number of unknowns, i.e., mn. It implies that there might be multiple solutions of (3.1), which prevents the aggregator from determining the exact values of x_{ij} $(i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m)$. Therefore, our problem is to determine the unknowns x_{ij} $(i = 1, 2, \ldots, n,$ $j = 1, 2, \ldots, m)$ from the linear equations in (3.1), datasets (a)–(e) in Section 3.2.2, and the inspections of the smart meters of a few participants.

In the rest of this chapter, let $x_i \in \mathbf{R}^m$ $(i = 1, 2, \ldots, n)$ denote the collection of the anomaly rate of participant i at each time slot, i.e., $x_i := [x_{i1}\ x_{i2}\ \cdots\ x_{im}]^\top$, called the *anomaly rate vector of participant i*. Let $x \in \mathbf{R}^{mn}$ be the collection of x_i, i.e., $x := [x_1^\top\ x_2^\top\ \cdots\ x_n^\top]^\top$, called the *anomaly rate vector*.

3.3 Preliminaries on Sparse Reconstruction

As a preparation, we introduce a framework of sparse reconstruction of unknown vectors.

Consider the problem of solving an unknown vector $x \in \mathbf{R}^n$ from the following

linear equation

$$Ax = b, \tag{3.2}$$

where $A \in \mathbf{R}^{m \times n}$ and $b \in \mathbf{R}^m$ are a known matrix and vector, respectively. When $m < n$, (3.2) might have multiple solutions, implying that x can not be uniquely determined.

If we have prior knowledge that x has a few nonzero elements, i.e., x is sparse, then x might be uniquely determined. The process of determining a sparse unknown vector x from (3.2) is called the *sparse reconstruction* [45, 46].

The sparse reconstruction of (3.2) is typically formulated as an ℓ_0-optimization problem as follows [45]:

$$\min_{x \in \mathbf{R}^n} \|x\|_0 \quad \text{s.t.} \quad (3.2). \tag{3.3}$$

Because $\|x\|_0$ is the number of nonzero elements of x, (3.3) provides the sparsest solution to (3.2). Meanwhile, the objective function is known to be nonconvex; as a result, the problem in (3.3) is NP-hard [46]. Therefore, the following ℓ_1-optimization problem is useful for the convex relaxation of (3.3):

$$\min_{x \in \mathbf{R}^n} \|x\|_1 \quad \text{s.t.} \quad (3.2). \tag{3.4}$$

It can equivalently transformed into a linear programming problem that can be efficiently solved. Moreover, its solution is sparse and equal to the solution of (3.3) with rare exceptions [45]. Therefore, (3.4) is a practical solution to the sparse reconstruction of (3.2).

Next, let us consider the sparse reconstruction with more prior knowledge about the vector x: Consider a permutation matrix $P \in \{0, 1\}^{n \times n}$ of x, with which x is divided into p subvectors $x_{(1)}, x_{(2)}, \ldots, x_{(p)}$, called *block* $1, 2, \ldots, p$, i.e., $Px = [x_{(1)}^\top \; x_{(2)}^\top \; \cdots \; x_{(p)}^\top]^\top$. Among $x_{(1)}, x_{(2)}, \ldots, x_{(p)}$, only a few blocks are nonzero vectors. Such an x is called the *block-sparse vector*. In this case, the following ℓ_2/ℓ_1-optimization problem can be used for sparse reconstruction [111]:

$$\min_{x \in \mathbf{R}^n} \sum_{k=1}^{p} \|x_{(k)}\|_2 \quad \text{s.t.} \quad (3.2). \tag{3.5}$$

Since (3.5) is a convex programming problem, it can be efficiently solved [112].

Furthermore, if we have prior knowledge about the degree to which $x_{(k)}$ ($k = 1, 2, \ldots, p$) tends to zero, the following weighted ℓ_2/ℓ_1-optimization problem is a

promising solution to the sparse reconstruction [113]:

$$\min_{x\in\mathbf{R}^n} \sum_{k=1}^{p} w_{(k)}\|x_{(k)}\|_2 \quad \text{s.t.} \quad (3.2), \tag{3.6}$$

where $w_{(k)} \in \mathbf{R}_+$ is the weight of the k-th block that quantifies the tendency of $x_{(k)}$ to be zero.

3.4 Anomaly Detection Based on Sparse Reconstruction and Sequential Inspections

To address the two challenges for the practical application of the detection algorithm in [60] introduced in Section 3.1, we generalize the algorithm to handle time-varying anomaly rates and incorporate data and prior information. In addition, we present a termination condition for it, under which the algorithm is terminated at an early stage and outputs the estimations with guaranteed exactness.

3.4.1 Generalized Detection Algorithm

The generalized iterative algorithm is shown in Algorithm 2, where the objective function $J : \mathbf{R}^{mn} \to [0, \infty)$ is the design parameter of the algorithm, which will be designed in Section 3.4.2. The set $\mathbf{P}(t)$ denotes the index set of participants whose smart meter has never been inspected until t-th iteration. The algorithm iterates the following three steps: (a) solving the optimization problem OP(t) and determining the most suspicious participant, (b) inspecting the smart meter of the most suspicious participant, and (c) adding the result of (b) into the problem OP($t+1$) as additional knowledge. In the t-th iteration, step (a) is executed in 1 and 2, step (b) is performed in 3, and (c) is realized in 4.

For Algorithm 2, we propose a termination condition, under which the detection algorithm is terminated after a few iterations and outputs the estimations with the guarantee of exactness.

Theorem 3 *Consider Algorithm 2. Let $x^*_{ij} \in [0, 1]$ be the true value of the anomaly rate x_{ij} and let $x^* \in [0, 1]^{mn}$ be the collection of x^*_{ij} ($i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$). Assume that $c_{ij} > 0$ ($i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$) and $J : \mathbf{R}^{mn} \to [0, \infty)$ is arbitrarily given for* OP(t) *($t = 0, 1, \ldots$). If $x_{i(t)} = 0$ in 2 of Algorithm 2 for an iteration step t, then $x(t) = x^*$.*

Proof: See Appendix C. ■

Algorithm 2 Detection Algorithm.

Initialization: Let $J : \mathbf{R}^{mn} \to [0, \infty)$ be arbitrarily given and define OP(0) as $\min_{x \in [0,1]^{mn}} J(x)$ s.t. (3.1). Let $\mathbf{P}(0) := \{1, 2, \ldots, n\}$.
for $t = 0, 1, \ldots, n-1$, **do**:

1. Solve OP(t), and let $x(t)$ denote a solutions of it. Let $x_{ij}(t)$ be the element of $x(t)$ that corresponds to participant i at time slot j.
2. Let $i(t) \in \mathbf{P}(t)$ denote the index of the participant who is estimated to be the most suspicious participant in the sense of $\max_{i \in \mathbf{P}(t)} \|x_i(t)\|_2$, where $x_i(t) := [x_{i1}(t)\ x_{i2}(t)\ \cdots\ x_{im}(t)]^\top$.
3. Inspect the actual negawatt energy of participant $i(t)$ via its smart meter and obtain the true anomaly rates at each time slot, denoted by $x^*_{i(t)j}$ $(j = 1, 2, \ldots, m)$.
4. Let OP($t+1$) be the modified version of OP(t), such that $x_{i(t)j} = x^*_{i(t)j}$ $(j = 1, 2, \ldots, m)$ are added as constraints. Let $\mathbf{P}(t+1) = \mathbf{P}(t) - \{i(t)\}$.

end for

3.4.2 Properties of Contract-Based DR and Design of the Objective Function J

The key issue for Algorithm 2 is how to design objective function J of OP(t), since J is related to the performance of the algorithm. In this subsection, we extract four special properties of contract-based DR and propose the objective function incorporating the properties.

The four properties of contract-based DR are as follows:

- Sparsity of abnormal participants: There are only a few abnormal participants in contract-based DR.
- Temporal correlation of DR performance: If a participant defaults at a time slot, it is likely to default at other time slots during a DR event day.
- Classifiability of participants: Participants can be classified based on the characteristics related to the DR performance.
- Similarity between DR performance and past performance: The DR performance of each participant is similar to its past DR performance.

The first property is extracted from the contract that a default will result in a penalty. The second property is justified because if the default is caused by an instrument fault or insufficient PV generation and battery power, the default may last for a while. The third property is extracted from the inclination of participants with similar characteristics to have similar DR performance. For example, consider two participants

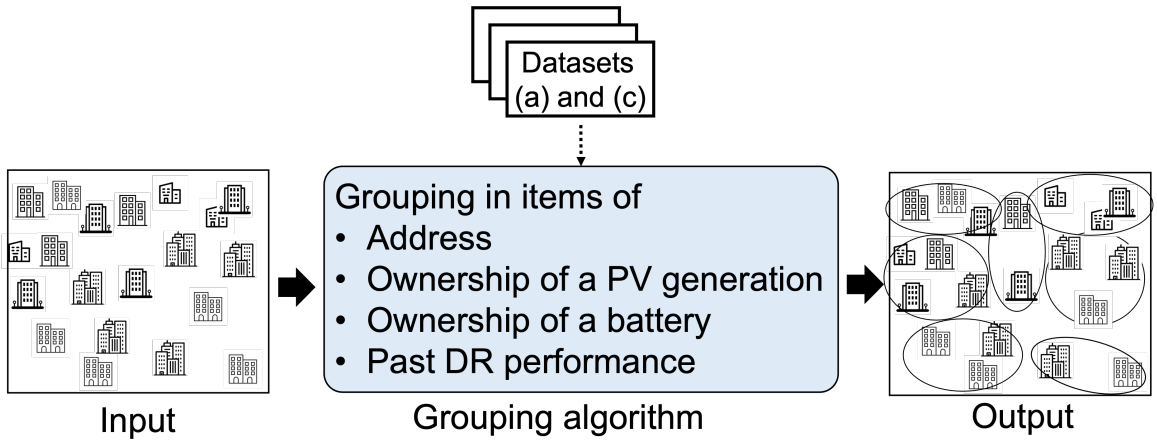


Figure 3-2: Grouping the participants.

located in an area, they plan to provide negawatt energy through PV generation. If the solar radiation is low in the area, then both of them may default. The final one comes from the fundamental assumption of data science that the future resembles the past.

The first three properties imply that the anomaly rate vector x has block sparsity. More specifically, the first property corresponds to the sparsity of the anomaly rate vector x, and the second and third properties indicate that x with appropriately defined blocks has block sparsity. The final property can be used to quantify the tendency of each block to be zero. Then, the detection problem can be reduced to a weighted ℓ_2/ℓ_1-optimization problem in (3.6). Based on the above consideration, the objective function J of OP(t) is designed as follows.

By datasets (a) and (c), the aggregator classifies the participants based on the characteristics related to the DR performance. As shown in Fig. 3-2, the participants are classified into $r \times 2 \times 2 \times q$ groups in terms of

- Address: area 1, area 2, ..., or area r,
- Ownership of a PV generation: own or not,
- Ownership of a battery: own or not,
- Past DR performance: grade 1, grade 2, ..., or grade q,

where the areas are the same as specified for dataset (e), and the grades of the past DR performance are given by the number of anomalies in a certain period. By denoting the resulting groups as group $1, 2, \ldots, p$, block $x_{(k)}$ is the collection of anomaly rate

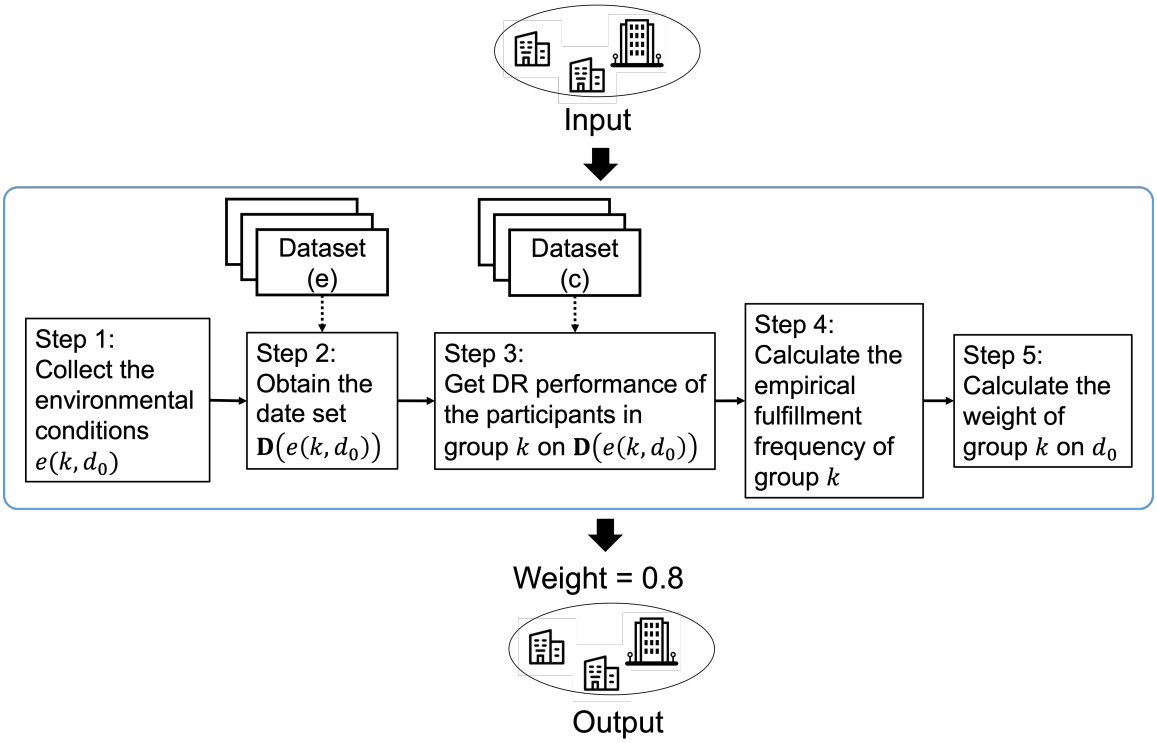


Figure 3-3: Calculating the weight of a group.

vectors x_i of the participants in group k. From the first three properties, we have that there are a few nonzero blocks among $x_{(1)}, x_{(2)}, \ldots, x_{(p)}$, which implies that x is block-sparse with the blocks of $x_{(1)}, x_{(2)}, \ldots, x_{(p)}$.

Next, let us consider the fourth property, by using which the empirical fulfillment frequency of group k can be set to the weight $w_{(k)} \in \mathbf{R}_+$ of block $x_{(k)}$. The process of calculating the weight of a block is shown in Fig. 3-3. Let $\mathbf{G}_k \subseteq \{1, 2, \ldots, n\}$ denote the index set of the participants in group k, and let $e(k, d) \in \mathbf{R}^{h_1+h_2+h_3}$ denote the environmental conditions on day d and the last several days in the area where group k are located. In other words, $e(k, d)$ is the collection of the daily total solar radiation over the past h_1 days, average daily temperature and humidity over the past h_2 and h_3 days, respectively, where $h_i \in \{1, 2, \ldots\}$ $(i = 1, 2, 3)$ are arbitrarily given numbers. Consider a DR event day on which an anomaly occurs, denoted by d_0. Let $\mathbf{D}(e(k, d_0))$ denote the set of the past DR event dates on which the environmental conditions are similar to $e(k, d_0)$ on dataset (e), i.e., $\mathbf{D}(e(k, d_0)) = \{d \mid e(k, d) \simeq e(k, d_0)$ on dataset (e) $\}$, where $\simeq$ is the similarity relation prespecified

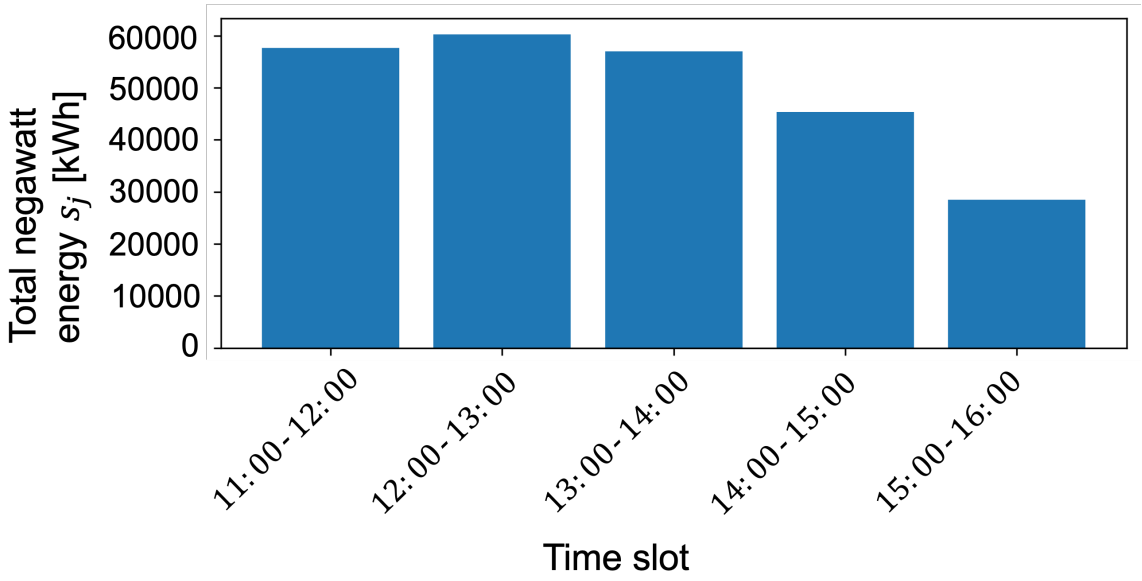


Figure 3-4: Total negawatt energy that the aggregator obtained.

by the aggregator. On the other hand, let

$$\bar{x}(i,d) = \begin{cases} 1 & \text{there exists a time slot } j \in \{1,2,\ldots,m\} \text{ during } d \\ & \text{such that an anomaly occurs,} \\ 0 & \text{otherwise,} \end{cases}$$

it can be calculated from dataset (c). Then, the cumulative set of the fulfilled participants in group k is given by $\{(i,d) \in \mathbf{G}_k \times \mathbf{D}(e(k,d_0)) \mid \bar{x}(i,d) = 0\}$, and the empirical fulfillment frequency of group k is given by

$$f_{(k)} := \frac{\left|\{(i,d) \in \mathbf{G}_k \times \mathbf{D}(e(k,d_0)) \mid \bar{x}(i,d) = 0\}\right|}{\left|\mathbf{G}_k \times \mathbf{D}(e(k,d_0))\right|}. \tag{3.7}$$

Thus, the weight $w_{(k)}$ is calculated by

$$w_{(k)} := \sqrt{|\mathbf{G}_k|} f_{(k)}. \tag{3.8}$$

The term $\sqrt{|\mathbf{G}_k|}$ is employed to adjust the effects of the difference in the block sizes on minimization.

Then the objective function J of OP(t) is set to the objective function in (3.6), where $x_{(k)}$ $(k = 1,2,\ldots,p)$ is obtained from our grouping algorithm and $w_{(k)}$ is given by (3.8).

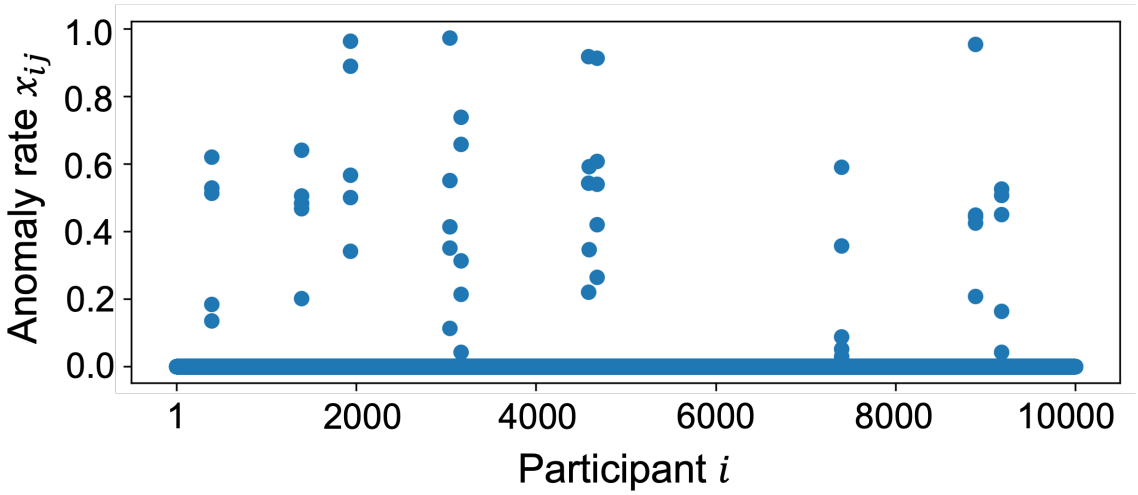


Figure 3-5: Anomaly rates of participants.

3.5 Performance Evaluation

In this section, we present simulation to evaluate the effectiveness of the proposed method.

3.5.1 Case with 10000 participants

Simulation Settings and Grouping Result

Consider a DR program with 10000 participants over five time slots from 11:00 to 16:00, i.e., $n = 10000$ and $m = 5$. From [114–116], we had the datasets (a)–(e) for 365 days and generated the data for the day on which the anomaly is to be detected.

Fig. 3-4 shows the total negawatt energy that the aggregator obtained on the detection day. The true anomaly rates of participants are shown in Fig 3-5, where the anomaly was made by ten participants, five dots represent the anomaly rates of a participant at five time slots, they are arranged vertically at participant i.

The parameters for grouping and calculating weights were given as follows: $r = 9$, $q = 2$, $h_1 = 3$, $h_2 = 1$, and $h_3 = 1$. The DR performance of a participant was set to grade 0 if the participant has never defaulted in the last three months; otherwise, it was set to grade 1. The similarity relation of the environmental condition was defined as the identity of the signs of deviations. The results of grouping and weights are shown in Table 3.6.

Table 3.6: Grouping result on the detection day

Group	Area	Ownership of a PV system	Ownership of a battery	Grade	Weight
1	1	True	True	0	1
2	1	True	True	1	1
3	1	True	False	0	1
4	1	True	False	1	1
⋮	⋮	⋮	⋮	⋮	⋮
71	9	False	False	0	1
72	9	False	False	1	0.95

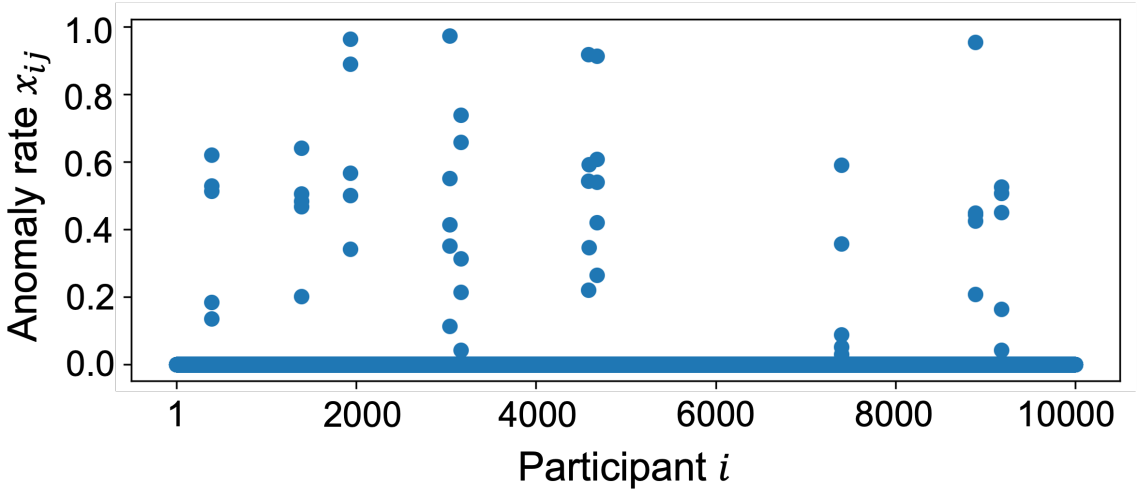


Figure 3-6: Anomaly rates estimated by the proposed method.

Detection Results

We applied Algorithm 2, the result of the detection method is shown in Fig. 3-6. The algorithm terminated after 25 inspections. The total computation time was 67 seconds. From this result and Fig. 3-5, we see that the proposed method can exactly identify the abnormal participants with a few inspections.

Next, we compare the detection result with that of the conventional method [60]. Although the conventional method is for the case of time-invariant anomaly rates, it almost corresponds to the case where the objective function of OP(t) is given by the objective function in (3.4). The detection results obtained by the method in [60] are the same as in Fig. 3-6, whereas it requires 4357 inspections (approximately 174 times of the number of the proposed method). It demonstrates that by improving

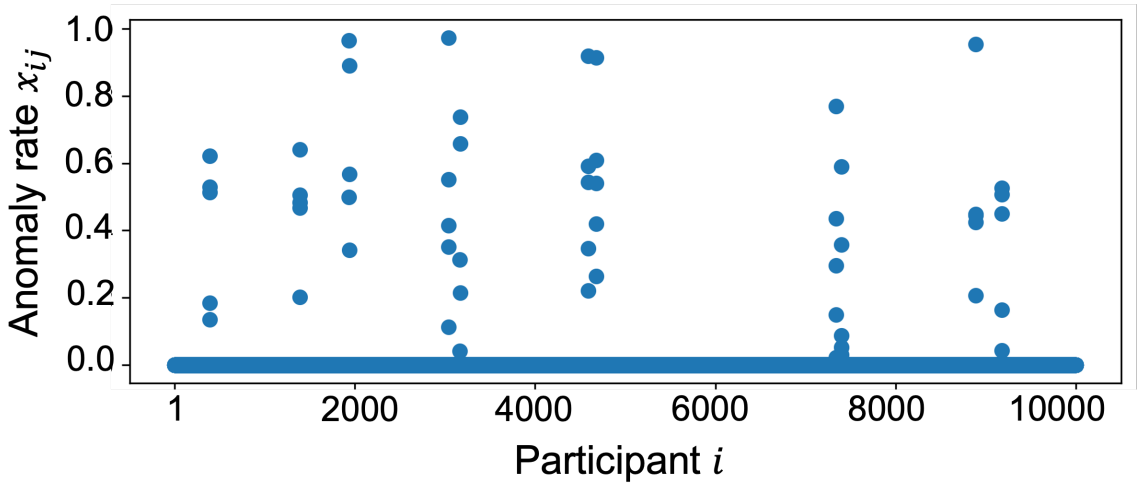


Figure 3-7: True anomaly rates of participants.

the design of the objective function, our method can significantly reduce the number of required inspections compared with the conventional method.

3.5.2 Case with Accidental Abnormal Participants

We also consider the case that there are some accidental abnormal participants, i.e., the participants who have a large value of the empirical fulfillment frequency but defaulted in the DR event. For example, a participant defaults to provide its scheduled negawatt energy due to the instrument failure. The true anomaly rates are shown in Fig. 3-7, there are 11 abnormal participants, where the participant $i = 7338$ is an accidental abnormal participant whose empirical fulfillment frequency is 100%.

Fig. 3-8 shows the results of the detection method through 46 inspections, which are equal to the true anomaly rates. In this case, the proposed method can also detect the abnormal participants exactly.

3.5.3 Statistical Evaluation

We conducted five experiments for each case of $(n, d) \in \{1000, 2000, 5000, 7000, 10000\} \times \{0.1\%, 0.3\%, 0.5\%, 0.7\%, 1.0\%\}$, where d is the ratio of the number of abnormal participants to n. The simulation conditions were set in the same manner as Section 3.5.1, and each experiment performed the following steps: (a) generating the data for the day on which the anomaly is to be detected and (b) applying the proposed method and estimating the anomaly rates.

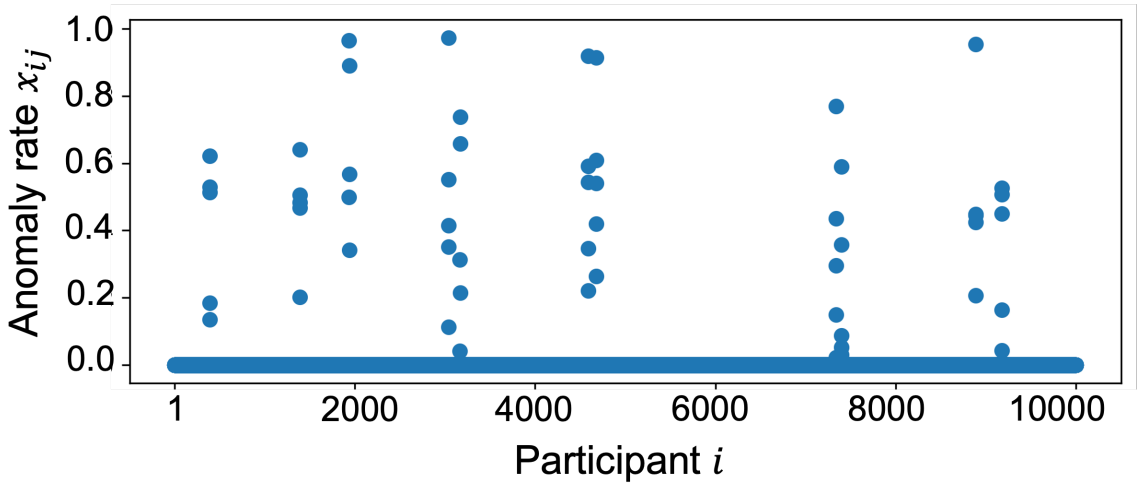


Figure 3-8: Anomaly rates estimated by the proposed method.

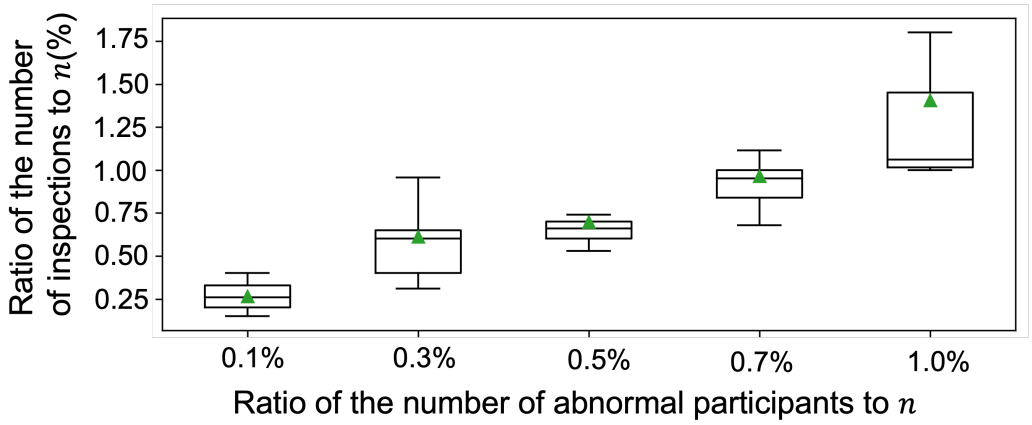


Figure 3-9: Number of inspections of the proposed method.

Fig. 3-9 shows the number of inspections of the proposed method in each case, where the triangle marks denote the average of the ratio of the number of measurements to n. Fig. 3-10 shows the average computation time for the cases of $n \in \{1000, 2000, 5000, 7000, 10000\}$. Simulation results indicate that our proposed method requires only a small number of inspections and a short computation time for detection.

3.6 Summary

In this chapter, a detection problem of abnormal participants in contract-based DR has been investigated. We presented a generalized detection algorithm that has

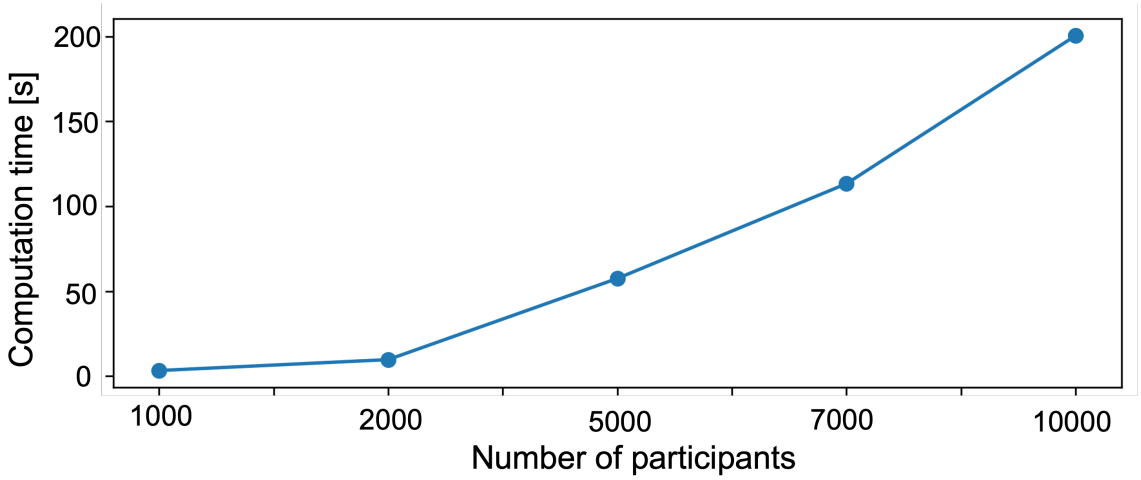


Figure 3-10: Computation time of the proposed method.

flexibility for incorporating prior knowledge and data of the aggregator. Furthermore, we developed a termination condition for the detection algorithm, under which the detection algorithm is terminated after a few iterations and outputs the estimations with the guarantee of exactness. The proposed method can significantly reduce the number of required inspections compared with the previous method.

Chapter 4

Tamper-Resistant Controller in CPSs

In this chapter, we propose a tamper-resistant controller in CPSs, which is based on our work in [117].

4.1 Introduction

As introduced in Chapter 1, it is important to improve the resistance of the CPSs to attacks. To protect the controller from attacks, in [65], a tamper-resistant controller is proposed. The concept of the controller is shown in Fig. 4-1, where the red dots denote the elements in the predefined finite set $\mathbf{Q}$, the blue line and orange curve represent the output of the original controller and the tamper-resistant controller, respectively. If the state is an element of $\mathbf{Q}$, the output of the proposed controller and the original controller are the same; otherwise, the proposed controller produces a different value from the original controller. Since the set $\mathbf{Q}$ is a subset of the set of states with measure zero, theoretically, without the knowledge of $\mathbf{Q}$, it is impossible to obtain the control law. The proposed controller is realized by a neural network, and a time-invariant quantizer is equipped in the system that maps the continuous states to the elements in $\mathbf{Q}$. The system is shown in Fig. 4-2. However, for the time-invariant quantization system, if the attacker observes the signals of the remaining system after stealing the controller, e.g., v, it is easy to obtain the information about the set $\mathbf{Q}$, resulting in the controller being vulnerable.

To address the above security vulnerability, in this chapter, we improve the tamper resistance by using time-varying quantization and propose a new tamper-resistant controller. If the state is an element of a time-varying set, the controller outputs the same value as the original controller; otherwise, it produces a different value from the original controller. By designing the time-varying set elaborately, its information is unattainable for the attackers from the observation of the signals. The proposed

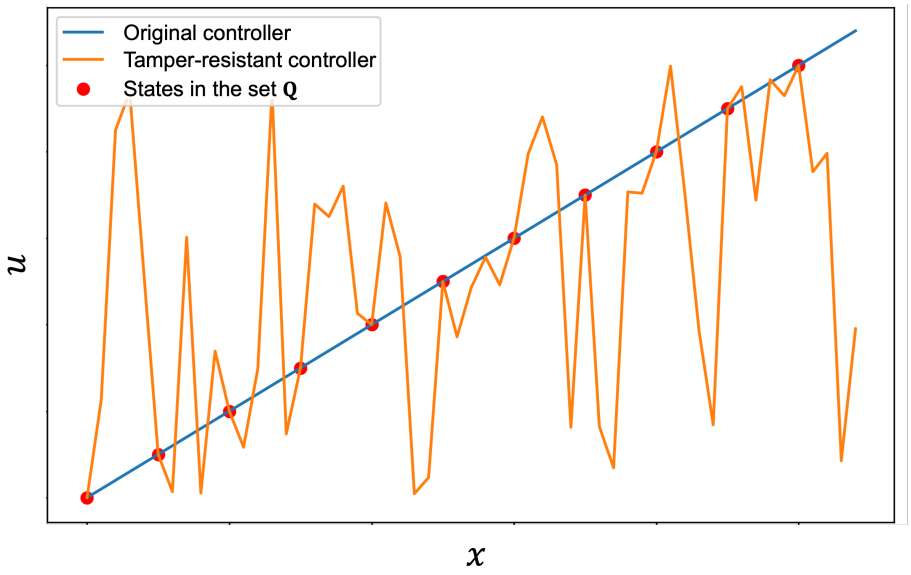


Figure 4-1: Concept of the tamper-resistant controller in [65].

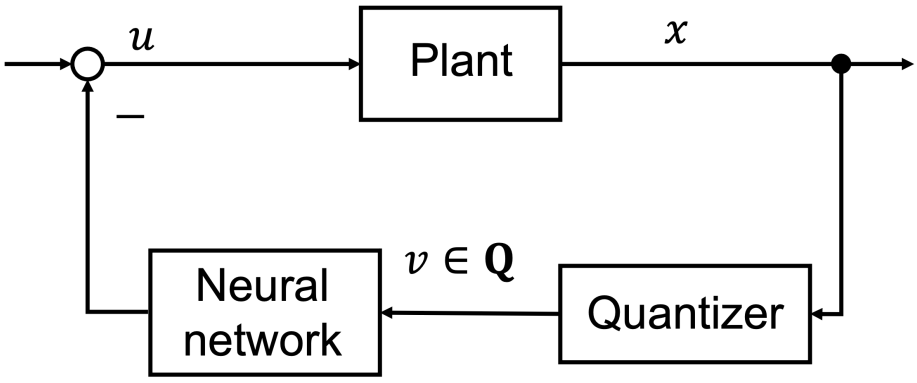


Figure 4-2: Realization of the tamper-resistant controller in [65].

controller is achieved based on a neural network and time-varying quantization.

The rest of this chapter is organized as follows: Section 4.2 presents the security requirements of a tamper-resistant controller and formulates the design problem. Section 4.3 introduces the realization of the tamper-resistant controller. Finally, the security of the proposed method is evaluated by simulation in Section 4.4.

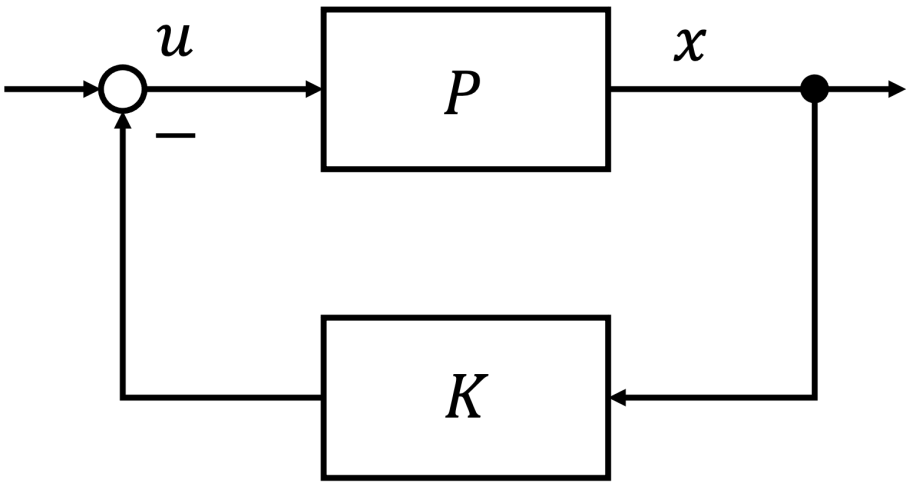


Figure 4-3: Control system.

4.2 Tamper-Resistant Control in CPSs

4.2.1 System

Consider the feedback system shown in Fig. 4-3, composed of the discrete time-invariant linear plant P and the controller K. The state-space representation of the plant is

$$x(t+1) = Ax(t) + Bu(t), \tag{4.1}$$

where $x \in \mathbf{X}(\subset \mathbf{R}^n)$ and $u \in \mathbf{R}^m$ are the state vector and input vector of the plant, respectively, the matrices $A \in \mathbf{R}^{n\times n}$ and $B \in \mathbf{R}^{n\times m}$ are the state matrix and the input matrix, respectively. The control law of the state feedback control system is given by

$$u(t) = -Fx(t), \tag{4.2}$$

where the matrix $F \in \mathbf{R}^{m\times n}$ is the constant feedback gain matrix that stabilizes the system.

4.2.2 Security Requirements for a Tamper-Resistant Controller and Problem Formulation

Suppose that the purpose of the attacker is to obtain the feedback gain matrix F of the system. Consider that the attacker employs the following tactics after stealing

the entity of the controller to obtain the gain matrix F.

1. Code analysis: Analyzing the code of the controller.

2. Numerical analysis: Randomly sampling s states $x^{(1)}, x^{(2)}, \ldots, x^{(s)}$ and observing the state-input pairs of the controller, denoted by $\mathbf{D} = \{(x^{(1)}, K(x^{(1)})), (x^{(2)}, K(x^{(2)})), \ldots, (x^{(s)}, K(x^{(s)}))\}$, where $K(x^{(i)})$ is the output of the controller with respect to the state $x^{(i)}$. Then, numerical analysis methods, such as the least square method, are performed to derive the feedback gain F.

3. Observation: Monitoring the signals of the remaining system.

To protect the gain matrix F from the above attacks, a promising approach is given by the notions of *measure* and *dense set*. The definition of the latter is given as follows.

Definition 3 (Dense set) *Consider a set* $\mathbf{Q}$*. The set* $\mathbf{Q}$ *is said to be dense if the following condition is satisfied:*

$$\forall \epsilon > 0,\ \forall p \in \mathbf{Q},\ \exists q \in \mathbf{Q},\ \|p - q\|_2 < \epsilon \ \text{ s.t. } p \neq q. \tag{4.3}$$

□

Let $\mu(\mathbf{Q}, \mathbf{X})$ denote the measure of the set $\mathbf{Q}$ on the set $\mathbf{X}$. Then, the tamper-resistant controller needs to satisfy the following security requirements:

1. The gain matrix cannot be obtained from the code of the controller.

2. The control law is given by

$$u(t) = \begin{cases} -Fx(t) & x(t) \in \mathbf{Q}_t, \\ -h(x(t)) & \text{otherwise}, \end{cases} \tag{4.4}$$

   where h is an arbitrary given function such that $h(x) \neq Fx$, and $\mathbf{Q}_t \subset \mathbf{X}$ is predefined finite set such that $\mu(\mathbf{Q}_t, \mathbf{X}) = 0$ for $t \in \mathbf{N}$.

3. The set $\bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n$ is dense.

The first requirement is to protect the gain matrix F from the code analysis. The second one is to protect the controller from unauthorized use and protect the gain matrix F from numerical analysis. Since the measure of $\mathbf{Q}_t$ on $\mathbf{X}$ is zero, by sampling the states on $\mathbf{X}$, it is theoretically impossible to obtain the states in $\mathbf{Q}_t$. The third requirement corresponds to the third attack. By using the property of the dense set,

it is unattainable for the attackers to obtain the nonzero elements in $\mathbf{Q}_t$ from the observation of the elements in $\bigcup_{t=0}^{\infty} \mathbf{Q}_t$.

Then, our problem is to design a controller that satisfies the above three security requirements.

4.3 Realization of the Tamper-Resistant Controller

4.3.1 Proposed Realization Method

In this study, we propose to realize the tamper-resistant controller based on a neural network and time-varying quantization. The time-varying quantization is defined as

$$v_t(x) = \arg\min_{q_t \in \mathbf{Q}_t} \|x - q_t\|_2. \tag{4.5}$$

If we can design the sets $\mathbf{Q}_t$ for $t \in \mathbf{N}$ and train the neural network to fit (4.4), the tamper-resistant controller can be realized. However, it brings a challenge with feasibility: The neural network needs to be trained for all $\mathbf{Q}_t$ ($t \in \mathbf{N}$), which leads to a tremendous amount of computation and is difficult to implement. Thus, we propose a practical realization method, detailed as follows.

First, train the neural network to fit

$$\mathrm{NN}(x) = \begin{cases} Fx & x \in \mathbf{Q}, \\ g(x) & \text{otherwise}, \end{cases} \tag{4.6}$$

where $\mathbf{Q} \subset \mathbf{X}$ is a predefined finite set such that $\mu(\mathbf{Q}, \mathbf{X}) = 0$, and g is an arbitrary given nonlinear function such that $g(x) \neq Fx$. Next, based on the set $\mathbf{Q}$, the set $\mathbf{Q}_t$ is given by

$$\mathbf{Q}_t = \{\alpha(t)q \mid q \in \mathbf{Q}\}, \tag{4.7}$$

where $\alpha : \mathbf{N} \to \mathbf{R}_+$ is an arbitrary given function. Then, the realization of the tamper-resistant controller is shown in Fig. 4-4, where the controller is composed of the trained neural network and two signal processing units based on the function α. The control law is given by

$$u(t) = -\alpha(t)\mathrm{NN}\left(\frac{x(t)}{\alpha(t)}\right). \tag{4.8}$$

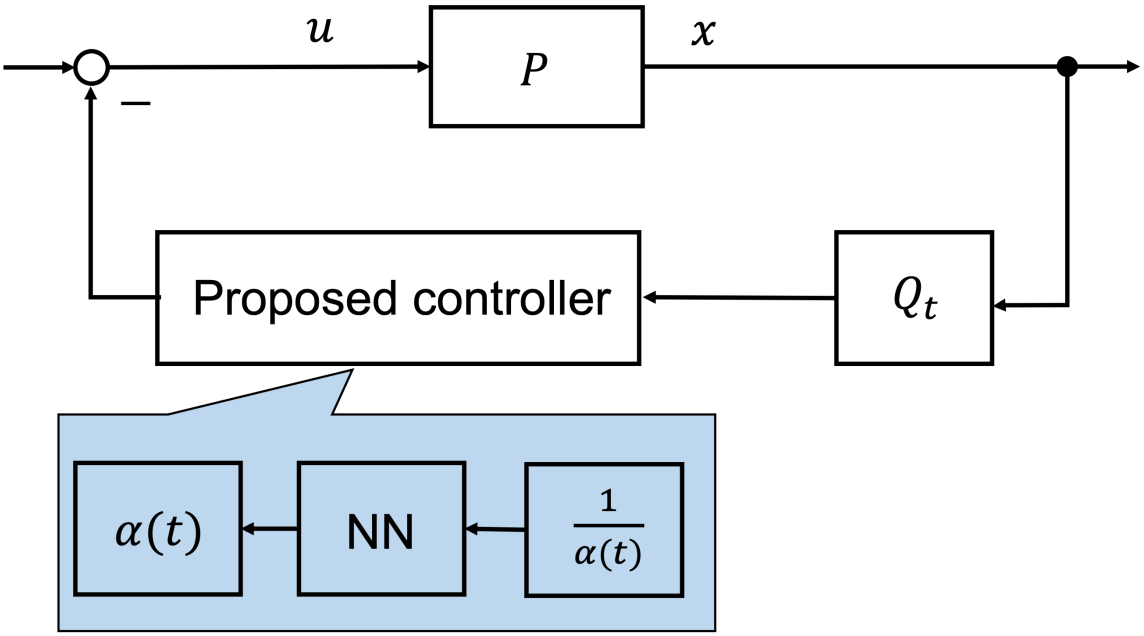


Figure 4-4: Proposed control system.

The time-varying quantizer Q_t is given by (4.5), it maps the continuous states to the elements in $\mathbf{Q}_t$. For security, the quantizer is placed in a separate location from the proposed controller.

For example, consider the control system in Fig. 4-4, where $\mathbf{Q} = \{0, 0.2, 0.4\}$. For $t = \tau$, assume that $\alpha(\tau) = 0.8$ and the state $x(\tau) = 0.3$. The signals in the proposed control system are as follows. From (4.7), we have $\mathbf{Q}_\tau = \{0, 0.16, 0.32\}$. The state is quantized by the time-varying quantizer to $v_\tau(0.3) = 0.32$. Next, the quantized state is multiplied by $\frac{1}{\alpha(\tau)}$ and mapped to an element in $\mathbf{Q}$, i.e., 0.4. Then, we have $\mathrm{NN}(0.4) = 0.4F$, and $u(\tau) = -0.32F$.

4.3.2 Tamper Resistance of the Proposed Method

In this subsection, we analyze the tamper resistance of the proposed method in terms of the three security requirements in Section 4.2.2.

For the proposed controller, since the code of the neural network only includes forward propagation, it is impossible to obtain the gain matrix F from the code. This satisfies the first security requirement.

From (4.6) and (4.8), we have that if the state x is an element of $\mathbf{Q}_t$, the controller outputs Fx; otherwise, it produces $\alpha(t)g\left(\frac{x}{\alpha(t)}\right)$. On the other hand, by the definitions of the sets $\mathbf{Q}$ and $\mathbf{Q}_t$, we have that $\mu(\mathbf{Q}_t, \mathbf{X}) = 0$ for $t \in \mathbf{N}$. They imply that the

second security requirement is satisfied.

For the third security requirement, we have the following result.

Lemma 2 *Consider a function $\alpha : \mathbf{N} \to \mathbf{R}_+$, a finite set $\mathbf{Q}$, and set $\mathbf{Q}_t$ given by (4.7). If $\{\alpha(t) \mid t \in \mathbf{N}\}$ is dense, then the set $\bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n$ is dense.*

Proof: See Appendix D. □

From Lemma 2, the third security requirement can be achieved by letting $\alpha : \mathbf{N} \to \mathbf{R}_+$ be a function such that $\{\alpha(t) \mid t \in \mathbf{N}\}$ is dense. We propose the following necessary conditions for $\{\alpha(t) \mid t \in \mathbf{N}\}$ to be dense, which facilitates the selection of α.

1. When $t \to \infty$, $\alpha(t)$ does not diverge or converge to a specific value.
2. There is no $T \in \mathbf{N}$ such that $\alpha(t+T) = \alpha(t)$ for every $t \in \mathbf{N}$.

In addition, one might consider that the function $\alpha(t)$ is directly represented in the controller, and its details can be easily obtained by the attackers after stealing the controller. However, because the knowledge of the time-varying set $\mathbf{Q}_t$ is unattainable for the attackers, they can not extract useful information (e.g., set $\mathbf{Q}$) from $\alpha(t)$. Furthermore, in a practical system, if the elements in $\mathbf{Q}_t$ are generated by a digital component, such as a digital computer, there is a quantization interval, denoted by δ, between the elements, resulting in $\bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n$ is not dense. In this case, $\bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n$ can be generated to be δ-dense, i.e.,

$$\forall p \in \bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n,\ \exists q \in \bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n,\ \|p-q\|_2 \leq \delta \ \text{ s.t. } p \neq q. \tag{4.9}$$

By setting the quantization intervals of the time-varying quantizer to be greater than δ, the attacker cannot identify the quantization intervals of the time-varying quantizer from the observation of the elements in $\bigcup_{t=0}^{\infty} \mathbf{Q}_t$, which ensures the security of the set $\mathbf{Q}_t$.

4.4 Numerical Verification

4.4.1 Simulation Setting

Consider the plant in (4.1), where

$$A = \begin{bmatrix} 1 & 2 \\ -3 & -4 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

The set of the state was defined as $\mathbf{X} = [-2, 2]^2$. The feedback gain matrix was

$$F = [\ 10 \quad 5\ ]. \tag{4.10}$$

Let $\mathbf{Q} = \{-2, -1.8, \ldots, -0.2, 0, 0.2, \ldots, 2\}^2$ and set

$$\alpha(t) = 0.05 \cos t + 0.95. \tag{4.11}$$

Then, the sets $\mathbf{Q}_t$ $(t \in \mathbf{N})$ was given by (4.7).

The training set of the neural network was constructed as follows. Let $\mathbf{S}_1 = \{(x, Fx) \mid x \in \mathbf{Q}\}$. Generate 100 and 200 elements from the uniform distribution on $\mathbf{X} \setminus \mathbf{Q}$, and let $\mathbf{M}_1$ and $\mathbf{M}_2$ denote the sets of the 100 and 200 elements, respectively. By letting

$$F_1 = [\ 5 \quad 35\ ],$$
$$F_2 = [\ 70 \quad 200\ ],$$

we set $\mathbf{S}_2 = \{(x, F_1 x) \mid x \in \mathbf{M}_1\}$ and $\mathbf{S}_3 = \{(x, F_2 x) \mid x \in \mathbf{M}_2\}$. Thus, the training set was given by $\mathbf{S} = \mathbf{S}_1 \cup \mathbf{S}_2 \cup \mathbf{S}_3$.

In this simulation, we constructed a neural network with one input layer, two hidden layers, and one output layer, with 2, 500, 500, and 1 neuron in a layer, respectively. We employed Swish function as the activation function of the neural network:

$$f(x) = \frac{x}{1 + e^{-x}}. \tag{4.12}$$

By letting $(s_1, r_1),\ (s_2, r_2),\ \ldots,\ (s_z, r_z)$ denote the elements in the training set $\mathbf{S}$, the cost function J was given by

$$J = \sqrt{\frac{1}{2z} \sum_{i=1}^{z} (r_i - \hat{r}_i)^2}, \tag{4.13}$$

where $\hat{r}_i$ denotes the output of the neural network. The Adam was set to the optimizer, where the learning rate was defined as 0.01. Batch learning was employed, and the epoch was set to two million times.

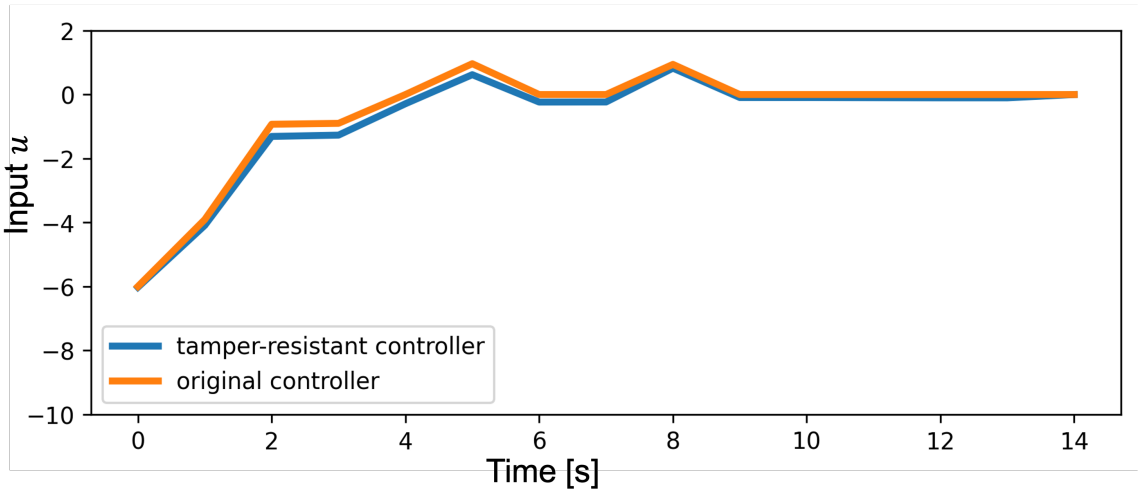


Figure 4-5: The input responses comparison of the original controller and proposed controller.

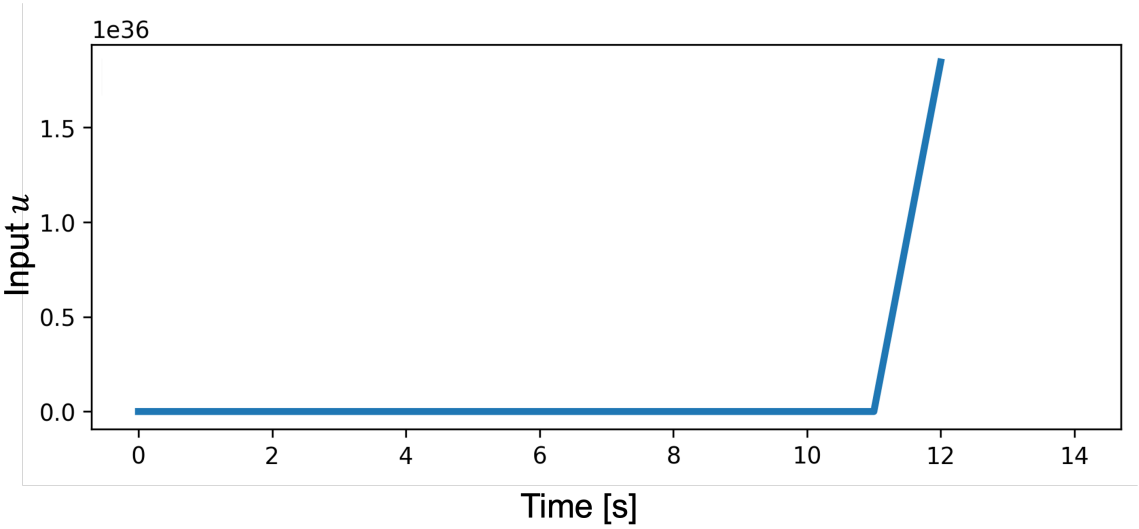


Figure 4-6: The input responses when the states are not quantized correctly.

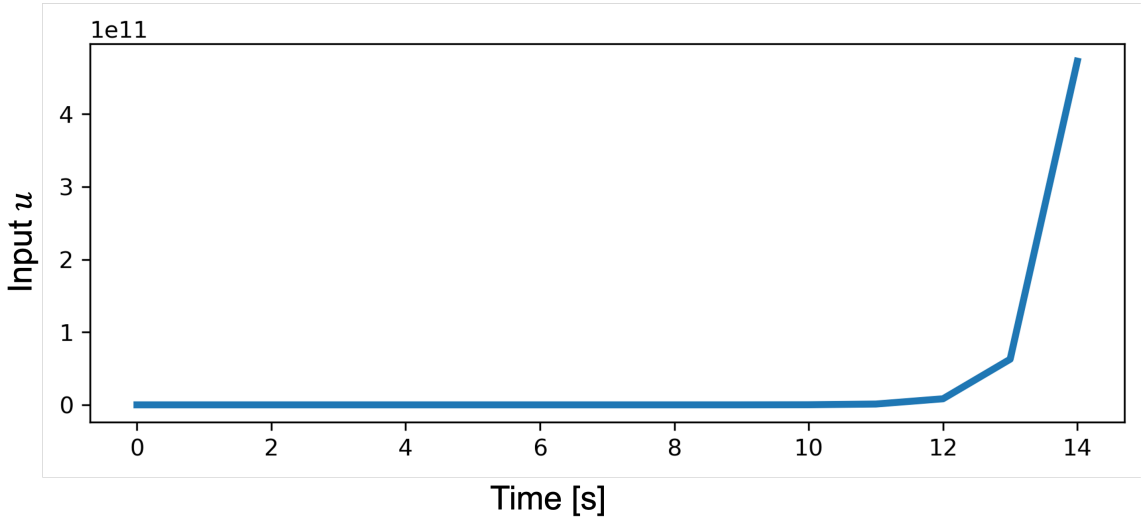


Figure 4-7: The input responses with the estimated gain.

4.4.2 Verification of the Control Performance

In this subsection, we verify the control performance of the proposed controller in terms of the input response of the system. Fig. 4-5 shows the comparison of initial value responses of the original controller and proposed controller with the initial states $x(0) = [\, 0.5 \;\; 0.5 \,]^\top$, from which we have that the performance of the original controller and the proposed controller almost coincide when $x \in \mathbf{Q}_t$.

On the other hand, when $x \notin \mathbf{Q}_t$, the controller needs to perform differently from Fx. Fig. 4-6 shows the input responses when the states are not quantized correctly. The initial responses diverged, and the controller failed to stabilize the system.

4.4.3 Verification of the Tamper Resistance

In this subsection, we verify the tamper resistance of the proposed controller by numerical analysis.

Assume that after stealing the controller, i.e., the blue box in Fig. 4-4, the attacker randomly samples 10000 states from the uniform distribution on $\mathbf{X}$, and obtains the state-input pairs $\mathbf{D} = \{(x^{(1)}, K(x^{(1)})), ..., (x^{(10000)}, K(x^{(10000)}))\}$ of the controller. To obtain F, the attacker fits the data $\mathbf{D}$ to a linear function $u = Kx$ by the least square method and gets the estimation of the gain matrix F, denoted by $\hat{K}$. The estimated gain by the above procedure is

$$\hat{K} = [\, 0.19 \;\; 69.38 \,]$$

which is far from the gain F. Fig. 4-7 shows the initial responses with the gain $\hat{K}$, it is clear that the controller with estimated gain cannot stabilize the system.

4.4.4 Verification of the Security of the Set $\mathbf{Q}_t$

In this subsection, we consider the security of the set $\mathbf{Q}_t$.

From [117], we have that $\{\cos(t)|t \in \mathbf{N}\}$ is dense, from which $\{\alpha(t) \mid t \in \mathbf{N}\}$ is dense. By the definition of $\mathbf{Q}_t$, we have that $\bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n$ is a dense set. Then, it is unattainable for the attackers to obtain the nonzero elements in $\mathbf{Q}_t$ from the observation of the elements in $\bigcup_{t=0}^{\infty} \mathbf{Q}_t$. Compared with the previous method in [65], where the elements in $\mathbf{Q}$ can be observed by the attackers directly, our method improves the tamper resistance of the controller.

4.5 Summary

In this chapter, we proposed a tamper-resistant controller in CPSs. If the state is an element of a time-varying set, the controller outputs the same value as the original controller; otherwise, it produces a different value from the original controller, where the measure of the time-varying set in the set of continuous states is zero. We designed the time-varying set elaborately such that the union of the sets over time is a dense set. By using the property of a dense set, the information of the time-varying set is unattainable for the attackers from the observation of the signals. Furthermore, since the measure of the time-varying set in the set of continuous states is zero, without the information of the time-varying set, the probability of an attacker obtaining the information of the controller is theoretically zero. The tamper-resistant controller is achieved by a neural network and time-varying quantization.

Chapter 5

Conclusion

In this thesis, we proposed a solution to improve the resilience of the CPSs, which consists of an anomaly detection framework and tamper-resistant control for a CPS.

We proposed a generalized anomaly detection framework that iterates sparse reconstruction and sequential measurement. The detection method can detect the anomalies exactly with a small number of measurements, which is expected to be applied to a variety of CPSs. In this thesis, we presented the applications of the detection framework in the case of there is no prior knowledge and there is prior knowledge, using the examples of network systems and demand response of smart grids, respectively. Furthermore, we developed a termination condition for the iterative detection algorithm that allows the algorithm to terminate after a few sequential measurements and locate the anomalies with guaranteed exactness.

Then, we proposed a framework of tamper-resistant control in CPSs, which can handle physical attacks on the controller, such as stealing the entity or copying the code of the controller. The tamper-resistant controller outputs the same values as the original controller if the state is an element of a finite time-varying quantized set; otherwise, it produces a different value from the original controller. By designing the time-varying set elaborately, the union of the sets over time is a dense set. By using the property of a dense set, the attackers cannot obtain the information of the time-varying set by observing the signals of the system. Furthermore, since the measure of the time-varying set in the set of continuous states is zero, without the information of the time-varying set, the probability of an attacker obtaining the information of the controller is theoretically zero. In this thesis, we realized the tamper-resistant controller by a neural network and time-varying quantization.

We have not considered the effect of the measurement noise in anomaly detection. In addition, in some systems, the states are discrete, resulting in the measure of the time-varying set in the set of discrete states is not zero. This has the potential to

affect the tamper resistance of the proposed controller. Therefore, further studies should be conducted to address these cases.

Appendix A

Proof of Theorem 1

In this chapter, we prove Theorem 1.

Table A.1 summarizes the notation to be used in the proof with respect to the number of nonzero elements in matrix C.

A.1 Theorem 1.1: Deriving $m^*(n, f)$

A.1.1 Preparation

From [76, 118], we have the following lemmas.

Lemma 3 *Consider a binary correlation matrix $C \in \{0,1\}^{m\times n}$. Let $d_{ri}(C)$ and $d_{cj}(C)$ denote the number of nonzero elements in the i-th row and j-th column vector of C, respectively. Let $\bar{d}_r(C)$ and $\bar{d}_c(C)$ denote the average of the number of nonzero elements in per row and column in C, respectively. Let $p(C) = \min_{i\in\{1,2,\ldots,m\}} d_{ri}(C)$. If $d(C) \geq 2$ and $p(C) \geq 2$, then*

$$m \geq \sum_{k=0}^{2} \left(\left(\bar{d}_c(C) - 1\right)^{\lceil \frac{k}{2} \rceil} \left(\bar{d}_r(C) - 1\right)^{\lfloor \frac{k}{2} \rfloor} \right). \tag{A.1}$$

□

Table A.1: Summary of notations about the number of nonzero elements in $C \in \{0,1\}^{m\times n}$

Notation	Meaning
$d_{cj}(C)$	Number of nonzero elements in the j-th column vector of C
$d_{ri}(C)$	Number of nonzero elements in the i-th row vector of C
$\bar{d}_c(C)$	Average number of nonzero elements in a column in C
$\bar{d}_r(C)$	Average number of nonzero elements in a row in C
$d(C)$	Minimum number of nonzero elements in a column of C, i.e., $\min_{j\in\{1,2,\ldots,n\}} \|c_j\|_2 = \min_{j\in\{1,2,\ldots,n\}} d_{cj}(C)$
$p(C)$	Minimum number of nonzero elements in a row of C, i.e., $\min_{i\in\{1,2,\ldots,m\}} d_{ri}(C)$

For example, consider a binary correlation matrix

$$C = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}, \tag{A.2}$$

in which $m = 6$, $n = 7$, $\bar{d}_c(C) = 2$, and $\bar{d}_r(C) = \frac{7}{3}$. The relation in (A.1) holds.

Lemma 4 *Consider three positive integers d_r, d_c, and m. If*

$$\frac{\log\left(md_r - \frac{md_r}{d_c} - m + 1\right)}{\log\left((d_r-1)(d_c-1)\right)} - 1 \geq 1, \tag{A.3}$$

then there exist an $m \times n$ binary correlation matrix with

$$\max_{i\in\{1,2,\ldots,m\}} d_{ri}(C) = d_r, \tag{A.4}$$

$$\max_{j\in\{1,2,\ldots,n\}} d_{cj}(C) = d_c. \tag{A.5}$$

□

For example, consider $d_r = 3$ and $d_c = 2$, there exists a binary correlation matrix in $\{0,1\}^{6\times 7}$ as shown in (A.2).

A.1.2 Proof

Let $\mathbf{C}(n, f) = \{C \in \bigcup_{i=1}^{n} \{0,1\}^{i \times n} \mid C$ is a binary correlation matrix that satisfies (2.5)$\}$, and let

$$d_{min} = \min_{C \in \mathbf{C}(n,f)} d(C). \tag{A.6}$$

By the definition of $\mathbf{C}(n, f)$ and $m^*(n, f)$, it is clear that

$$m^*(n, f) = \min_{C \in \mathbf{C}(n,f)} m(C). \tag{A.7}$$

Now, consider a matrix $C \in \mathbf{C}(n, f)$. Because $d(C) \in \mathbf{Z}_+$, we have

$$d(C) \geq f + 1. \tag{A.8}$$

Therefore,

$$d_{min} = f + 1. \tag{A.9}$$

Then, the statement 1 of Theorem 1 is the consequence of (A.9) and the following two facts:
(a) $m^*(n, f) \geq \left\lceil \sqrt{d_{min} n(d_{min} - 1) + \frac{1}{4}} + \frac{1}{2} \right\rceil$, the equality holds if there is an $m \times n$ binary correlation matrix C with $m = \left\lceil \sqrt{d_{min} n(d_{min} - 1) + \frac{1}{4}} + \frac{1}{2} \right\rceil$ and $d(C) = d_{min}$.
(b) $m^*(n, f) \leq \left\lceil d_{min} \sqrt{n(d_{min} - 1) + \frac{1}{4}} + \frac{1}{2} d_{min} \right\rceil$.
Facts (a) and (b) are proved as follows.

Proof of (a): Consider an $m \times n$ matrix $C \in \mathbf{C}(n, f)$ with $d(C) \geq 2$ and $p(C) \geq 2$. Then

$$\bar{d}_c(C) \geq d(C), \tag{A.10}$$

$$\bar{d}_r(C) \geq \frac{n d(C)}{m}. \tag{A.11}$$

From (A.1) in Lemma 3, we have

$$m \geq \sqrt{d(C) n(d(C) - 1) + \frac{1}{4}} + \frac{1}{2}, \tag{A.12}$$

from which we have that a small $d(C)$ improves the bound of m. Because d_{min} is the smallest integer that satisfies (2.5), then by regarding d_{min} as $d(C)$ in (A.12), from Lemma 1, we have the inequation in fact (a). Next, consider an $m \times n$ binary

correlation matrix C with $m = \left\lceil \sqrt{d_{min} n(d_{min}-1) + \frac{1}{4}} + \frac{1}{2} \right\rceil$ and $d(C) = d_{min}$. It is clear that the matrix $C \in \mathbf{C}(n, f)$. Then, we have fact (a).

Proof of (b): The condition in (A.3) can be expressed as

$$m \geq d_c + d_c(d_c - 1)(d_r - 1), \tag{A.13}$$

from which small values of d_r and d_c improve the bound of m. Consider a binary correlation matrix $C \in \{0,1\}^{m \times n}$ with

$$d_{c1}(C) = d_{c2}(C) = \cdots = d_{cn}(C) = d_c, \tag{A.14}$$

$$\max_{i \in \{1,2,\ldots,m\}} d_{ri}(C) \leq \left\lceil \frac{n d_c}{m} \right\rceil. \tag{A.15}$$

From Lemma 4, if

$$m \geq d_c \sqrt{n(d_c - 1) + \frac{1}{4}} + \frac{1}{2} d_c, \tag{A.16}$$

holds, then there exist such a binary correlation matrix C. Therefore, by regarding d_{min} as d_c in (A.16), if

$$m \geq d_{min} \sqrt{n(d_{min} - 1) + \frac{1}{4}} + \frac{1}{2} d_{min}, \tag{A.17}$$

then there exist an $m \times n$ matrix $C \in \mathbf{C}(n, f)$. This proves fact (b).

A.2 Theorem 1.2: Finding $\mathcal{G}^*$

A.2.1 Preparation

From [119, 120], we have the following lemma.

Lemma 5 *Consider a graph $\mathcal{G} = (\mathbf{V}, \mathbf{E})$ with n nodes and a nonnegative integer p. If*

$$\delta(\mathcal{G}) \geq n - \frac{p}{2}, \tag{A.18}$$

then for each set of nodes $\mathbf{P} \subseteq \mathbf{V}$ such that $|\mathbf{P}| \geq p$, the subgraph of $\mathcal{G}$ induced by $\mathbf{P}$ has a Hamiltonian path. □

A.2.2 Proof

The statement 2 of Theorem 1 is the consequence of the following two facts:
(c) Consider a network $\mathcal{G} \in \mathbf{G}(n)$ and a matrix $C \in \{0,1\}^{m\times n}$. If

$$\delta(\mathcal{G}) \geq n - \frac{p(C)}{2}, \tag{A.19}$$

then $C \in \mathbf{C}(\mathcal{G})$.
(d) There is an $m^*(n,f) \times n$ matrix $C \in \mathbf{C}(n,f)$ with

$$p(C) \geq \left\lfloor \frac{n(f+1)}{m^+} \right\rfloor. \tag{A.20}$$

Facts (c) and (d) are proved as follows.

Proof of (c): Consider a matrix $C \in \{0,1\}^{m\times n}$, and set it to the measurement matrix of network $\mathcal{G} \in \mathbf{G}(n)$. Let $\mathbf{T}_i(C) = \{v_j \in \mathbf{V} \mid c_{ij} = 1\}$. In other words, $\mathbf{T}_i(C)$ denotes the set of the nodes to be measured by probe i. Then, we have

$$|\mathbf{T}_i(C)| \geq p(C) \ (i = 1, 2, \ldots, m). \tag{A.21}$$

From Lemma 5 and (A.21), if (A.19) holds, there is a Hamiltonian path in $\mathcal{G}_{\mathbf{T}_i(C)}$ $(i = 1, 2, \ldots, m)$. It implies that the manager can send m probe along the m Hamiltonian paths and the measurement results are given by (2.1). Therefore, the matrix C is feasible in the network $\mathcal{G}$, i.e., $C \in \mathbf{C}(\mathcal{G})$. This proves fact (c).

Proof of (d): From [77], there is an $m^*(n,f) \times n$ matrix $C \in \mathbf{C}(n,f)$ with

$$d(C) = d_{min} \tag{A.22}$$

$$p(C) = \left\lfloor \frac{n\bar{d}_c(C)}{m^*(n,f)} \right\rfloor. \tag{A.23}$$

From (A.9), it is clear that

$$\bar{d}_c(C) \geq f + 1 \tag{A.24}$$

Then, from (A.23) and (A.24), the matrix C has

$$p(C) \geq \left\lfloor \frac{n(f+1)}{m^*(n,f)} \right\rfloor. \tag{A.25}$$

Therefore, fact (b) and (A.25) complete the proof.

A.3 Theorem 1.3

In this section, we find an f-identifiable measurement matrix for network $\mathcal{G}^*$.

From (A.9), facts (c) and (d), there is a binary correlation matrix $C \in \{0,1\}^{m^*(n,f)\times n}$ with $d(C) = f + 1$ in $\mathbf{C}(\mathcal{G}^*)$. From Lemma 1, it is clear that the matrix C is f-identifiable. This completes the proof of Theorem 1.3.

Appendix B

Proof of Theorem 2

Let τ represents the iteration number t when $r(t) = 0$, i.e., $r(\tau) = 0$. Let $\bar{\mathbf{L}}(t) = \{1, 2, \ldots, n\} \setminus \mathbf{L}(t)$, and it is clear that

$$\bar{\mathbf{L}}(\tau) \cup \mathbf{L}(\tau) = \{1, 2, \ldots, n\}, \tag{B.1}$$

$$\bar{\mathbf{L}}(\tau) \cap \mathbf{L}(\tau) = \emptyset. \tag{B.2}$$

Then, the statement of Theorem 2 is the consequence of the following three facts:
(a) For each $j \in \bar{\mathbf{L}}(\tau)$, $l^*(v_j) = l_j(\tau)$.
(b) For each $j \in \mathbf{L}(\tau)$, $l_j(\tau) = 0$.
(c) For each $j \in \mathbf{L}(\tau)$, $l^*(v_j) = 0$.

Next, we prove the three facts, respectively.

Proof of (a): By the definitions of $\mathbf{L}(\tau)$ and $l(\tau)$, we have that $l^*(v_j) = l_j(\tau)$ for each $j \notin \mathbf{L}(\tau)$. Then, from (B.1) and (B.2), we have fact (a).

Proof of (b): Fact (b) follows directly from the definition of $l(\tau)$.

Proof of (c): Let $r_i(t)$ denote the i-th element of $r(t)$. From the definition of $r(t)$, we have

$$r_i(t) = y_i - \sum_{j \in \mathbf{P}_i} l_j(t) \tag{B.3}$$

for each $i \in \{1, 2, \ldots, m\}$. Since $r(\tau) = 0$, then

$$y_i = \sum_{j \in \mathbf{P}_i} l_j(\tau) = \sum_{j \in \mathbf{P}_i \cap \bar{\mathbf{L}}(\tau)} l_j(\tau) + \sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l_j(\tau) \tag{B.4}$$

for each $i \in \{1, 2, \ldots, m\}$. On the other hand, by the definition of $l^*(v_j)$, it is clear

that

$$y_i = \sum_{j \in \mathbf{P}_i} l^*(v_j) = \sum_{j \in \mathbf{P}_i \cap \bar{\mathbf{L}}(\tau)} l^*(v_j) + \sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l^*(v_j) \tag{B.5}$$

holds for all $i \in \{1, 2, \ldots, m\}$. From (B.4) and (B.5), we have that for each $i \in \{1, 2, \ldots, m\}$,

$$\sum_{j \in \mathbf{P}_i \cap \bar{\mathbf{L}}(\tau)} l^*(v_j) + \sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l^*(v_j) = \sum_{j \in \mathbf{P}_i \cap \bar{\mathbf{L}}(\tau)} l_j(\tau) + \sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l_j(\tau). \tag{B.6}$$

Then, from fact (a) and (C.1), we have

$$\sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l^*(v_j) = \sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l_j(\tau) \tag{B.7}$$

for each $i \in \{1, 2, \ldots, m\}$, which implies that

$$\sum_{i=1}^{m} \left(\sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l^*(v_j) \right) = \sum_{i=1}^{m} \left(\sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l_j(\tau) \right). \tag{B.8}$$

According to fact (b) and (C.4), we have

$$\sum_{i=1}^{m} \left(\sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l^*(v_j) \right) = 0. \tag{B.9}$$

Since

$$\bigcup_{i=1}^{m} \mathbf{P}_i = \{1, 2, \ldots, n\}, \tag{B.10}$$

then

$$\sum_{i=1}^{m} \left(\sum_{j \in \mathbf{P}_i \cap \mathbf{L}(\tau)} l^*(v_j) \right) \geq \sum_{j \in \mathbf{L}(\tau)} l^*(v_j). \tag{B.11}$$

Since $x^* \in [0, \infty)^n$ and (B.9), we have fact (c).

Appendix C

Proof of Theorem 3

Let $x^*_{ij} \in [0,1]$ be the true value of the anomaly rate of participant i at time slot j, and let $\bar{\mathbf{P}}(t) := \{1,2,\ldots,n\} \setminus \mathbf{P}(t)$, which is the list of the participants whose smart meter has been inspected until the t-th iteration in the algorithm. Furthermore, we use τ to represent the iteration number t when $x_{i(t)} = 0$, i.e., $x_{i(\tau)} = 0$.

The following four facts hold for τ:
(a) $x_{ij}(\tau) = 0 \ \ (j = 1,2,...,m)$ for every $i \in \mathbf{P}(\tau)$.
(b) $x_{ij}(\tau) = x^*_{ij} \ \ (j = 1,2,...,m)$ for every $i \in \bar{\mathbf{P}}(\tau)$.
(c) The following relation holds:

$$\sum_{i \in \mathbf{P}(\tau)} c_{ij}(1 - x^*_{ij}) + \sum_{i \in \bar{\mathbf{P}}(\tau)} c_{ij}(1 - x^*_{ij}) = s_j \ \ (j = 1,2,...,m).$$

(d) The modified version of (c) holds:

$$\sum_{i \in \mathbf{P}(\tau)} c_{ij}(1 - x_{ij}(\tau)) + \sum_{i \in \bar{\mathbf{P}}(\tau)} c_{ij}(1 - x_{ij}(\tau)) = s_j \ \ (j = 1,2,...,m).$$

Facts (a) and (b) are trivial from the definitions of $\mathbf{P}(t)$, $\bar{\mathbf{P}}(t)$, τ, and $i(t)$, while (c) and (d) are given by (3.1), the definitions of $\mathbf{P}(t)$ and $\bar{\mathbf{P}}(t)$ (in particular, the list $\{1,2,\ldots,n\}$ of the participants is divided into $\mathbf{P}(t)$ and $\bar{\mathbf{P}}(t)$), and the fact that $x(t)$ is a solution to the optimization problem OP(t) for the linear equation in (3.1).

By using (a)–(d), we now prove
(e) $x_{ij}(\tau) = x^*_{ij} \ \ (j = 1,2,...,m)$ for every $i \in \mathbf{P}(\tau)$
because (b) and (e) imply the consequence of Theorem 3.

Suppose that $j \in \{1,2,...,m\}$ is arbitrarily given. From (a), (b), and (d), we

obtain

$$\sum_{i\in\mathbf{P}(\tau)} c_{ij} + \sum_{i\in\bar{\mathbf{P}}(\tau)} c_{ij}(1-x^*_{ij}) = s_j, \tag{C.1}$$

which, together with (c), provides

$$\sum_{i\in\mathbf{P}(\tau)} c_{ij}(1-x^*_{ij}) - \sum_{i\in\mathbf{P}(\tau)} c_{ij} = 0, \tag{C.2}$$

i.e.,

$$\sum_{i\in\mathbf{P}(\tau)} c_{ij}x^*_{ij} = 0. \tag{C.3}$$

Since $c_{ij} > 0$ and $x^*_{ij} \geq 0$ $(i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m)$, it follows from (C.3) that

$$x^*_{ij} = 0 \ (j = 1, 2, ..., m) \quad (\forall i \in \mathbf{P}(\tau)). \tag{C.4}$$

This and (a) prove (e).

Appendix D

Proof of Lemma 2

Let $\mathbf{A} = \{\alpha(t) \mid t \in \mathbf{N}\}$. Since $\mathbf{A}$ is dense, we have that

$$\forall \epsilon > 0,\ \forall a \in \mathbf{A},\ \exists a' \in \mathbf{A},\ \|a - a'\|_2 < \epsilon \ \text{ s.t. } a \neq a'. \tag{D.1}$$

Then,

$$\forall \delta > 0,\ \forall a \in \mathbf{A},\ \forall q \in \mathbf{Q},\ \exists a' \in \mathbf{A},\ \|qa - qa'\|_2 < \delta \ \text{ s.t. } a \neq a'. \tag{D.2}$$

In other words, by letting $\mathbf{Q}_\Sigma = \bigcup_{t=0}^{\infty} \mathbf{Q}_t \setminus \{0\}^n$,

$$\forall \delta > 0,\ \forall p \in \mathbf{Q}_\Sigma,\ \exists p' \in \mathbf{Q}_\Sigma,\ \|p - p'\|_2 < \delta \ \text{ s.t. } p \neq p'. \tag{D.3}$$

This complete the proof.

Acknowledgment

I would like to express my gratitude to all those who have helped me.

First of all, I would like to express my deepest gratitude to my advisor, Prof. Azuma Shun-ichi, for his guidance, support, and help throughout my master's and doctoral journey. His expertise, constructive feedback, and kind guidance have shaped not only this thesis but also my growth as a researcher. I am truly fortunate to have been his student!

I extend my appreciation to Prof. Asai Toru for his enlightening advice and great seminars in these years of study. I want to express my thanks to Prof. Ariizumi Ryo for his generous help and kind guidance over these years.

Thanks to Prof. Azuma Shun-ichi, Prof. Asai Toru, Prof. Matsumoto Toshiro, Prof. Takeuchi Ichiro, and Prof. Izumi Shinsaku. Their kind comments and constructive suggestions significantly improve the quality of this thesis.

I am grateful to Nagoya University for providing a comfortable learning environment, where I have spent six years in quiet and peaceful. My heartfelt thanks go to my friends and schoolmates for their accompany and support.

Thanks to my country for financial support, thanks China Scholarship Council.

Finally, I want to thank my family, especially my grandfather and mother, who have always encouraged and supported me. Their encouragement, love, and support have been a constant source of my strength. I am grateful to my cat and chinchilla, Rika and Pepper, for their psychosocial support.

Bibliography

[1] R. Baheti and H. Gill, "Cyber-physical systems," *The Impact of Control Technology*, vol. 12, no. 1, pp. 161–166, 2011.

[2] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.

[3] N. Jazdi, "Cyber physical systems in the context of Industry 4.0," in *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, Cluj-Napoca, Romania, 2014, pp. 1–4.

[4] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27–40, 2017.

[5] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, and K. Ueda, "Cyber-physical systems in manufacturing," *CIRP Annals*, vol. 65, no. 2, pp. 621–641, 2016.

[6] S. Karnouskos, "Cyber-physical systems in the smartgrid," in *2011 9th IEEE International Conference on Industrial Informatics*, Lisbon, Portugal, 2011, pp. 20–23.

[7] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proceedings of the 47th Design Automation Conference*, New York, NY, USA, 2010, pp. 731–736.

[8] T. Sanislav and L. Miclea, "Cyber-physical systems-concept, challenges and research areas," *Journal of Control Engineering and Applied Informatics*, vol. 14, no. 2, pp. 28–33, 2012.

[9] E. A. Lee and S. A. Seshia, *Introduction to Embedded Systems, A Cyber-Physical Systems Approach*, Second Edition, MIT Press, ISBN 978-0-262-53381-2, 2017.

[10] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, Orlando, FL, USA, 2008, pp. 363-369.

[11] A. V. Jha, B. Appasani, A. N. Ghazali, P. Pattanayak, D. S. Gurjar, E. Kabalci, and D. K. Mohanta, "Smart grid cyber-physical systems: Communication technologies, standards and challenges," *Wireless Networks*, vol. 27, pp. 2595–2613, 2021.

[12] S. Zanero, "Cyber-physical systems," *Computer*, vol. 50, no. 4, pp. 14–16, 2017.

[13] K. J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," *Computer Communications*, vol. 36, no. 1, pp. 1–7, 2012.

[14] K. D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, 2012.

[15] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 12, pp. 4242–4268, 2014.

[16] M. Sadiku, Y. Wang, S. Cui, and S. M. Musa, "Cyber-physical systems: A literature review," *European Scientific Journal*, vol. 13, no. 36, pp. 52–58, 2017.

[17] M. Hamzah, M. M. Islam, S. Hassan, M. N. Akhtar, M. J. Ferdous, M. B. Jasser, and A. W. Mohamed, "Distributed control of cyber physical system on various domains: A critical review," *Systems*, vo. 11, no. 4, pp. 208, 2023.

[18] K. Thramboulidis, "A cyber–physical system-based approach for industrial automation systems," *Computers in Industry*, vol. 72, pp. 92–102, 2015.

[19] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. S. Tavares, "Medical cyber-physical systems: A survey," *Journal of Medical Systems*, vol. 42, pp. 1–13, 2018.

[20] S. A. Haque, S. M. Aziz, and M. Rahman, "Review of cyber-physical system in healthcare," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, pp. 217415, 2014.

[21] D. B. Rawat, C. Bajracharya, and G. Yan, "Towards intelligent transportation Cyber-Physical Systems: Real-time computing and communications perspectives," in *SoutheastCon 2015*, Fort Lauderdale, FL, USA, 2015, pp. 1-6.

[22] Y. W. Ma, J. L. Chen, Y. M. Huang, and M. Y. Lee, "An efficient management system for wireless sensor networks," *Sensors (Basel)*, vol. 10, no. 12, pp. 11400–11413, 2010.

[23] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *ACM International Conference on Wireless Sensor Networks and Applications*, New York, NY, USA, 2002, pp. 122–130.

[24] National Intelligence Council, "Disruptive civil technologies: Six technologies with potential impacts on US interests out to 2025," Conference Report CR 2008-07, 2008.

[25] European Commission, "Horizon2020," [Online]. Available: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en

[26] M. Fukuyama, "Society 5.0: Aiming for a new human-centered society," *Japan Spotlight*, vol. 27, no. 5, pp. 47–50, 2018.

[27] S. Colabianchi, F. Costantino, G. D. Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Computers & Industrial Engineering*, vol. 160, pp. 107534, 2021,

[28] F. Hu, Y. Lu, A. V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, and N. N. Xiong, "Robust cyber–physical systems: Concept, models, and implementation," *Future Generation Computer Systems*, vol. 56, pp. 449–475, 2016.

[29] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber-resilient systems: A systems security engineering approach" *NIST Special Publication 800-160*, vol. 2, 2021.

[30] G. Murino, A. Armando, and A. Tacchella, "Resilience of cyber-physical systems: An experimental appraisal of quantitative measures," in *2019 11th International Conference on Cyber Conflict*, Tallinn, Estonia, 2019, pp. 1–19.

[31] S. Talukder, M. Ibrahim, and R. Kumar, "Resilience indices for power/cyberphysical systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 4, pp. 2159–2172, 2021.

[32] F. Januário, A. Cardoso, and P. Gil, "A distributed multi-agent framework for resilience enhancement in cyber-physical systems," *IEEE Access*, vol. 7, pp. 31342–31357, 2019.

[33] L. Xu, Q. Guo, Y. Sheng, S. M. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renewable and Sustainable Energy Reviews*, vol. 152, pp. 111642, 2021.

[34] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, and E. Bartocci, "A roadmap toward the resilient internet of things for cyber-physical systems," *IEEE Access*, vol. 7, pp. 13260–13283, 2019.

[35] D. Silvestre, J. Hespanha, and C. Silvestre, "Fault detection for cyber-physical systems: Smart grid case," in *23rd International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, 2018, pp. 475–481.

[36] N. Oliveira, N. Sousa, J. Oliveira, and I. Praça, "Anomaly detection in cyber-physical systems: Reconstruction of a prediction error feature space," in *2021 14th International Conference on Security of Information and Networks (SIN)*, Edinburgh, United Kingdom, 2021, pp. 1–5.

[37] R. N. Jadoon, A. A. Awan, M. A. Khan, W. Y. Zhou, and A. Shahzad, "An efficient nodes failure recovery management algorithm for mobile sensor networks," *Mathematical Problems in Engineering*, vol. 2020, no. 1749467, pp. 1–14, 2020.

[38] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, 2002, pp. 122–130.

[39] A. Guo, D. Yu, H. Du, Y. Hu, Z. Yin, and H. Li, "Cyber-physical failure detection system: Survey and implementation," in *2016 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, Chengdu, China, 2016, pp. 428–432.

[40] Á. L. P. Gómez, L. F. Maimó, A. H. Celdrán, and F. J. G. Clemente, "MADICS: A methodology for anomaly detection in industrial control systems," *Symmetry*, vol. 12, no. 10, pp. 1583, 2020.

[41] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 104–111, 2015.

[42] L. Ma, T. He, A. Swami, D. Towsley, and K. K. Leung, "Network capability in localizing node failures via end-to-end path measurements," *IEEE/ACM Transactions on Networking*, vol. 25, no. 1, pp. 434–450, 2017.

[43] J. Tapolcai, L. Rónyai, È. Hosszu, P. -H. Ho, and S. Subramaniam, "Signaling free localization of node failures in all-optical networks," *IEEE Transactions on Communications*, vol. 64, no. 6, pp. 2527–2538, 2016.

[44] W. Xu, M. Wang, E. Mallada, and A. Tang, "Recent results on sparse recovery over graphs," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Pacific Grove, CA, USA, 2011, pp. 413–417.

[45] D. L. Donoho, "Compressed Sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[46] I. Rish and G. Grabarnik, *Sparse Modeling: Theory, Algorithms, and Applications*, CRC Press, 2014.

[47] M. F. Duarte and Y. C. Eldar, "Structured compressed sensing: From theory to applications," *IEEE Transactions on Signal Processing*, vol. 59, no. 9, pp. 4053–4085, 2011.

[48] M. Elad, "Optimized projections for compressed sensing," *IEEE Transactions on Signal Processing*, vol. 55, no. 12, pp. 5695–5702, 2007.

[49] S. J. Wright, R. D. Nowak, and M. A. T. Figueiredo, "Sparse reconstruction by separable approximation," *IEEE Transactions on Signal Processing*, vol. 57, no. 7, pp. 2479–2493, 2009.

[50] M. A. T. Figueiredo, R. D. Nowak, and S. J. Wright, "Gradient projection for sparse reconstruction: Application to compressed sensing and other inverse problems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 1, no. 4, pp. 586–597, 2007.

[51] M. Lustig, D. L. Donoho, J. M. Santos, and J. M. Pauly, "Compressed sensing MRI," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 72–82, 2008.

[52] M. Wang, W. Xu, E. Mallada, and A. Tang, "Sparse recovery with graph constraints," *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 1028–1044, 2015.

[53] M. Cheraghchi, A. Karbasi, S. Mohajer, and V. Saligrama, "Graph-constrained group testing," *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 248–262, 2012.

[54] W. Xu, E. Mallada, and A. Tang, "Compressive sensing over graphs," in *2011 Proceedings IEEE INFOCOM*, Shanghai, China, 2011, pp. 2087–2095.

[55] M. Aldridge, O. Johnson, J. Scarlett, "Group testing: An information theory perspective," *Foundations and Trends in Communications and Information Theory*, vol. 15, no. 3–4, pp. 196–392, 2019.

[56] D. Du and F. K. Hwang, *Combinatorial group testing and its applications*, Singapore: World Scientific, 2000.

[57] A. C. Gilbert, M. A. Iwenm, and M. J. Strauss, "Group testing and sparse signal recovery," in *2008 42nd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2008, pp. 1059–1063.

[58] C. L. Chan, S. Jaggi, V. Saligrama, and S. Agnihotri, "Non-adaptive group testing: Explicit bounds and novel algorithms," *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 3019–3035, 2014.

[59] E. Porat and A. Rothschild, "Explicit nonadaptive combinatorial group testing schemes," *IEEE Transactions on Information Theory*, vol. 57, no. 12, pp. 7982–7989, 2011.

[60] S. Azuma, D. Sato, K. Kobayashi, and N. Yamaguchi, "Detection of defaulting participants of demand response based on sparse reconstruction," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 368–378, 2020.

[61] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual Reviews in Control*, vol. 47, pp. 394–411, 2019.

[62] M. S. Hossain, M. H. Rahman, M. S. Rahman, A. S. M. S. Hosen, C. Seo, and G. H. Cho, "Intellectual property theft protection in IoT based precision agriculture using SDN," *Electronics*, vol. 10, no. 16, pp. 1987, 2021.

[63] X. Qiu, F. Cheng, W. Wang, G. Zhang, and Y. Qiu, "A security controller-based software defined security architecture," in *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, Paris, France, 2017, pp. 191–195.

[64] X. Wang, R. Habeeb, X. Ou, S. Amaravadi, J. Hatcliff, M. Mizuno, M. Neilsen, S. R. Rajagopalan, and S. Varadarajan, "Enhanced security of building automation systems through microkernel-based controller platforms," in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Atlanta, GA, USA, 2017, pp. 37–44.

[65] T. Takayama, R. Ariizumi, S. Azuma, T. Asai, and M. Tanemura, "Tamper resistant controller with neural network," in *The 63rd Annual Conference of the Institute of Systems, Control and Information Engineers*, Osaka, Japan, 2019 (in Japanese).

[66] H. Goto, M. Mambo, K. Matsumura, and H. Shizuya, "An approach to the objective and quantitative evaluation of tamper-resistant software," in *Information Security: Third International Workshop*, ISW 2000 Wollongong, Australia, 2000, Proceedings 3, pp. 82–96.

[67] F. Xu, S. Azuma, R. Ariizumi, and T. Asai, "Performance limitation of group testing in network failure detection," *IEEE Access*, vol. 11, pp. 102852–102859, 2023.

[68] J. L. Gross, J. Yellen, and M. Anderson, *Graph Theory and Its Applications*, New York, NY, USA: Chapman and Hall CRC, 2018.

[69] M. Subramanian, T. A. Gonsalves, and N. U. Rani, *Network Management: Principles and Practice*. New Delhi, India: Dorling Kindersley (India) Pvt. Ltd, 2010.

[70] Y. K. Joshi and M. Younis, "Autonomous recovery from multi-node failure in wireless sensor network," in *2012 IEEE GLOBECOM*, Anaheim, CA, USA, 2012, pp. 652–657.

[71] M. Younis, I. F. Senturk, K. Akkaya, S. Lee, and F. Senel, "Topology management techniques for tolerating node failures in wireless sensor networks: A survey," *Computer Network*, vol. 58, pp. 254–283, 2014.

[72] S. Perumal, M. Tabassum, G. Narayana, S. Ponnan, C. Chakraborty, S. Mohanan, Z. Basit, and M. T. Quasim, "ANN based novel approach to detect node failure in wireless sensor network," *Computers, Materials and Continua*, vol. 69, no. 2, pp. 1447–1462, 2021.

[73] F. Tong, L. Li, H. Peng, and Y. Yang, "Flexible construction of compressed sensing matrices with low storage space and low coherence," *Signal Processing*, vol. 182, pp. 107951, 2021.

[74] W. Lu, T. Dai, and S. T. Xia, "Compressed sensing performance of binary matrices with binary column correlations," in *2017 Data Compression Conference (DCC)*, Snowbird, UT, USA, 2017, pp. 151–160.

[75] W. Lu, K. Kpalma, and J. Ronsin, "Sparse binary matrices of LDPC codes for compressed sensing," in *2012 Data Compression Conference*, Snowbird, UT, USA, 2012, pp. 405–405.

[76] X. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386–398, 2005.

[77] H. Chen and Z. Cao, "A modified PEG algorithm for construction of LDPC codes with strictly concentrated check-node degree distributions," in *2007 IEEE Wireless Communications and Networking Conference*, Hong Kong, China, 2007, pp. 564–568.

[78] R. J. Wilson, *Introduction to graph theory*, Harlow, UK: Longman Group Ltd., 1979.

[79] C. Godsil and G. F. Royle, *Algebraic graph theory*, New York, NY, USA: Springer, 2001.

[80] L. Lovasz, "Random walks on graphs," *Combinatorics, Paul erdos is eighty*, vol. 2, pp. 1–46, 1993.

[81] S. T. Xia, X. J. Liu, Y. Jiang, and H. T. Zheng, "Deterministic constructions of binary measurement matrices from finite geometry," *IEEE Transactions on Signal Processing*, vol. 63, no. 4, pp. 1017–1029, 2015.

[82] J. Wang, S. Kwon, and B. Shim, "Generalized orthogonal matching pursuit," *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6202–6216, 2012.

[83] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[84] R. Albert and A. L. Barabasi, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.

[85] S. H. Yook, H. Jeong, and A. L. Barabasi, "Modeling the Internet's large-scale topology," *Proceedings of the National Academy of Sciences*, vol. 99, no. 21, pp. 13382–13386, 2002.

[86] M. H. Albadi and E. F. El-Saadany, "A summary of demand response in electricity markets," *Electric Power Systems Research*, vol. 78, no. 11, pp. 1989–1996, 2008.

[87] Federal Energy Regulatory Commission, "2012 Assessment of demand response and advanced metering, staff report," FERC, Washington, DC, USA, 2012. [Online]. Available: https://www.ferc.gov/sites/default/files/2020-05/12- 20-12-demand-response.pdf

[88] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28–42, 2013.

[89] S. Althaher, P. Mancarella, and J. Mutale, "Automated demand response from home energy management system under dynamic pricing and power and comfort constraints," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1874–1883, 2015.

[90] M. Yu, J. Jiang, X. Ye, X. Zhang, C. Lee, and S. H. Hong, "Demand response flexibility potential trading in smart grids: A multileader multifollower Stackelberg game approach," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, no. 5, pp. 2664–2675, 2023.

[91] P. Pinson P and H. Madsen, "Benefits and challenges of electrical demand response: A critical review," *Renewable and Sustainable Energy Reviews*, vol. 39, pp. 686–699, 2014.

[92] P. Siano, "Demand response and smart grids–A survey," *Renewable and Sustainable Energy Reviews*, vol. 30, pp. 461–478, 2014.

[93] W. Huang, N. Zhang, C. Kang, M. Li, and M. Huo, "From demand response to integrated demand response: Review and prospect of research and application," *Protection and Control of Modern Power Systems*, vol. 4, pp. 1–13, 2019.

[94] M. H. Albadi and E. F. El-Saadany, "Demand response in electricity markets: An overview," in *2007 IEEE Power Engineering Society General Meeting*, Tampa, FL, USA, 2007, pp. 1–5.

[95] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 3, pp. 381–388, 2011.

[96] T. Samad, E. Koch, and P. Stluka, "Automated demand response for smart buildings and microgrids: The state of the practice and research challenges," *Proceedings of the IEEE*, vol. 104, no. 4, pp. 726–744, 2016.

[97] H. Zhong, L. Xie, and Q. Xia. "Coupon incentive-based demand response: Theory and case study," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1266–1276, 2013.

[98] J. Aghaei and M. Alizadeh, "Demand response in smart electricity grids equipped with renewable energy sources: A review," *Renewable and Sustainable Energy Reviews*, vol. 18, pp. 64–72, 2013.

[99] S. Balasubramanian and P. Balachandra, "Effectiveness of demand response in achieving supply-demand matching in a renewables dominated electricity system: A modelling approach," *Renewable and Sustainable Energy Reviews*, vol. 147, pp. 111245, 2021

[100] J. Knudsen, J. Hansen, and A. M. Annaswamy, "A dynamic market mechanism for the integration of renewables and demand response," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 940–955, 2016.

[101] B. Dupont, C. De Jonghe, L. Olmos, and R. Belmans, "Demand response with locational dynamic pricing to support the integration of renewables," *Energy Policy*, vol. 67, pp. 344–354, 2014

[102] B. Zeng, J. Zhang, X. Yang, J. Wang, J. Dong, and Y. Zhang, "Integrated planning for transition to low-carbon distribution system with renewable energy generation and demand response," *IEEE Transactions on Power Systems*, vol. 29, no. 3, pp. 1153–1165,2014.

[103] L. Gkatzikis, I. Koutsopoulos, and T. Salonidis. "The role of aggregators in smart grid demand response markets," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7 pp. 1247–1257, 2013.

[104] X. Lu, K. Li, H. Xu, F. Wang, Z. Zhou, and Y. Zhang, "Fundamentals and business model for resource aggregator of demand response in electricity markets," *Energy*, vol. 204, pp. 117885, 2020.

[105] C. Zhang, Q. Wang, J. Wang, P. Pinson, J. M. Morales, and J. Østergaard, "Real-time procurement strategies of a proactive distribution company with aggregator-based demand response," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 766–776, 2018.

[106] M. Parvania, M. Fotuhi-Firuzabad, and M. Shahidehpour, "Optimal demand response aggregation in wholesale electricity markets," *IEEE Transactions on Smart Grid*, vol. 4, no. 4, pp. 1957–1965, 2013.

[107] Y. Wang, Q. Chen, C. Kang, Q. Xia, and M. Luo, "Sparse and redundant representation-based smart meter data compression and pattern extraction," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2142–2151, 2017.

[108] K. Buchanan, N. Banks, I. Preston, and R. Russo, "The British public's perception of the UK smart metering initiative: Threats and opportunities," *Energy Policy*, vol. 91, pp. 87–97, 2016.

[109] M. J. Fell, D. Shipworth, G. M. Huebner, and C. A. Elwell, "Public acceptability of domestic demand-side response in Great Britain: The role of automation and direct load control," *Energy research & social science*, vol. 9, pp. 72–84, 2015.

[110] M. R. Asghar, G. Dán, D. Miorandi and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[111] M. Stojnic, F. Parvaresh, and B. Hassibi, "On the reconstruction of block-sparse signals with an optimal number of measurements," *IEEE Transactions on Signal Processing*, vol. 57, no. 8, pp. 3075–3085, 2013.

[112] F. Alizadeh and D. Goldfarb, "Second-order cone programming," *Mathematical Programming*, no. 95, pp. 351, 2003.

[113] Z. Zeinalkhani and A. H. Banihashemi, "Iterative reweighted ℓ_2/ℓ_1 recovery algorithms for compressed sensing of block sparse signals," *IEEE Transactions on Signal Processing*, vol. 63, no. 17, pp. 4516–4531, 2015.

[114] "Dataset of a demand response program," [Online]. Available: https://drive.google.com/file/d/1w6Vco4RUhSSFfwNbNADOH4xNfXqlsvLs.

[115] Japan Meteorological Agency, "Historical weather data," [Online]. Available: https://www.data.jma.go.jp/risk/obsdl/index.php#.

[116] "Model of a demand response program," [Online]. Available: https://drive.google.com/file/d/1w7im4Zdy41rTpoaTdtXislElip5qxQlV.

[117] F. Xu, R. Ariizumi, S. Azuma, and T. Asai, "Tamper-resistant controller using neural network and time-varying quantization," *Artificial Life and Robotics*, vol. 25, pp. 596–602, 2020.

[118] S. Hoory, "The size of bipartite graphs with a given girth," *Journal of Combinatorial Theory, Series B*, vol. 86, no. 2, pp. 215–220, 2002.

[119] G. Chartrand, S. F. Kapoor, and D. R. Lick, "n-Hamiltonian graphs," *Journal of Combinatorial Theory*, vol. 9, no. 3, pp. 308–312, 1970.

[120] Y. Li, W. Liu, and L. Feng, "A survey on spectral conditions for some extremal graph problems," *arXiv preprint*, arXiv:2111.03309, 2021.