MODEL PREDICTIVE CONTROL FOR MITIGATING SENSOR ATTACKS ON MULTILEVEL INVERTERS

by

Rao Rao

A Thesis Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Master of Science

in Engineering

at

The University of Wisconsin-Milwaukee

May 2019

ABSTRACT

MODEL PREDICTIVE CONTROL FOR MITIGATING SENSOR ATTACKS FOR MULTILEVEL INVERTERS

by

Rao Rao

The University of Wisconsin-Milwaukee, 2019
Under the Supervision of Dr. Lingfeng Wang

Nowadays, multilevel power inverters have become a hot research topic which are being widely used in smart grids. They are also driving devices for conveyors, compressors, motors, and can enable uninterruptible power supply for critical loads such as database centers or telecommunications base stations. In the future, smart grids will play an important role to achieve higher efficiency, smarter control and better performance. Such an ambitious goal can only be achieved by inverters with higher voltage and power levels.

The smart grids are the typical cyber-physical systems that is composed of physical processes and computation units combined by sensors, actuators, and communication devices. The smart grids are apt to errors and vicious attacks on their physical construction leading to considerable damage, such as false data injection (FDI), denial of service (DOS). The vicious data injection can effectively bypass the detection of system and cause serious effects on the grid.

In recent years, some advanced control approaches have been proposed to perform inverter current control. Among them, model predictive control (MPC) is a promising one that makes use of explicit system models to predict its future response and optimize system performance. It has

unique advantages that can accurately forecast the future response of the system and have fast response.

However, the effectiveness and the accuracy of the conventional MPC rely on whether the system model is accurate. Uncertainty and false data injection in the system model sometimes lead to unresponsive or even unstable control systems. Conventional MPC is hard to keep the system stable when the uncertainty and malicious attack happen. In existing studies, although various attacks have been investigated, the undetectable false data injection aiming at the inverter system was rarely studied.

In the thesis, the model of the cascaded H-bridge inverter is established and conventional MPC to achieve load current control is applied. It shows great performance to achieve load current control and has fast dynamic control. Then considering various attack signals such as step attack signals, pulse attack signals to the sensors in the system, the conventional MPC loses the ability to achieve a stable and effective current control.

According to simulation results, Kalman Filter model is built which can filter some Gaussian noises from the sensors in the system. Then from the perspective of attacker, a special FDI attack is designed that can effectively bypass the Kalman Filter. For the system that targeted by the FDI and DOS attack, a new controller is designed based on the K-Nearest Neighbor (KNN) algorithm and MPC strategy which can achieve the load current control with high output quality. Finally, the new control method based on KNN and MPC is compared with conventional MPC. The simulation results are analyzed and conclusion have been made. A modified MPC combined with KNN algorithm proposed in this thesis can detect bad data that can enter the system without triggering

alarms. The case studies show the modified MPC based on KNN algorithm can achieve current control accurately when the system is injected by various attack signals showing better performance of current control with low total harmonic distortion (THD).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

Firstly, I want to appreciate my thesis advisor Dr. Lingfeng Wang. I am deeply influenced by Dr. Wang's rigorous, strict and enthusiastic attitude towards scientific research. Dr. Wang always gave me the most professional guidance on a weekly basis. During the group meeting every week, Dr. Wang listened to my presentations and gave me professional advices to ensure I could make continuous progresses on my research each week. In addition, Dr. Wang often cared about the lives and studies of the students here. When we had the group meeting every week, he always gave us some useful suggestions about how to adapt to the life in Milwaukee faster. During my study in UWM, every time I turned to him, he would give me professional advice on my research and I was really influenced by his broad knowledge in high-level research.

Then, I want to thank Dr. Zhaoxi Liu who always gave me a hand when I had problems on my research. I was deeply influenced by his rigorous scientific research attitude and profound knowledge. He always answered my doubts patiently and gave me so much help on my research.

I also want to appreciate my thesis committee: Dr. David Yu and Dr. Guangwu Xu. Thank you for taking the time to take part in my defense and giving me useful comments on my thesis.

In addition, I want to appreciate my labmates, Li Ma, Yitong Shen, Youqi Guo and Yunfan Zhang. They spent a lot of time discussing the problems that I faced in my research.

I am also grateful to the financial support for this research project. This work was supported in part by the National Science Foundation under Award ECCS1711617, in part by the Research

Growth Initiative Program of University of Wisconsin-Milwaukee under Award 101X360, and in part by the National Science Foundation Industry/University Cooperative Research Center on Grid-connected Advanced Power Electronic Systems (GRAPES) under Award GR-18-06.

Lastly, I want to express gratitude to my parents far in my homeland for their full support. Whenever I was in trouble, they always gave me support.

Chapter 1 Introduction

1.1Research Background

In recent years, multilevel power inverter has been a hot research topic which is often used in new energy grids [1-3]. The multilevel inverter output waveform is more approaching to the ideal wave with better output power quality and reduces the electromagnetic noise. Moreover, it can also effectively reduce the volume and weight of the filter. Power inverters are so vital in the future for smart grid for higher efficiency, smarter control and better performance [4-7].

The smart grids is the typical cyber-physical systems that consists of physical processes, computation and communication units connected by sensors, actuators, and communication devices [8]. The smart grid is apt to errors and vicious attacks happened on their physical construct leading considerable damage such as false data injection (FDI), denial of service (DOS). The vicious data injection can effectively enter the detection of the system and has serious effects on the grid. The most basic impact is to modify the results of system state estimation, which finally affects the decision of the closed-loop control system and stability analysis module. Therefore, cyber-attackers could make huge influence on the economy and society by breaking normal operation of the smart gird. For example, the Ukrainian power grid was attacked by cyber-attackers, and the SCADA (Supervisory control and data acquisition) system was severely damaged [9]. About 700,000 households in the western part of Ukrainia had power outages for several hours. This incident was considered to be the first blackout caused by cyber attacks.

1.1.1 Multilevel Inverter Topologies

Nowadays, due to energy shortages and environmental crises, the demand for sustainable and clean energy has become more urgent, enabling new energy generation technologies to be widely developed. Solar cells and fans are widely used as power generation systems in power generation systems. Because of the intermittent features of solar power and wind power generation, energy storage systems as buffer devices have also developed rapidly. The introduction of new energy and energy storage systems has brought about tremendous changes in the infrastructure of the power grid. The huge changes in the new energy smart grid are shown in Figure 1-1 [10-11].

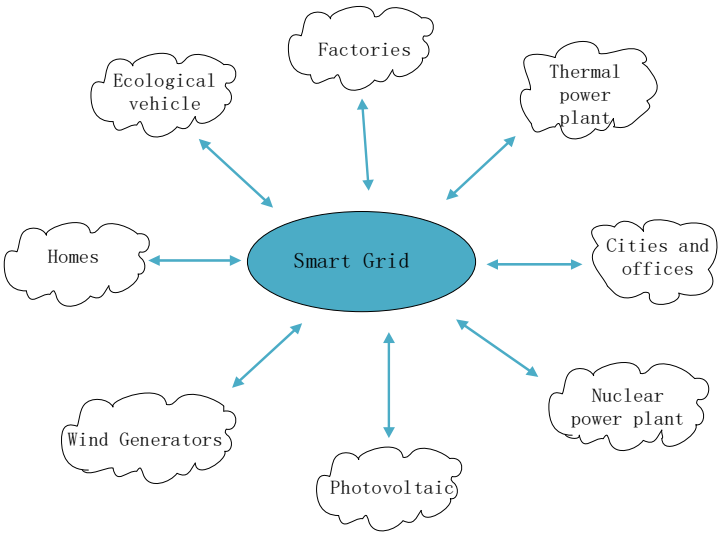


Figure 1-1 Infrastructure of future renewable energy smart grid

For example, rooftop photovoltaic cells, electric vehicles and ultra-high-power appliances have been widely used for civil and commercial electricity. On the power generation side, the power converter is the interaction of the new energy grid. In the aspects of energy transmission and distribution, the high voltage level power converter is a key part of the HVDC transmission and flexible AC transmission system. In terms of power consumption, it is a driving device for conveyors, compressors, motors. It can also be used as an uninterruptible power supply for critical

loads such as database centers or telecommunications base stations. In the future, smart grids will play an important role to achieve higher efficiency, smarter control and better performance. Such an ambitious goal can only be achieved with higher voltage inverters.

Due to the many unique features of multilevel inverter it has been rapidly developed in recent decades, resulting in a variety of topologies. In summary, multilevel inverter topology can be divided into four main types of topology, including flying-capacitor, neutral point clamped (NPC), cascaded multilevel inverters, and hybrid multilevel inverters [12]. Among them, the flying capacitor, the neutral point clamped and the cascade type inverter originated in the 1980s. Hybrid multilevel inverters are also combined by these three basic converters.

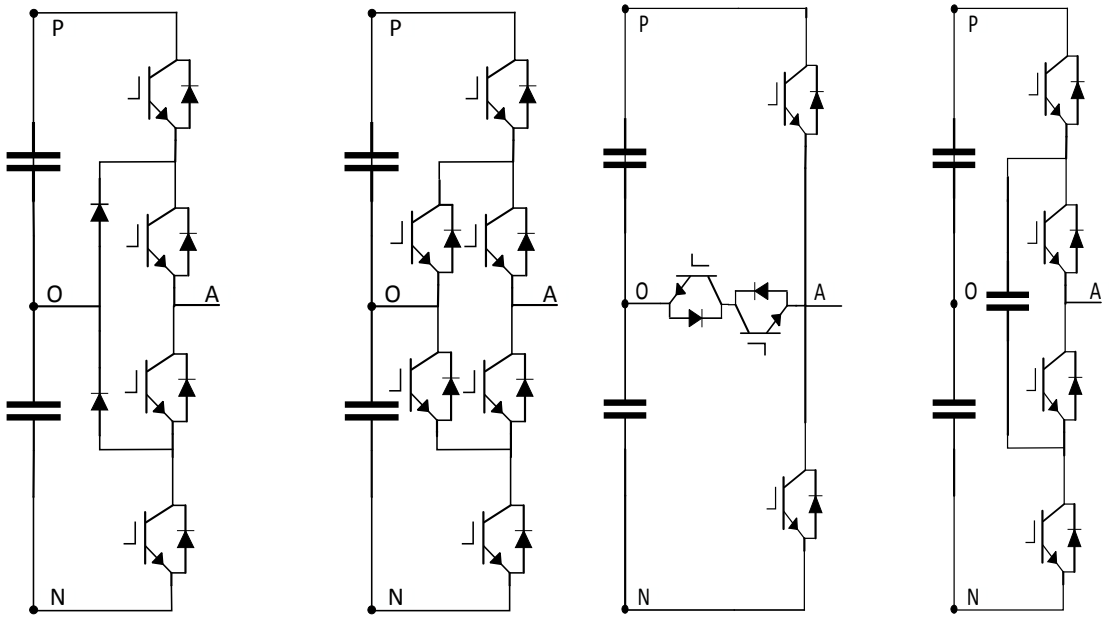


Figure 1-2 Subdivisions of NPC and FC topologies

For NPC three-level inverters, they are classified into three topologies, including diode-clamped, active-clamped, and T-type inverter displayed in Figure 1-2. Essentially, the diode neutral-point clamped inverter topology itself causes device losses and voltage stress imbalances, while active neutral-point clamped inverters can solve this problem with control strategies. The T-type three-level inverter reduces the number of switching transistors in the active midpoint clamp type inverter from six to four, and the device loss also decreases as the number of devices decreases. When the neutral-point clamp type inverter and the T type inverter work, the unequal voltage division of the two capacitors intensify the switching device voltage stress with high harmonic distortion rate. Therefore, it requires additional control strategy to solve unbalanced the neutral-point voltage.

Although the flying-capacitor multilevel inverter does not have a neutral-point voltage balance problem, it also requires an additional control strategy to keep the flying capacitor voltage balanced. The voltage balancing problem complicates the control strategy.

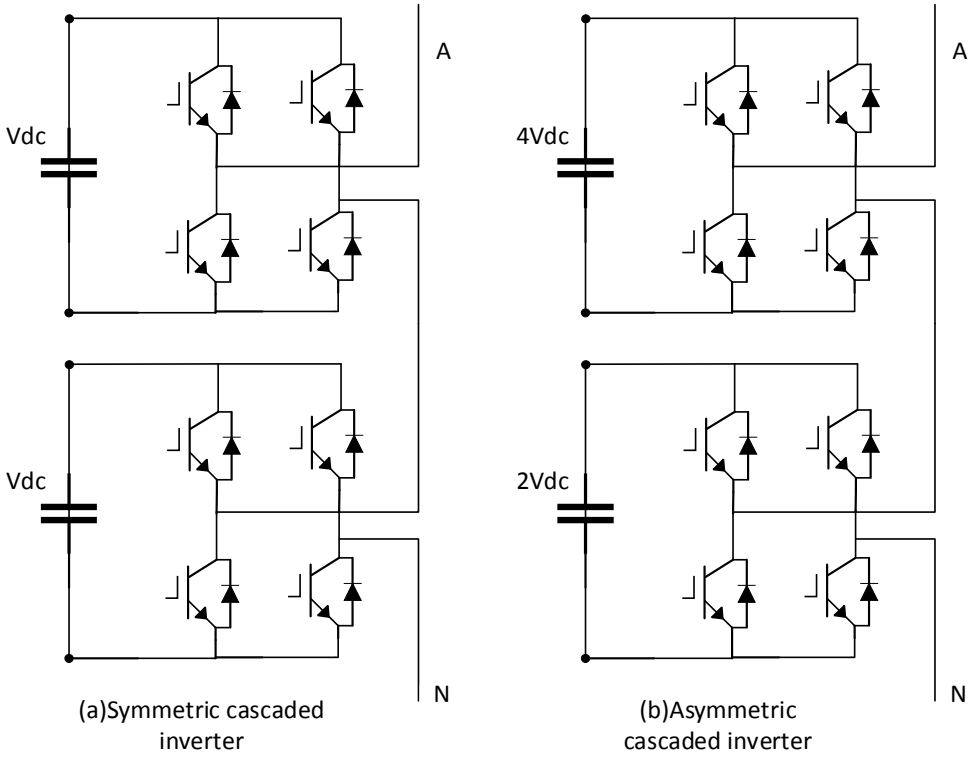


Figure 1-3 Subdivision of cascaded topology

Compared with other inverters, cascaded multilevel inverters have many unique advantages that are popular in various areas. The essence of single-phase cascaded multilevel inverters is to combine two-level inverters as basic units. As the output level increases with the number of basic units, the cascaded multilevel inverter is very suitable for high level voltage. Moreover, the remarkable character of cascaded multilevel inverter is the modular structure with high scalability and it does not need to balance the voltage with high reliability. The topology of cascaded inverters shows in Figure 1-3.

1.1.2 Cyber-security of Smart Grid

With continuous advancement of smart grid, advanced sensor, computation, communication and control units are deeply connected in the power system. Conventional power systems are gradually integrated with information control equipment and communication sensor networks to

form a cyber-physical system (CPS) [13−14]. By Promoting efficient allocation of power resources, real-time analysis as well as the scientific decision-making, security vulnerabilities in communication networks and information devices also pose potential threats [15−16].

The smart grid is the typical cyber-physical system that is composed of physical processes, computation units connected by sensors, actuators, and communication devices. The smart grid is apt to errors and vicious attacks on their physical construct caused considerable damage such as false data injection (FDI), denial of service (DOS). Cyber-attackers could make huge economic losses and societal impacts though causing serious consequence to the normal operation of the smart gird. For example, the failures that happen in the power grid of New York (2003) and Mumbai (2012) lead to catastrophic effects.

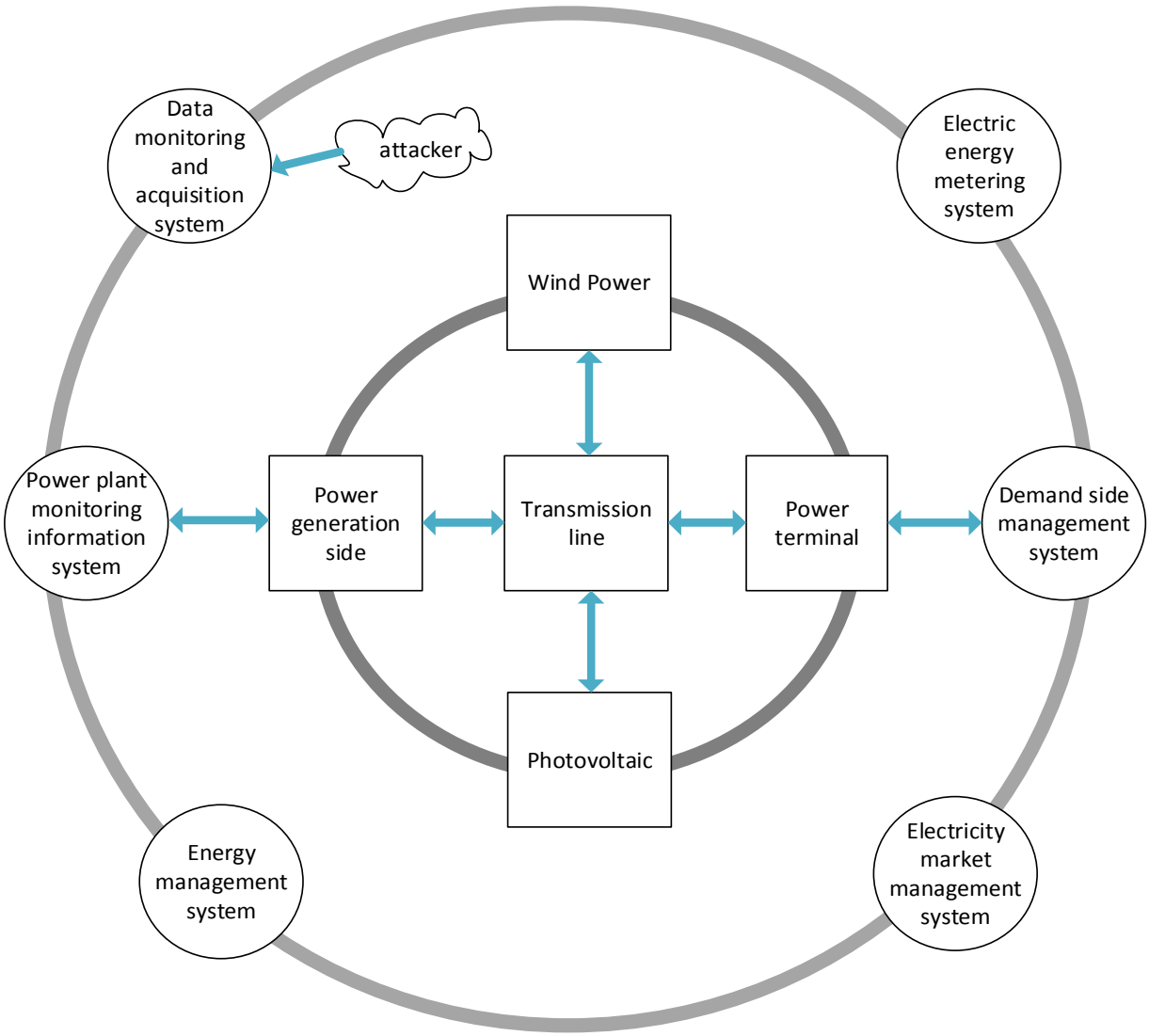


Figure 1-4 The framework of cyber physical power system

Taking FDI for SCADA in Figure 1-4 as an example, an attacker can inject false data through multiple channels such as measurement unit, communication network and control device, and then carry out follow-up attacks on the power service.

1.2 False Data Injection Detection Technologies

Various attacks can result in serious damage to public safety and economic losses [17-19]. There some common approaches that study how to deal with some specific attacks in the systems. For instance, [18] defined the deception attacks and denial of service attacks, then it came up with a new measurement to do with the denial of service attacks efficiently. Deception attacks take into account the damaging the control package or measurements, which changes the actions of the sensors. A denial of service attack can affect the information, such as interference with communication channels.

False data injection attack (FDIA) is defined as an attack method that destroys the integrity of the grid information by tampering with the measurement and control data. It has strong accessibility, concealment and interference which can influence the analysis decision of the upper control center. FDI is one of the most threatening methods to destroy the power system and makes serious consequences. In recent years, there have been many large-scale power network security incidents around the world, including many scenarios using data tampering mechanisms. Consider the vicious attack on the Ukrainian power grid. Cyber-attackers design false data into control and data acquisition and falsifies the original data, so that the operator and the control device may lose considerable controllability, and the fault spreads massively. The systems are difficult to recover [20−21].

Many attacks specifically aiming at the control systems in smart grid are proposed [22]-[29]. Security dangers such as unattended monitoring sensors or actuators in the power system may lead to false data. In the existing studies, a general method proposed arranges a special controller combined an estimator with a detector. The Kalman Filter which is a popular estimator produces estimations for state variables [22]-[23]. The system touches off an alarm if the estimated value

and the measured value do not coincide with each other. In other words, a significant difference from the estimated value and the measured value represents an erroe or an attack that may happen in the system. Kebina Manandhar proposed a new indication for the Kalman Filter to detect for the FDI whether the systems need to trigger an alarm efficiently[28].

In [30], a special false data injection attacks which are opposed to state estimators are designed. That means unnoticeable false data injection attacks are devised even if limited information is obtained by cyber-attackers. The principle of FDIA is to use the limitations of the bad data identification method in the state estimator and maliciously tamper the measurement of the component in order to cause the controller to misjudge the current state of the system, which leads to stability control of the power system to be mis-moved or rejected in turn [31-33].

In existing studies, there are various detection methods for the FDI. If the cyber-attacker has sufficient information related to the power grid and power protection algorithms, it is easy to construct a bad data identification detection algorithm that can avoid the existing least squares state estimation. Based on the characteristics of this kind data distortion, the current detection method improves the original state estimation algorithm and enhances the ability to identify human malicious data. The improved method mainly includes residual detection method, measurement mutation detection method and measurement correlation detection method, etc. [34-36].

In addition, considering the detection threshold is greatly affected by the system scale, the global system can be partitioned for large systems, and different thresholds are set according to the actual parameters of each subsystem [37]-[38]. The special feature of this approach is that it makes use of a mature algorithm, which has a fast detection speed and can better reflect the trait of power

system. However, the setting of detection threshold has a great influence on the detection accuracy, and it is prone to miss detection and false detection. The state estimation based detection method is mainly used for static analysis. Some scholars can consider using historical data for trajectory analysis, predicting the current value of the grid, and comparing it with the actual amount measurement to analyze the areas that may be attacked. The detection methods based on trajectory prediction mainly include statistical consistency test, sequential detection based on generalized likelihood ratio and sensor trajectory prediction [39]-[41].

This method can effectively detect various kinds of false data according to the operating rules of the system state and the historical database, and predict the distribution law of the state variables. Various types of false data can be effectively detected by matching the running track, but the computational complexity is high, the detection speed is slow, and it is not suitable for complex systems. Besides conventional mathematical modeling research approaches, artificial intelligence-based FDIA detection ways has been proposed recently such as neural network [42]-[43]. The significant feature of the artificial intelligence approach is the powerful computation ability and has a clear frame.

1.3 Control Strategies of Multilevel Inverter

At present, there are two main types of classical modulation methods for cascaded H-bridge multilevel inverters: 1.Selective harmonic elimination PWM which is simple to calculate and easy to implement, but the utilization effectiveness of DC voltage is low and the output voltage performance is poor; 2. Space vector modulation. Although its DC voltage utilization effectiveness is high and current ripple is small with better quality, the amount of voltage vectors intensifies

cubically and the amount of switching states increases accordingly as the voltage levels increase. Therefore, the space vector modulation is very complicated and limited when the voltage levels are high.

Recently, some new control methods have been investigated to realize current control. Among them, model predictive control (MPC) is a professional term for computer approaches that use explicit system model to predict its future response that optimizes system performance [44-46]. The idea of MPC can be traced back to 19 years old. In the 1960s, due to the simple concept of MPC and the ability to effectively handle complex system constraints and achieve complex control objectives, MPC has been usually used in extensive range of fields such as process industry, automotive, energy, environment, aviation. MPC can be summarized as follows:(1) Obtain current state measurement of the system; (2) Solve the optimal control problem (optimal control problem, OCP); (3) Only use the first control amount in the predicted time domain as the system input; (4) return (1) in the next moment. Because this process has been repeated, MPC is also known as rolling time domain control and can accurately forecast the future response of the system.

The effectiveness and the accuracy of the MPC depend on whether the system model is accurate. Uncertainty of the system model sometimes leads to unresponsive or even unstable control systems. Although the way of rolling time domain makes MPC have certain robustness, traditional MPC is not designed to deal with the uncertainty of the system. The implementation of robust stability requires that the external noise is small enough or that the state constraints do not exist, so it does not satisfy the requirement of system. So as to solve this problem systematically, minimum-maximum robust model predictive control (RMPC) algorithm was firstly proposed. But

in the smart grid, there are various malicious data that happens. For the MPC, it is hard to keep the stability of system.

Firstly, we consider the state estimation by using Kalman Filter. Then we come up with an advanced detection method of cyber-attacks in a linear system equipped with a model predictive controller, where the feedback loop is closed over a non-ideal network and the process is simulated with both the FDI attack and DOS attack.

1.4 Research Objective and Thesis Layout

The primary goal of this thesis first applies the conventional MPC on the cascaded multilevel inverters to achieve load current control. And then standing on the perspective of attacker and considering Kalman Filter in the system a special FDI attack is designed that can not be detected by the Kalman Filter. For the system that injecting the FDI and DOS attack, a new controller is designed based on KNN and MPC strategy which can achieve the load current control with high output quality. Then, the simulation results are analyzed and some conclusion have been made. Finally, the new control method based on KNN and MPC is made to compare with conventional MPC.

The thesis is organized as following. Chapter 2 provides cascaded multilevel inverter model with MPC strategy for tracking the reference current. Chapter 3 presents the Kalman Filter model for cascaded multilevel inverter considering the Euclidean-detector, also makes special FDI attack model for the system that can not be detected by the Kalman Filter. And the new control approach considering KNN and MPC is came up with to achieve system stability and the case studies for

the conventional and new method are compared in chapter 4; The conclusions are presented and ongoing work is prospected in chapter 5.

Chapter 2 Model Predictive Control for Cascaded Multilevel Inverter

2.1 Introduction

The multilevel inverter is very popular due to the unique features such as small voltage change rate dv/dt, small electromagnetic interference, the large output levels, the small THD, low switching frequency[1-4]. Multilevel inverters mainly include three mature types: neutral point clamped, flying capacitor and cascaded H-bridge[5]. As the amount of voltage levels increases, the neutral point clamped and flying capacitor inverter require a huge number of clamp diodes or flying capacitors. Moreover, both of them need to keep the capacitor voltage balanced. The cascaded H-bridge inverter is widely used in high-power drives, active filters, high-power supply because it is easy modular to control with high reliability [6-7].

2.2 CHB Model with MPC

2.2.1 CHB Topology

Cascaded multilevel inverters are also widely used. The essence of cascaded multilevel inverters is to combine two-level inverters as basic units. Figure 2-1 displays a symmetrical Cascaded H-Bridge (CHB) inverter topology that is the most basic cascaded multilevel inverter. It can produce 2N+1 levels when a single-phase has N cascaded units. The asymmetric cascaded H-bridge inverter topology is derived from the symmetric cascaded H-bridge multilevel inverter topology. They have some similarities. The difference between them is that the DC supply voltage of each leg of an asymmetric cascaded H-bridge multilevel inverter is different. If the DC voltage is proportionally arranged, asymmetric cascaded H-bridge multilevel inverter can obtain more

voltage levels when it has the same basic unit number with different DC voltage. The amount of output levels is exponentially related to the amount of basic units. When the number of basic units is N, it can generate 2^{N+1}-1 different output levels. However, the voltage stress and voltage loss of each switching device are different due to the different voltages of the input power supplies of each of the bridge arms. Therefore, the switching device level selection of different basic units is also different, and the system cannot be fully modularized. A modular multilevel converter (MMC) consists of two bridge arms each phase. These basic units share the voltage of the DC side power supply. Modular multi-level with N half-bridge structure can get 2N-1 different output levels, and its output level has the same characteristics as symmetric cascade H-bridge inverter.

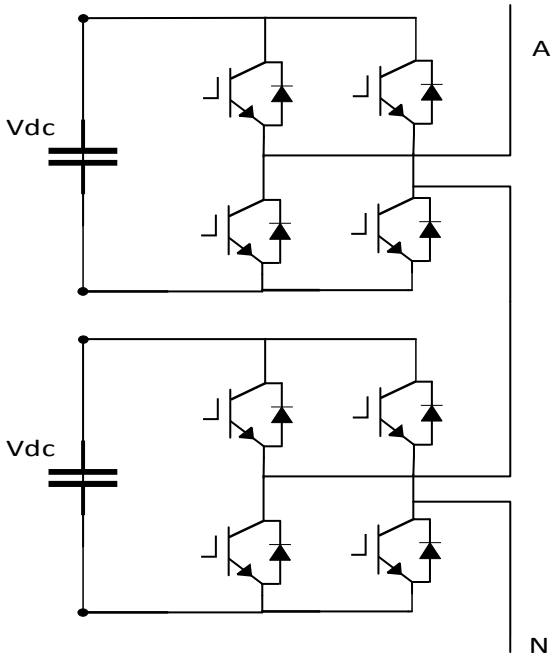


Figure 2-1 The symmetrical Cascaded H-Bridge multilevel inverter Topology

The cascaded multilevel H-bridge inverter makes up H-bridge basic power units in every phase. Figure 2-2 presents a three-phase five-level symmetrical H-bridge inverter that has two basic power units in every phase. Every H-bridge basic power unit has an independent DC voltage

source V_{DC}, four IGBTs, four diodes shown in Figure 2-3. By controlling the switching tubes, each H-bridge basic power unit can produce three output voltages $-V_{DC}$, 0 and V_{DC}.

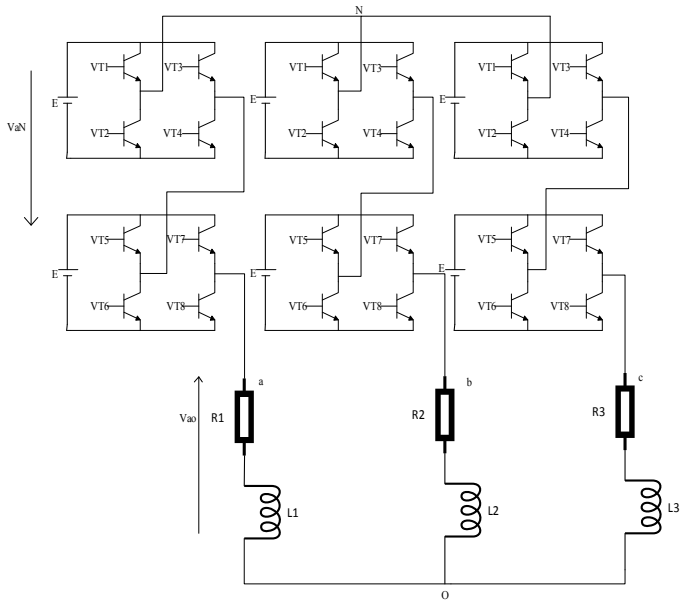


Figure 2-2 Three-phase five-level H-bridge inverter topology

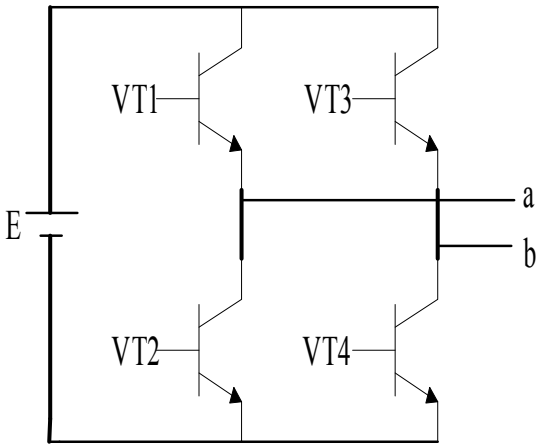


Figure 2-3 H-bridge basic power unit structure

Taking the phase A for example, the working principle is analyzed. By controlling the two H-bridge basic power units, the on/off of the eight IGBT switch tubes control the inverter A phase. Defined the DC voltage source as E, each H-bridge basic power unit has 4 switching states, so the

A phase has 16 working states with 5 voltage levels (E, -E,2E, -2E, 0).The working states is displayed in Table 2-1.

Number	VT1~VT8	Voltage of A phase	Sa
1	0,1,1,0,0,1,1,0	-2E	-2
2	0,1,0,1,0,1,1,0	-E	-1
3	1,0,1,0,0,1,1,0		
4	0,1,1,0,0,1,0,1		
5	0,1,1,0,1,0,1,0		
6	1,0,1,0,1,0,1,0	0	0
7	1,0,1,0,0,1,0,1		
8	0,1,0,1,1,0,1,0		
9	0,1,0,1,0,1,0,1		
10	1,0,0,1,0,1,1,0		
11	0,1,1,0,1,0,0,1		
12	0,1,0,1,1,0,0,1	E	1
13	1,0,1,0,1,0,0,1		
14	1,0,0,1,0,1,0,1		
15	1,0,0,1,1,0,1,0		
16	1,0,0,1,1,0,0,1	2E	2

Table 2-1 The working states of A phase

We define the switching function as $S_k = (1,0,-1)$of each H-bridge basic power unit. On the basis of DC voltage source and switching state of each phase, the output voltage of entire system can be expressed as

$$\begin{cases} V_{aN} = V_{DC}(S_{a1} - S_{a2}) \\ V_{bN} = V_{DC}(S_{b1} - S_{b2}) \\ V_{cN} = V_{DC}(S_{c1} - S_{c2}) \end{cases} \tag{2.1}$$

According to (2.1), it has a total of 125 voltage vectors. Assuming three-phase grid voltage balance, the differential equation for the inverter system which has the RL load is

$$\begin{cases} v_{a0} = v_{aN} + v_{N0} \\ L\frac{di_a}{dt} + Ri_a = v_{a0} \end{cases} \tag{2.2}$$

Where v_{N0} is the common mode voltage, defined as

$$v_{N0} = \frac{v_{aN}+v_{bN}+v_{cN}}{3} \tag{2.3}$$

Vectorial transformation:

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} \\ 0 & \frac{\sqrt{3}}{3} & -\frac{\sqrt{3}}{3} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \tag{2.4}$$

Using abc/αβ transformation, the load model is

$$L\frac{di_{\alpha,\beta}}{dt} + Ri_{\alpha,\beta} = v_{\alpha,\beta} \tag{2.5}$$

2.2.2 MPC Model

The most popular used in the field of power electronic inverters control strategy is model predictive control, which has the unique characteristics of flexible control target with fast response speed. This control method is on the basis of mathematical model of inverter, and predicts new circuit parameters generated by the different switching states at the next moment of the converter through the circuit parameters at the current time. The tracking function is defined by the tracking

current or the tracking voltage, the switching frequency, etc., and the circuit parameters of the next time corresponding to different switching states are substituted. Then, the switching state which obtains minimum value in cost function is the most ideal switching state.

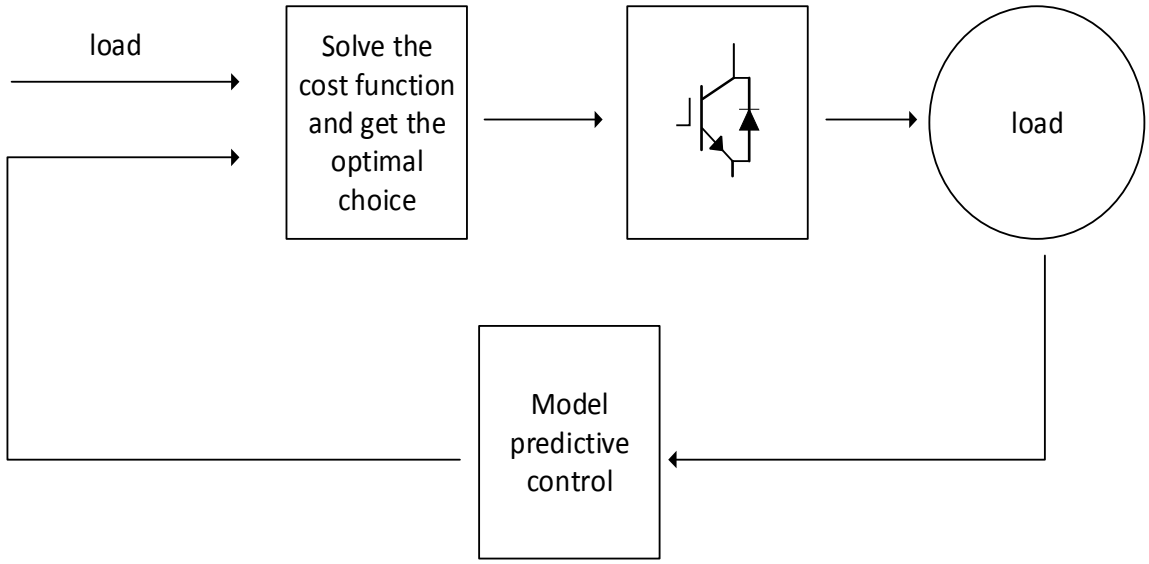


Figure 2-4 Block diagram of MPC

The principal idea of model prediction current control algorithm makes predictions of load current generated by every feasible voltage vector at next moment of the inverter, and choose the optimal voltage vector that has minimum value acting on inverter at following moment for load current tracking. The mechanism of MPC is presented in Figure 2-4.

The derivative di/dt can be expressed approximately as

$$\frac{di_{\alpha,\beta}}{dt} \approx \frac{i_{\alpha,\beta}[k+1]-i_{\alpha,\beta}[k]}{dt} \tag{2.6}$$

The future load current is obtained by substituting (2.6) in (2.5),

$$i_{\alpha,\beta}[k+1] = \frac{T_s}{L}(v_{\alpha,\beta}[k] - i_{\alpha,\beta}[k](R - \frac{L}{T_s})) \quad (2.7)$$

The chosen cost function is in equation (2.8).

$$\mathrm{g}[\mathrm{k}+1] = |i_a^*[k+1] - i_a[k+1]| + \left|i_\beta^*[k+1] - i_\beta[k+1]\right| \quad (2.8)$$

Where i_a^*, i_β^* are the reference current at time k+1, and i_a, i_β are the actual current produced by each possible voltage vector at time k+1.

According to equations, using the load current $i(\alpha, \beta)$ at time k, all voltage vectors that may be generated at the next moment of the inverter are brought into equation (2.7) to calculate all possible next-time load currents. The value, that is, for any given voltage vector, its corresponding next-time load current value is predicted. In this inverter system, cost function (2.8) is caculated for every feasible voltage vector, and the voltage vector that has smallest data of cost function is acted at the next moment of system, which requires calculation 125 times for optimal control. The steps of the predicted current control is displayed in Figure 2-5.

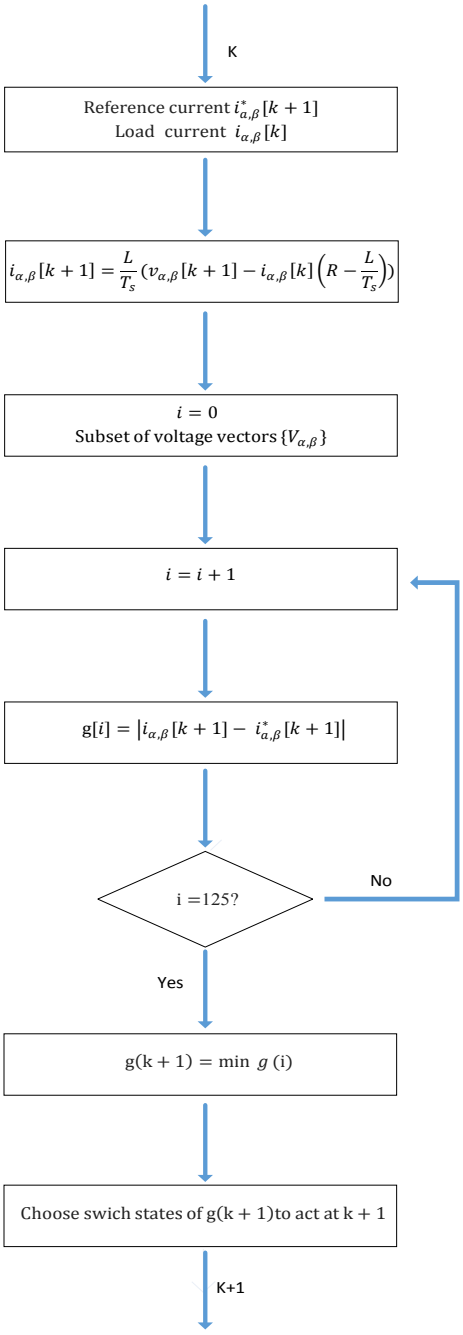


Figure 2-5 Steps of MPC

2.3 Model Test

So as to demonstrate the correctness of the model predictive current control strategy, we get simulation results of the cascaded three-phase five-level H-bridge inverter with MPC strategy on the MATLAB/Simulink. The main circuit topology is the same as Figure 2-2. Moreover, we also consider three different type of FDI on the sensors of the system:

1) Injecting step signals as the attack signals into the feedback of load current. The attack signal amplitude is 10A from the 0.05 second to 0.15 second;

2) Injecting ramp signals as the attack signals into feedback of load current. The attack signal rises at the 0.05 second with 10A per second rising rate and the duration is 0.1 seconds.

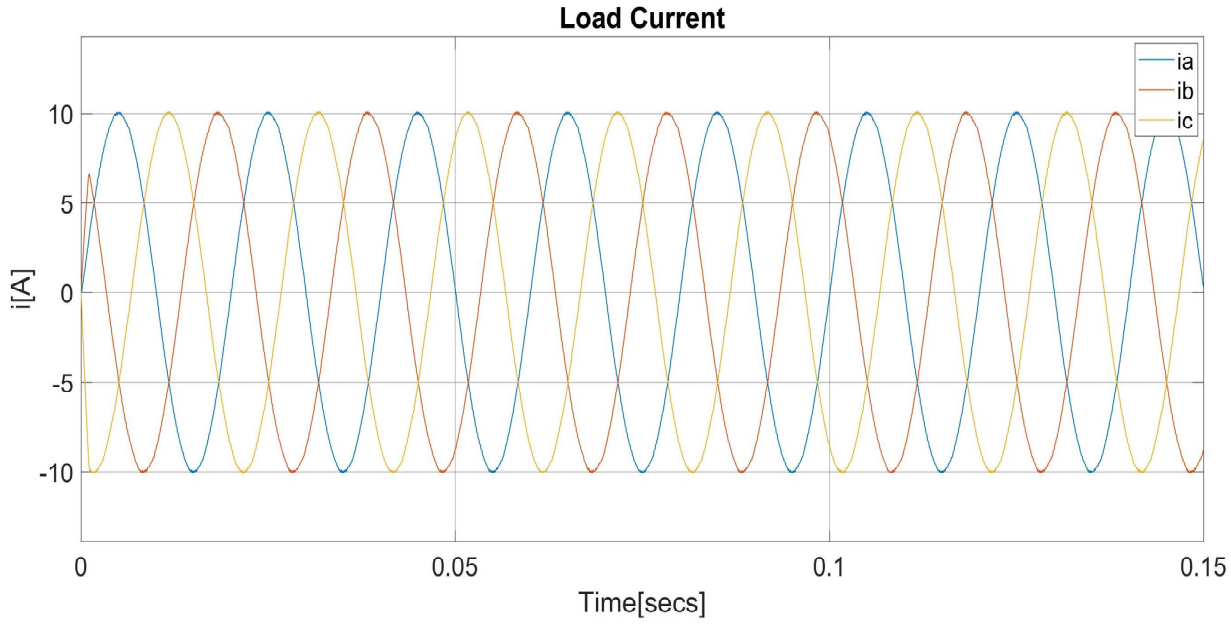
3) Injecting pulse signals as the attack signals into feedback of load current. The attack signal rises at the 0.02 second with 10A per 0.02 second and the duration is 0.1 seconds.

Primary parameters are displayed in Table 2-2. The simulation results demonstrate the conventional MPC loses ability to keep the system stable when the system injecting false data. The performance is not accurate.

parameters	values
L	15mH
R	50 Ω
f	50Hz
$Sample\ time$	Ts=10e-6s
V_{DC}	700V
I_{ref1}	10A
I_{ref2}	20A

Table 2-2 Primary parameters of the inverter system

Figure 2-6 shows the load current has good performance to track the refence current with low THD when no false data is injected into the inverter. We can see that when the sampling time (Ts=10e -6 [s]) is small, the model prediction control strategy shows great ability to track the reference current with the low harmonic distortion rate.



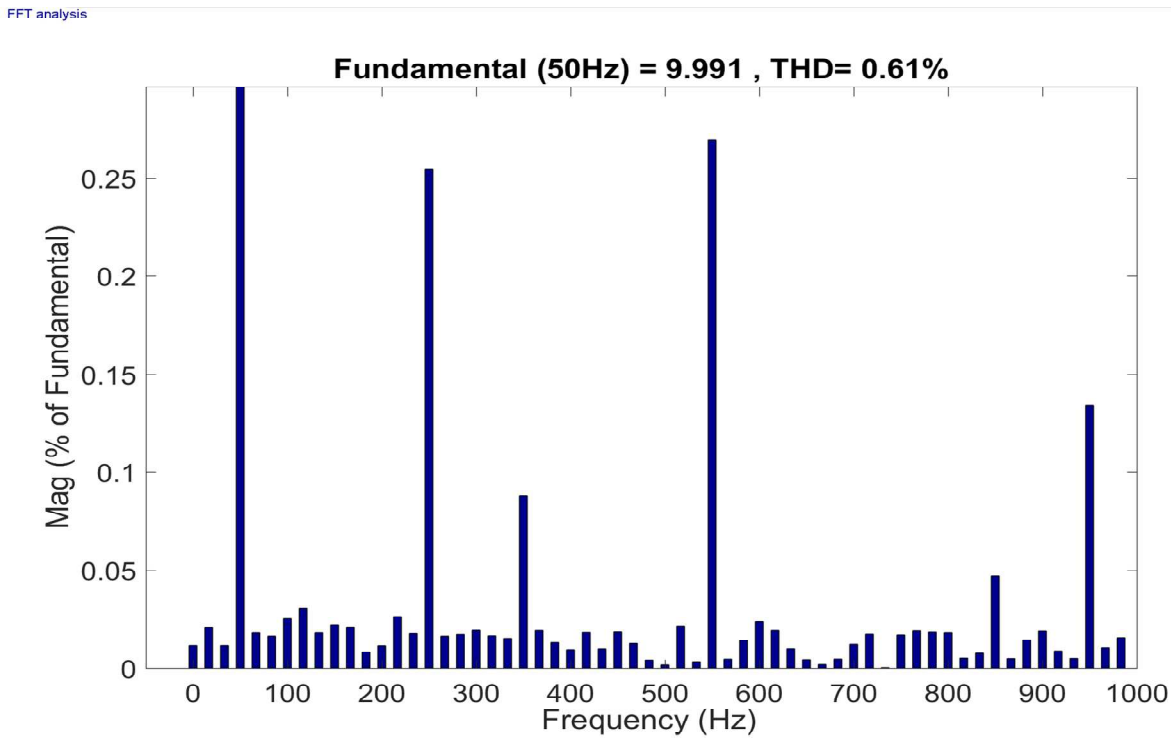


Figure 2-6 Model predictive control

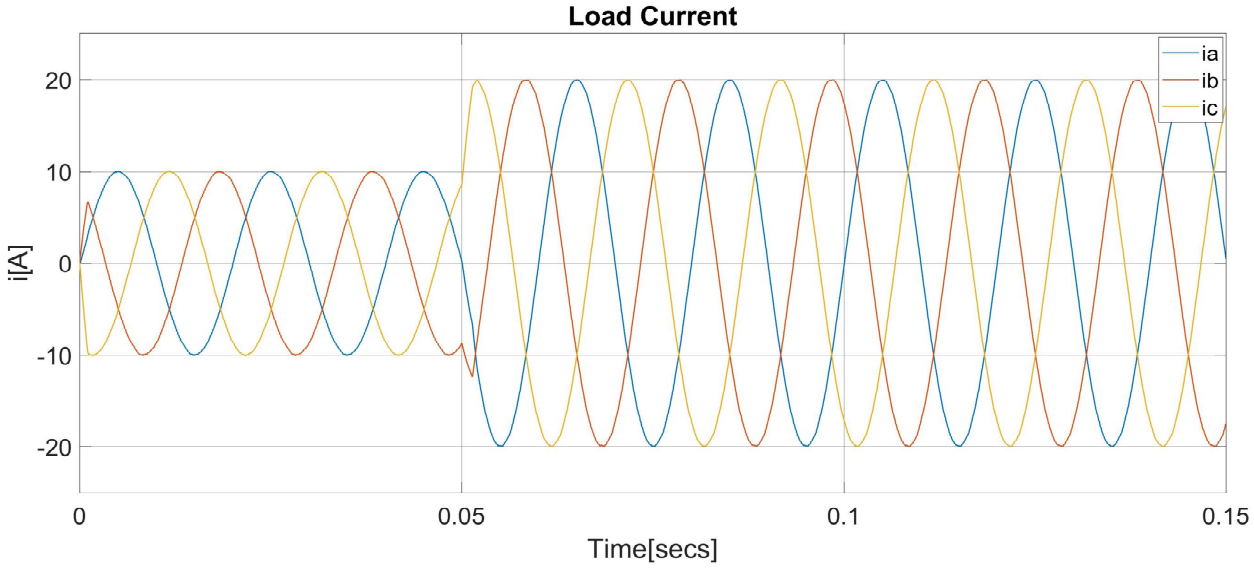


Figure 2-7 Dynamic model predictive control

From the load current and the reference current waveform in Figure 2-7, it can be seen that when the reference current is dynamically switched between i=10sinɯ(100πt) and i=20sinɯ(100πt), The model prediction control strategy system still has better tracking effect with fast dynamic response.

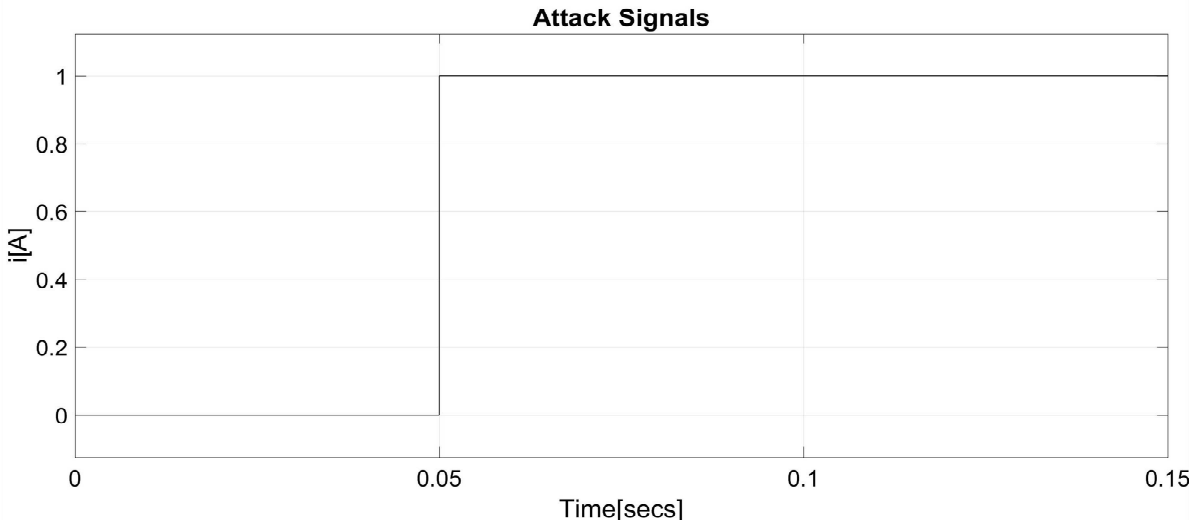
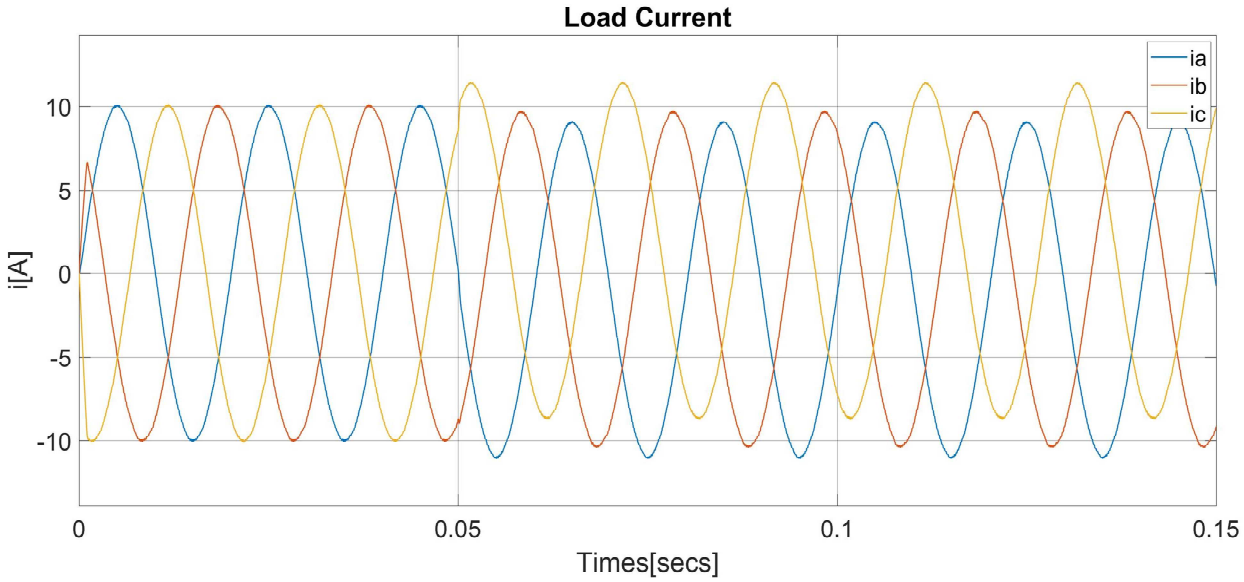


Figure 2-8 Step attack signals

The system is injected with the step attack signal shown in Figure 2-8 on the sensors which is from 0.05 seconds displayed in Figure 2-9. The simulation results in Figure 2-10 demonstrate the load current can not track the reference current. From 0.05 seconds, the performance of MPC is not accurate.



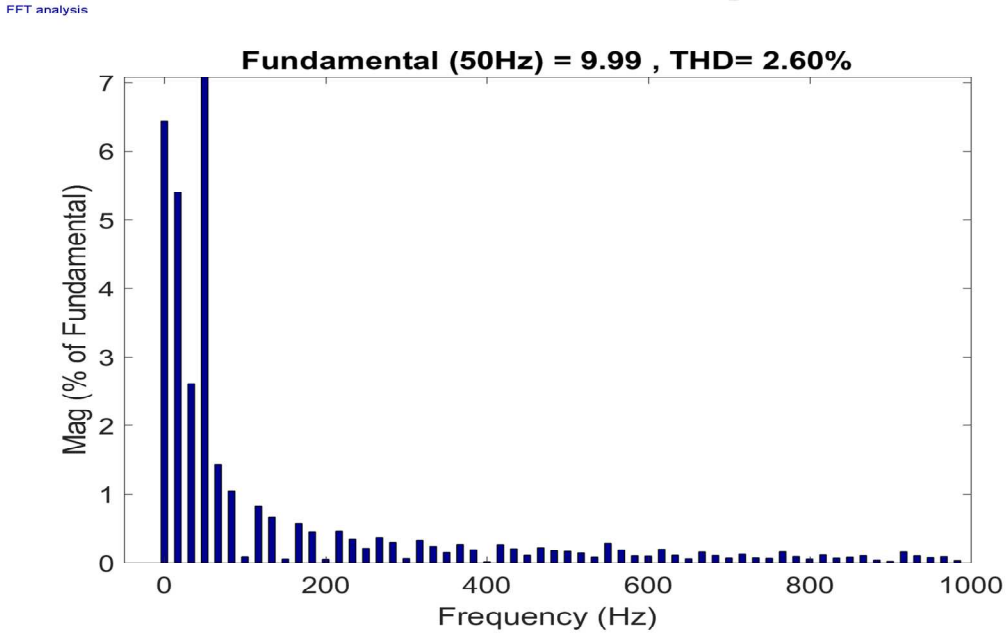


Figure 2-9 Model predictive control

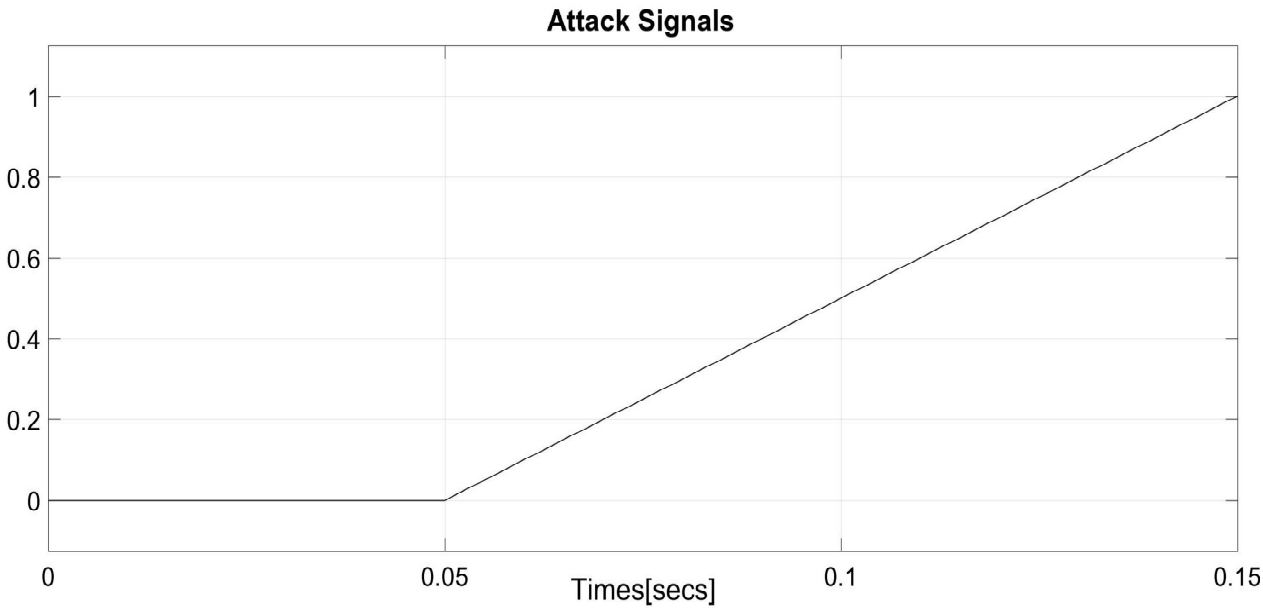


Figure 2-10 Ramp attack signals

The system is injected with the ramp attack signal on the sensors which is from 0.05 seconds displayed in Figure 2-10. The simulation results in Figure 2-11 demonstrate the load current is unable to follow the reference current. From 0.05 seconds, the performance of MPC is not accurate.

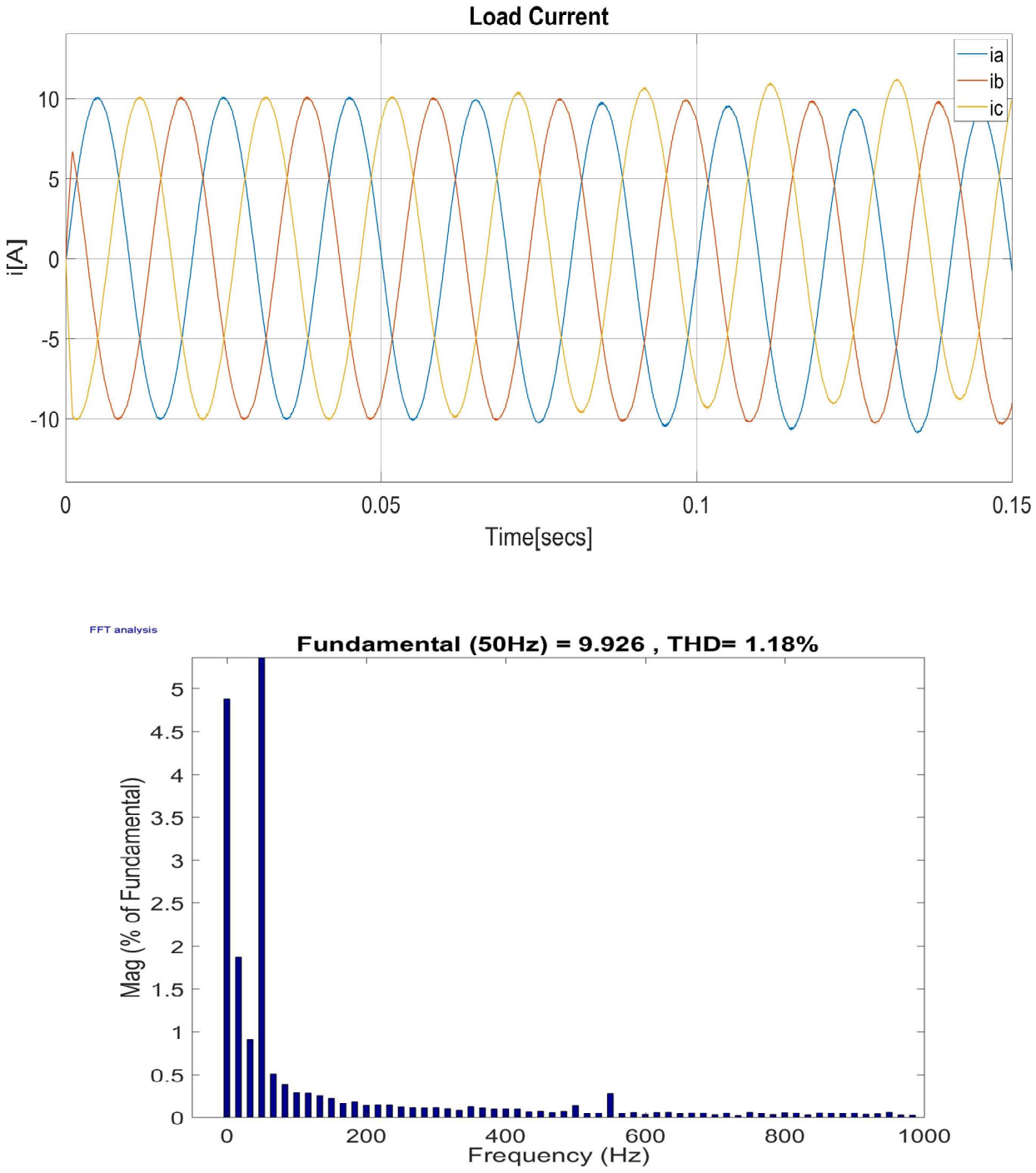


Figure 2-11 Model predictive control

The system is injected with the pulse attack signal on the sensors which is from 0.05 seconds displayed in Figure 2-12. The simulation results in Figure 2-13 demonstrate the load current is unable to follow the reference current. From 0.05 seconds, the performance of MPC is not accurate.

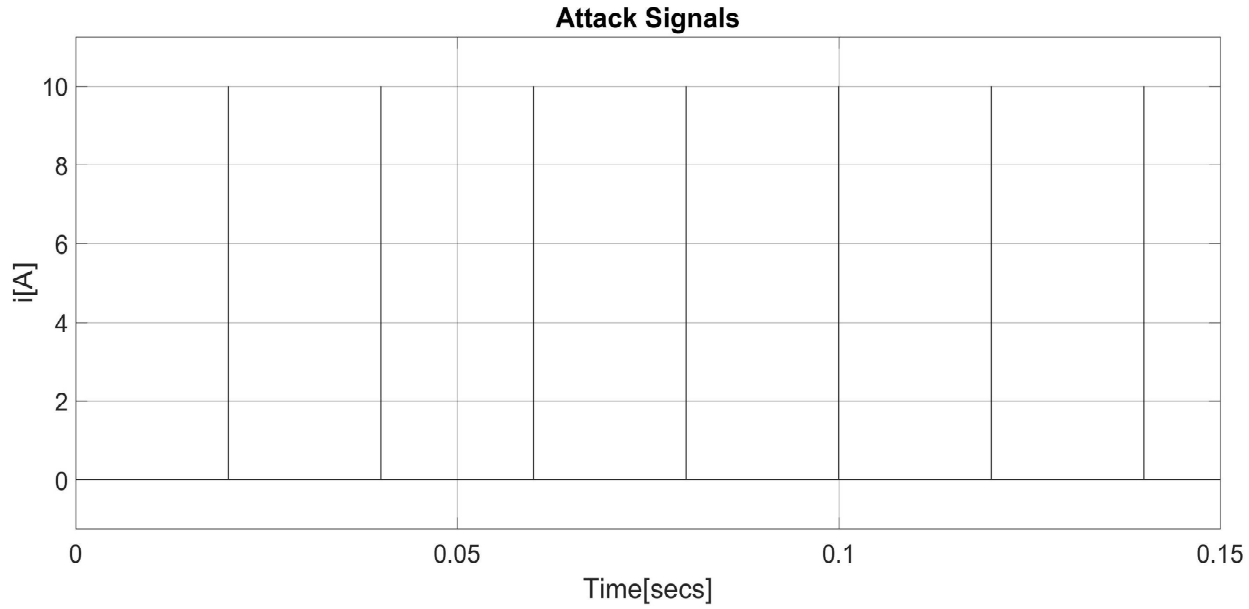
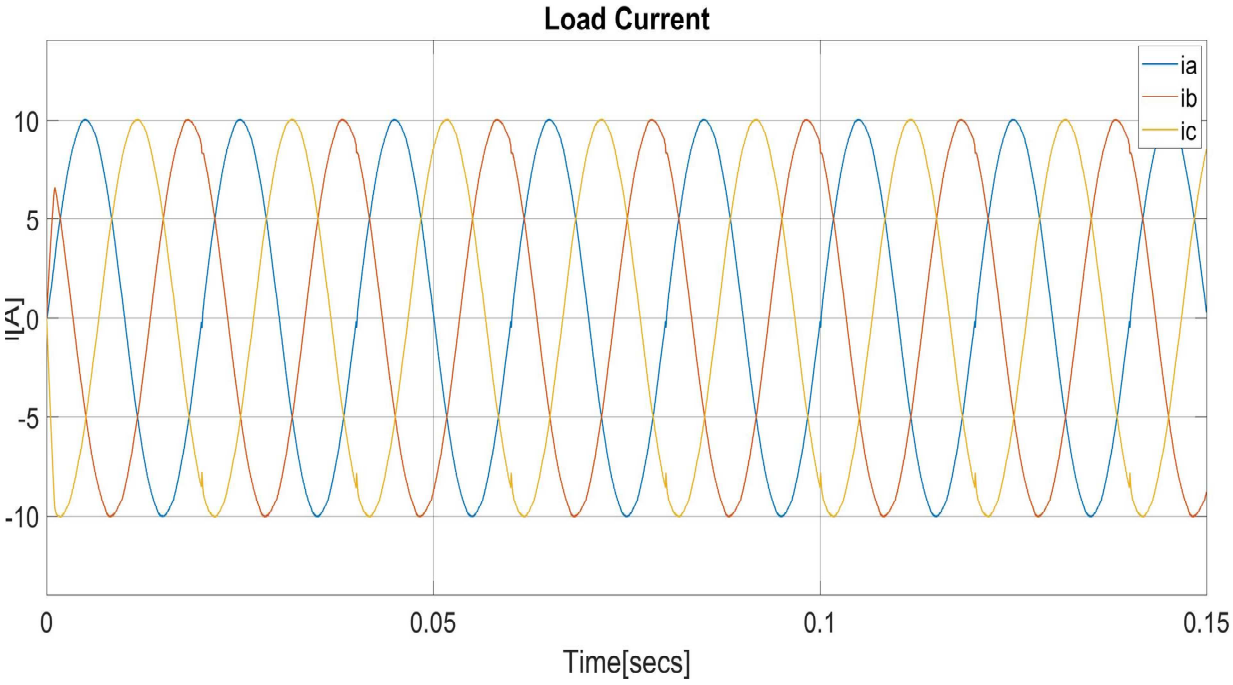


Figure 2-12 Pulse attack signals



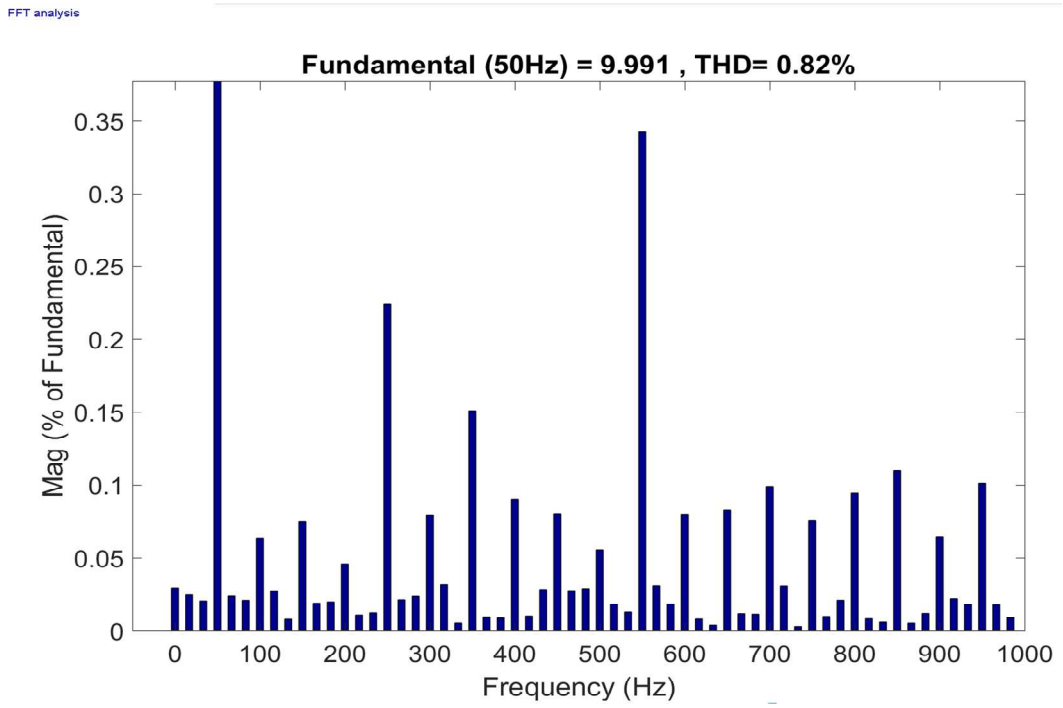


Figure 2-13 Model predictive control

2.4 Conclusion

In this chapter MPC model for CHB converters in smart grid is established and tested. For this model, we think about the current control. Firstly, the system state equations are obtained from the CHB. Then the next current is calculated by discretized the system state equations. Finally, the next optimal switch states are chose by the cost function of MPC and acted at next time to achieve the current control.

To test this model, we did the simulations in Simulink and consider three scenarios:

(1) By using the conventional MPC strategy for the CHB system without injecting false data to achieve the current control.

(2) By using the conventional MPC strategy for the CHB system without injecting false data to achieve the current control which is dynamic.

(3) By using the conventional MPC strategy for the CHB system with injecting false data to achieve the current control.

In general, MPC strategy can perform well and shows fast dynamic response without injecting FDI attack to track the reference current. The load current has high quality and the THD is less than 1%. MPC shows great performance in current control of CHB system, which accurately forecast the future response. But it does not have ability to guarantee a better performance of current control when the FDI attack happens.

Future work can be focused on the following aspects: considering the impact of FDIA; how to distinguish the FDIA in the system like using Kalman Filter; how to distinguish the bad data from the normal ones by using machine learning ; considering the other improved MPC methods like RMPC,SMPC.

Chapter 3 Kalman Filter

3.1 Introduction

Large-scale application of power electronics and other nonlinear components in electricity cause noise and harmonic interference to be introduced into various types of signals, which adversely affects the normal operation of the grid. Moreover, with the rapid progress of smart grid, there are various attacks happened in the system which also make bad influence on the system. Therefore, it needs to separate from the observation signal mixed with random interference. Conventional separation methods include fast Fourier transform, minimum mean square error method, least squares method, adaptive notch filter method and so on. With the continuous development and improvement of Kalman Filter theory, it is widely used in power systems, mainly in the short-term load forecasting of power systems, dynamic state estimation, power quality analysis, relay protection, wind farm wind speed prediction, motor state and parameter estimation.

Kalman Filter has the ability of optimal state estimation and iterative calculation form, which is widely used in state estimation, state prediction, fault detection. It is a popular state estimation approach.

Recently, many attacks specifically aiming at sensor and actuator are exposed [22]–[27]. Security dangers involve modifying the physically unattended monitoring sensors which may result in false data. A common approach distinguishes modifying is though designing a special controller that is composed of an estimator and a detector. The estimator is used to contrast the calculation data with the actual data [22], [23]. The detector touches off an alarm while the

estimated value and measured value do not coincide. The methods of bad data detection are various. In-depth study of bad data detection based on state estimator now, Kalman Filter is undoubtedly an optimal filtering method that is widely used in many areas around our life. Figure 3-1 shows a smart grid system with Kalman Filter for state estimation.

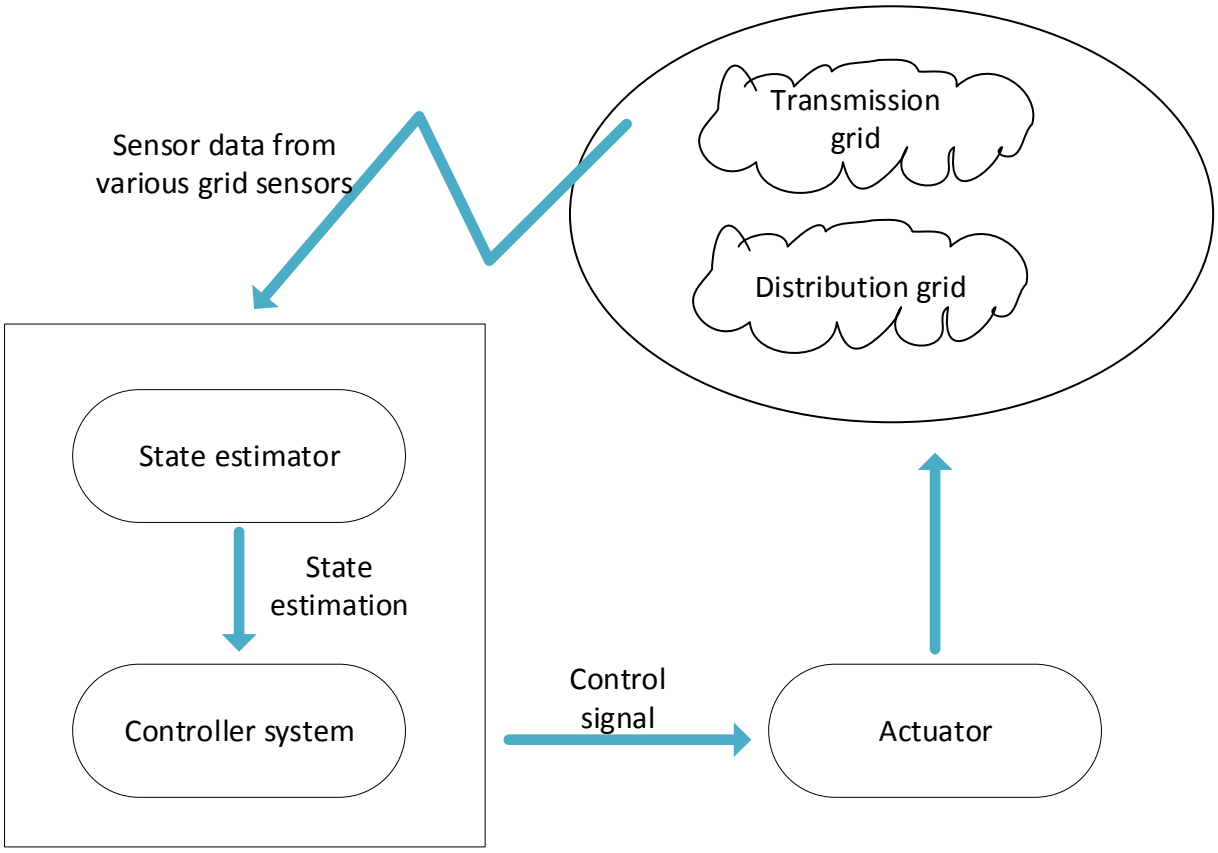


Figure 3-1 Block diagram of smart grid system

In this chapter, firstly basic Kalman Filter model is described and then the cascaded multilevel inverter with Kalman Filter is established which can filter the noise in the system and increase the accuracy of current control. Then, the Euclidean-detector is defined whether the attacks can be detected and the alarm can be triggered. Finally, a special false data injection attack is established considering incomplete inverter system information which can not be detected by the Euclidean-detector of the Kalman Filter.

3.2 Kalman Filter Model

In early 1960s, Kalman and Bucy first proposed a state space-based recursive filtering method. The Kalman Filter is an autoregressive filter that uses a recursive algorithm to make state estimation of a dynamic system through limited and noise-containing measurements.

The Kalman Filter-based approach requires knowledge of the system model. When it is more accurate, the parameters of the filter are actually changed from the output of the filter and the residual of the actual value.

Considering the target system is a linear stable system, and dynamic model is

$$x(k+1) = Ax(k) + Bu(k) + w(k) \tag{3.1}$$

$$y(k) = Cx(k) + v(k) \tag{3.2}$$

Where $x(k)$ represents the n-dimensional state variable of the linear time-invariant stationary system, $u(k)$ denotes that the system control variable is M-dimensional, $w(k)$ and $v(k)$ are respectively existing process noise and measurement noise in inverter system, y is the result signal of the entire inverter system.

Assuming noises $w_t$and v_t obey Gaussian random vectors with a mean of 0, and the covariance is Q >0and R>0.

Kalman Filter has abilities to recursively estimate the system state. It first makes estimations of process state at a certain moment, and then gets the feedback in the form of noise measurement variables. The filtering is classified into following parts: the time updating part and the measurement updating part. Specifically, the time updating equation part mainly plays a predictive role which is reliable for estimating the state and the estimated data of the error covariance matrix and then provides a priori estimation at the next time. The measurement updating part primarily serves as a correction that is reliable for feedback and integrates the a priori estimate with the new measured value in order to produce a corrected posterior estimate for the next time state. The working principle diagram is shown in Figure 3-2.

For the first step, updating time

$$\hat{x}(k+1|k) = A\hat{x}(k|k) + Bu(k) \tag{3.3}$$

$$\mathrm{P(k+1|k)} = \mathrm{AP(k|k)}A^T + \mathrm{Q} \tag{3.4}$$

The optimal estimated value $\hat{x}$ at k time is known, state prior estimation $\hat{x}(k+1|k)$ is predicted from (3.3), and the a priori error covariance matrix $\mathrm{P(k+1|k)}$of (3.4) predicted state.

Kalman Filter gain K is

$$\mathrm{K(k+1)} = \mathrm{P(k+1|k)}C(\mathrm{CP(k+1\,|\,k)\ C\hat{}T} + \mathrm{R})^{-1} \tag{3.5}$$

For the second step: the update of the measurement

$$\hat{x}(k+1|k+1) = \hat{x}(k+1|k) + \mathrm{K}(\mathrm{k}+1)(y(k+1) - C\hat{x}(k+1|k)) \tag{3.6}$$

$$\mathrm{P}(\mathrm{k}+1|\mathrm{k}+1) = (\mathrm{I} - \mathrm{K}(\mathrm{k}+1)\mathrm{C})\mathrm{P}(\mathrm{k}+1|\mathrm{k}) \tag{3.7}$$

The Kalman gain is obtained by observing the error minimum variance and the unbiased state principle. The optimal estimated value $\hat{x}(k+1|k+1)$ of the state variable can be obtained from (3.6), and the optimal estimated variance matrix $\mathrm{P}(\mathrm{k}+1|\mathrm{k}+1)$is obtained from (3.7).

It can be seen from (3.3)-(3.7) that it is a recursive algorithm. Under initial conditions of $x_0$and p_0, the a priori estimation $\hat{x}(k+1|k)$ is continuously corrected by the deviation between measurement of $y(k+1)$ at k+1 time and the output observation $\hat{\mathrm{y}}(k+1) = C\hat{x}(k+1|k)$.

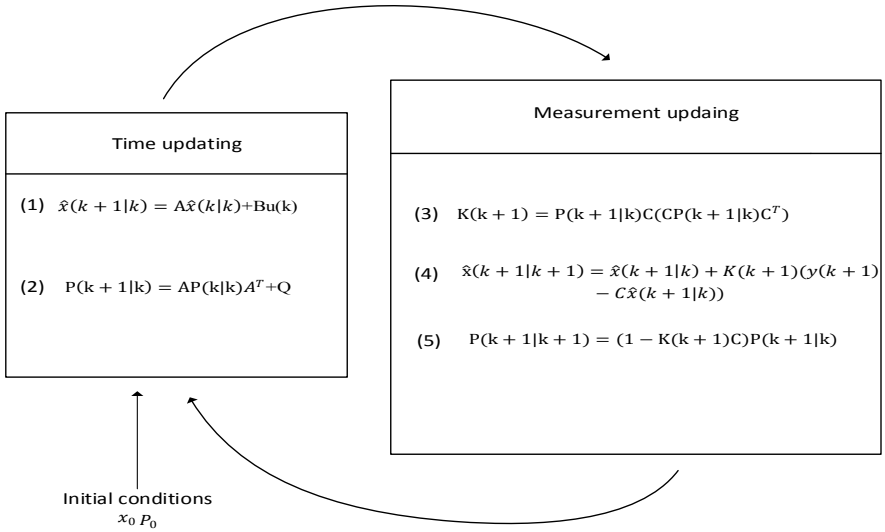


Figure 3-2 Block diagram of Kalman Filter

3.3 Model Test

In this part, Kalman Filter is established for the cascaded multilevel inverter and the Gaussian noises are considered in the system. The system is the same as the Figure 2-2.

System state equation of the three-phase five-level inverter:

$$X = \frac{1}{L}u - \frac{R}{L}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \tag{3.8}$$

$$y = [1 \quad 1]\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \tag{3.9}$$

where $X = \begin{bmatrix} \dot{\imath_\alpha} \\ \dot{\imath_\beta} \end{bmatrix}$,u =$\begin{bmatrix} v_\alpha \\ v_\beta \end{bmatrix}$is the output of the inverter.

Transfer to the Kalman Filter form

$$\begin{bmatrix} \dot{\imath_\alpha} \\ \dot{\imath_\beta} \end{bmatrix} = \frac{1}{L}\begin{bmatrix} v_\alpha \\ v_\beta \end{bmatrix} - \frac{R}{L}\begin{bmatrix} i_\alpha \\ i_\beta \end{bmatrix} \tag{3.10}$$

$$y = [1 \quad 1]\begin{bmatrix} i_\alpha \\ i_\beta \end{bmatrix} \tag{3.11}$$

Let

$$\mathrm{A} = \begin{bmatrix} \frac{1}{L} & 0 \\ 0 & \frac{1}{L} \end{bmatrix}$$

$$\mathrm{B} = \begin{bmatrix} -\frac{R}{L} & 0 \\ 0 & -\frac{R}{L} \end{bmatrix}$$

$$C = [1 \quad 1]$$

$$\mathrm{D} = 0$$

Bring system parameters in Table 2-2 to (3.10) and (3.11), the Kalman Filter equations of the system are expressed as

$$\begin{bmatrix} \dot{\imath_\alpha} \\ \dot{\imath_\beta} \end{bmatrix} = \begin{bmatrix} 66.67 & 0 \\ 0 & 66.67 \end{bmatrix} \begin{bmatrix} v_\alpha \\ v_\beta \end{bmatrix} + \begin{bmatrix} -0.75 & 0 \\ 0 & -0.75 \end{bmatrix} \begin{bmatrix} i_\alpha \\ i_\beta \end{bmatrix} \tag{3.12}$$

$$y = [1 \quad 1] \begin{bmatrix} i_\alpha \\ i_\beta \end{bmatrix} \tag{3.13}$$

So as to demonstrate the correctness of Kalman Filter designed in this part, we compare load current of CHB system considered the Kalman Filter with the one that dose not have Kalman Filter when considering the Gaussian noises from the sensor. We get simulation results both of two CHB systems in the MATLAB/Simulink.

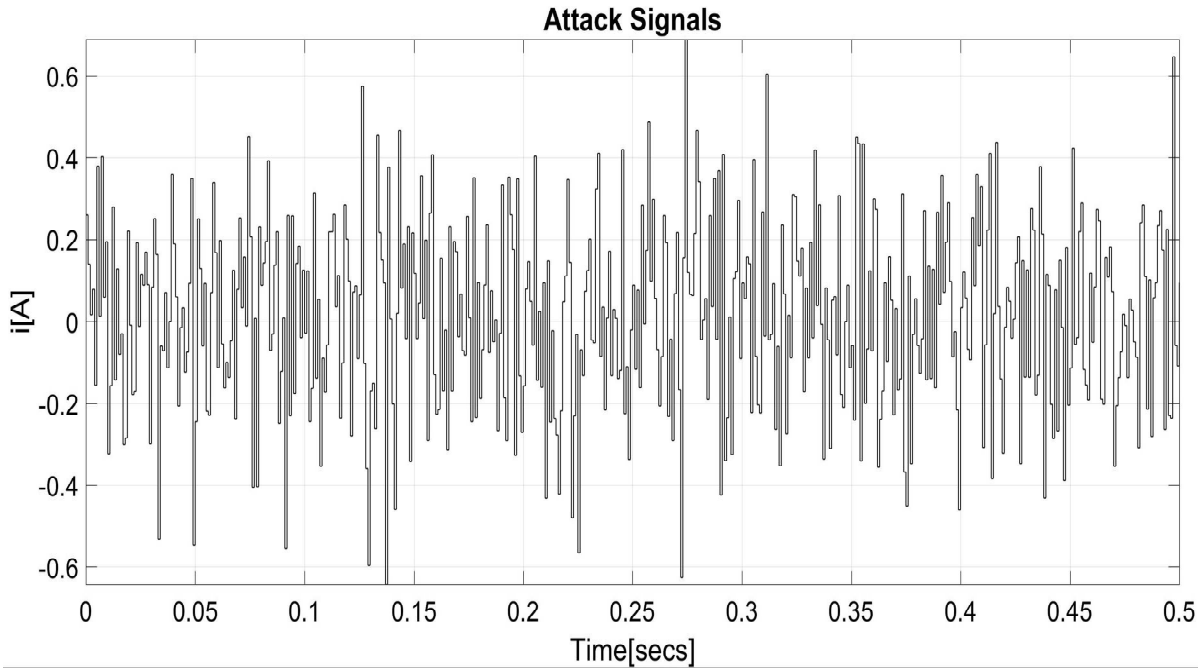


Figure 3-3 Gaussian noises

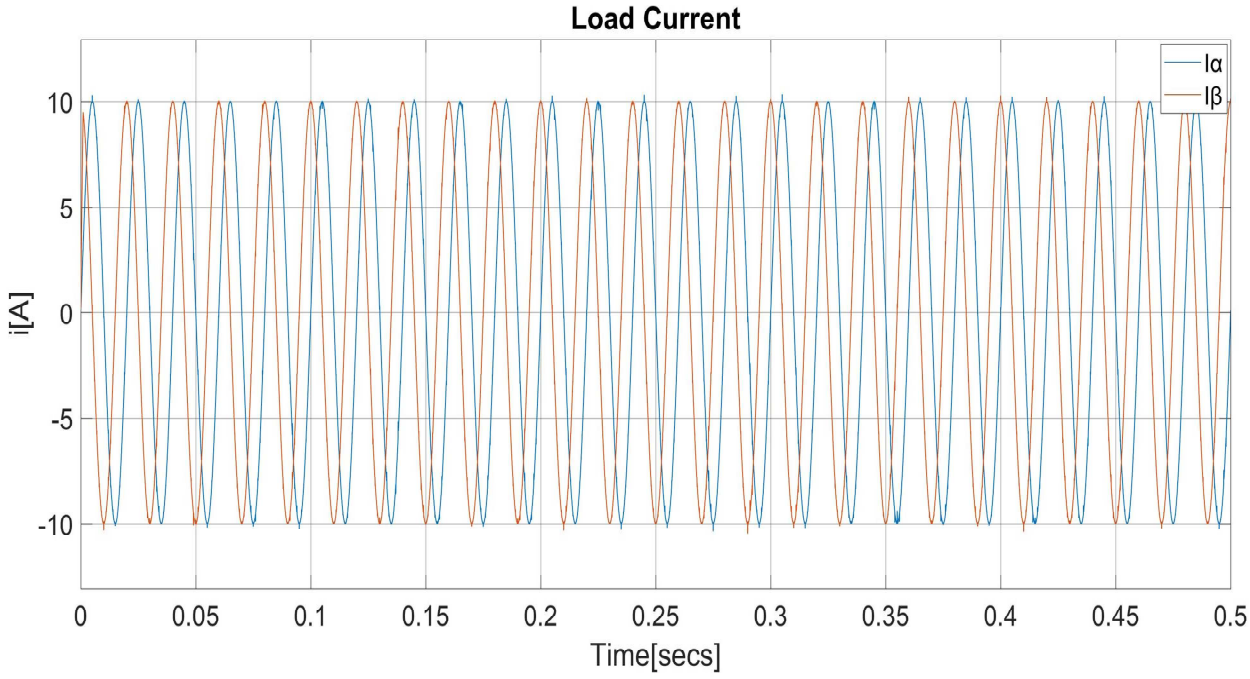


Figure 3-4 Load current without Kalman Filter

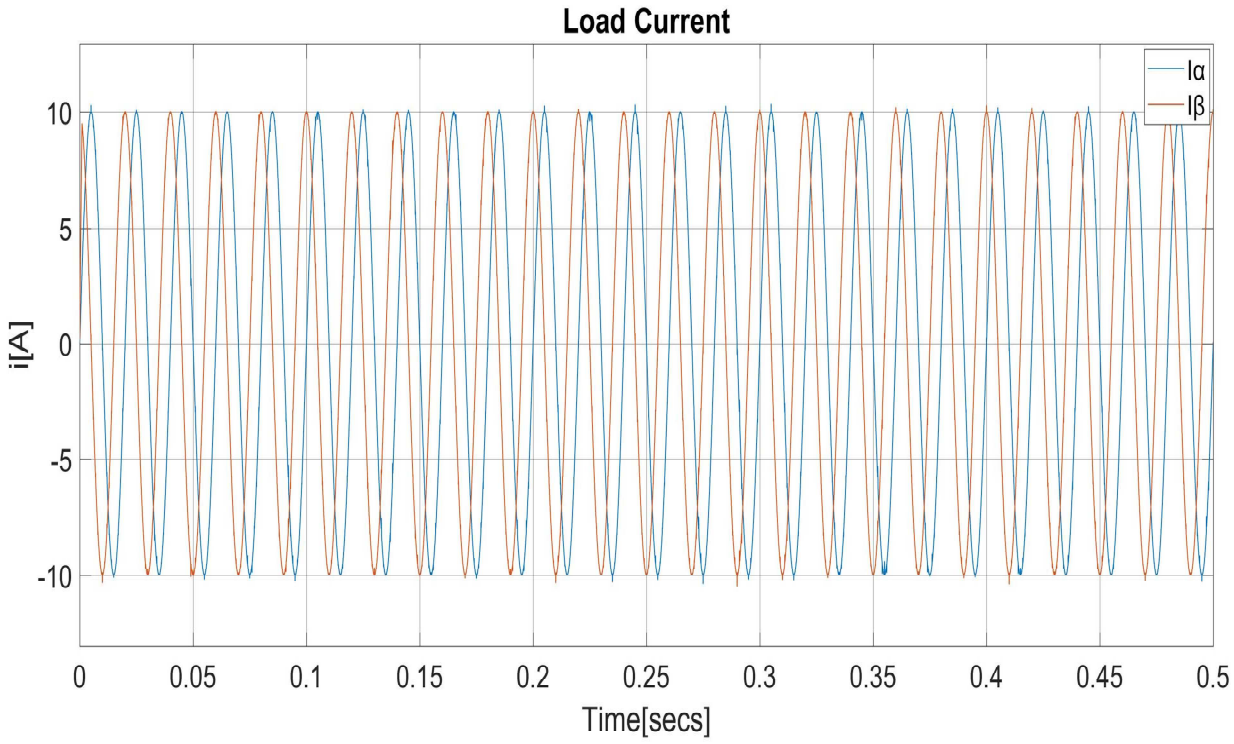


Figure 3-5 Load current with Kalman Filter

The Gaussian noises on the feedback of the load current produced by the sensor is displayed in Figure 3-3. The system with the Kalman Filter shows the filtering ability. To some extend, the Kalman Filter can filter some noise in the system. From Figure 3-4 and Figure 3-5, the max noise amplitude reduces from 0.5 A to 0.38 A. Therefore, the Kalman Filter can filter some noise and the system with Kalman Filter shows better performance to track reference current when the noise exits in system.

3.4 Attack Model Based on Kalman Filter

3.4.1 Detection Indicator

The Kalman Filter generates the state estimate by using accurate model of the smart grid and the data information got from the sensors in the system to monitor whether the system is on right operating mode.

There are various indicators proposed by scholars to detect the malicious attacks. A $\chi 2$-detector is designed to distinguish the deviation from the estimation data and the measurement data from Kalman Filter, then decides whether the system needs to trigger alarms. The $\chi 2$-detector has great effect to detect many attacks. However, the existing researches show that conventional $\chi 2$-detector and Kalam Filter are unable to do with false data injection attack. Some scholars investigate the advanced false data injection attack that happens in the system by considering the Kalman Filter and propose a new detection indicator called Euclidean indicator to deal with the FDIA. Figure 3-6 presents a security framework that KF produces the state estimation on account of the system state information and the data got from sensors. The Euclidean distance detector calculates the difference between the estimation and measurement from Kalman Filter. If the Euclidean distance is greater than a precomputed threshold, the system would make an alarm.

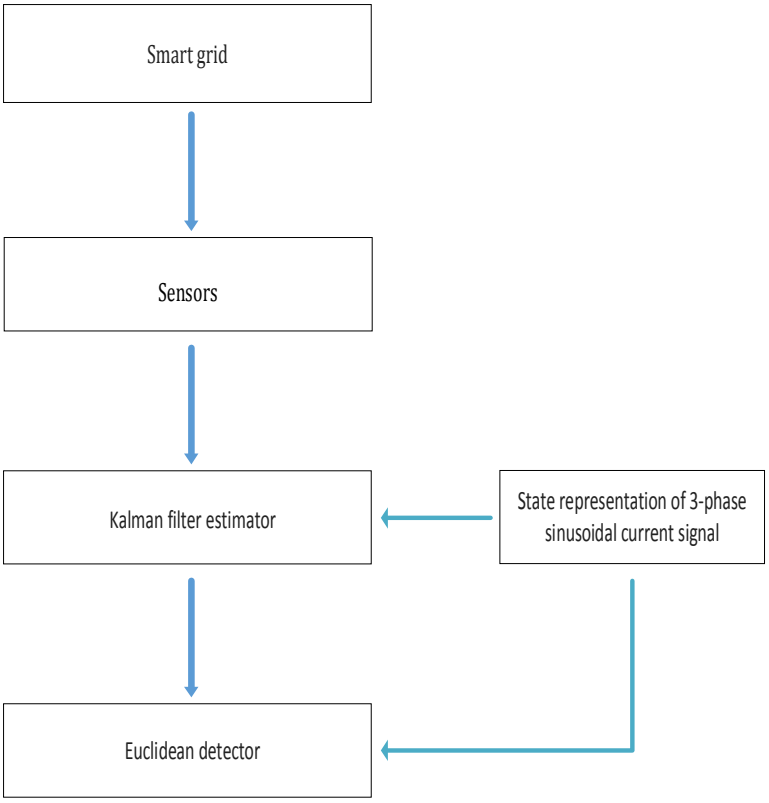


Figure 3-6 Security framework for smart grid

The Euclidean detector is expressed as

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots\cdots + (p_n - q_n)^2}$$

where p is the load current measurement value and q is the estimation value of load current.

3.4.2 Attack Model

In this part, we do research on the false data injection attack standing the perspective of control system security and consider a linear dynamic time-invariant control system for input tracking control system dynamic model. First, from the view of the attacker, it is assumed that cyber-attacker can steal the data transmitted by the target system in the network. First, the indicator

detected by the Kalman Filter is set; Then if the indicator exceeds the set value, the system will trigger an alarm; From the perspective of attacker, a secret FDI attack sequence is designed through the Kalman Filter, its indicator and system parameters. The purpose is that the attack signal can avoid the detection of the Kalman Filter to make the system controlled object deviate from the given reference signal. The diagram of FDIA in the system is shown in Figure 3-7.

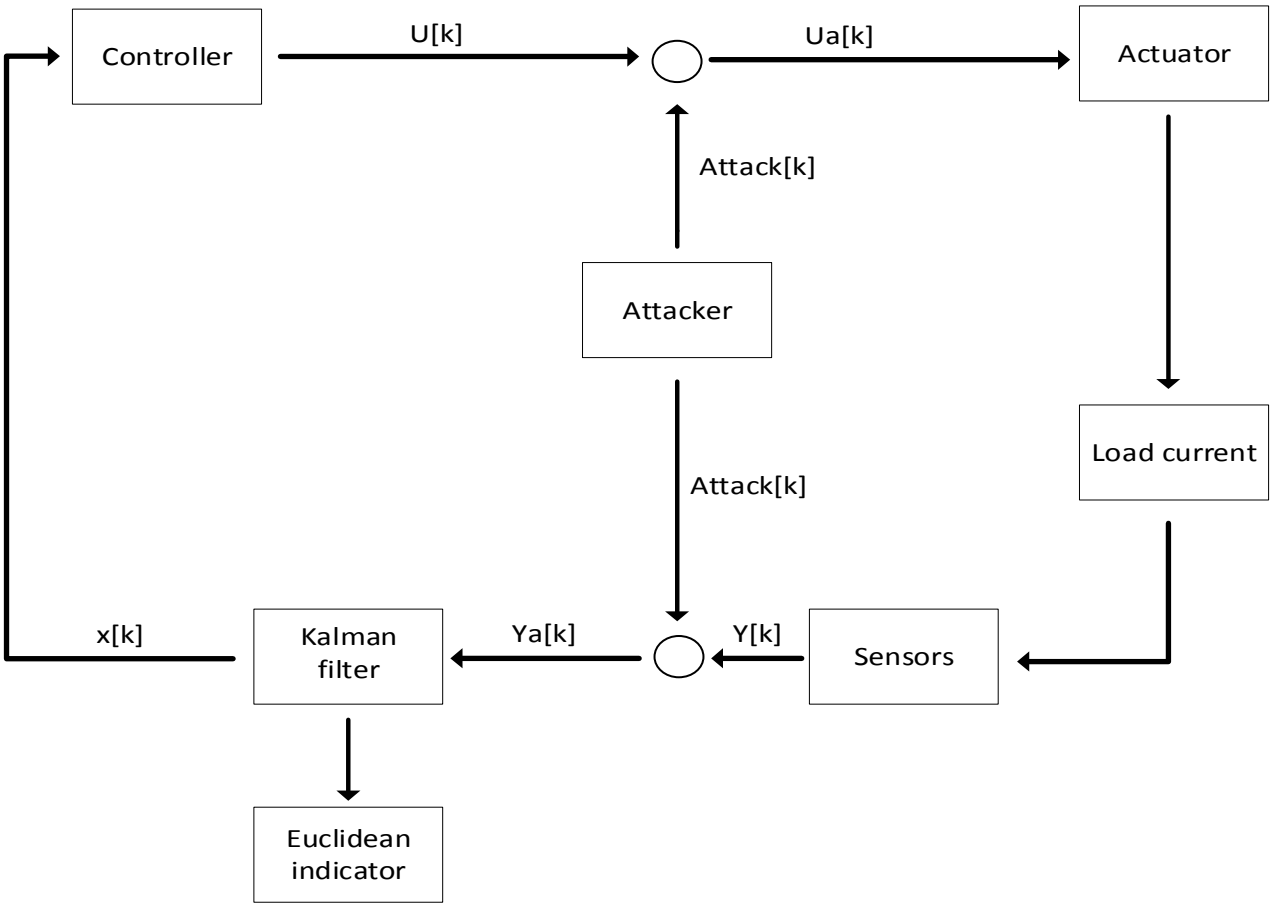


Figure 3-7 Block diagram of FDIA on forward ad feedback

For Kalman Filter in the system, the Euclidean-detector is chose to decide whether the FDI can be detected.

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots\cdots + (p_n - q_n)^2} \tag{3.14}$$

Which means the distance between measurement of Kalman Filter and estimation of Kalman Filter. Here, the d is defined smaller than 0.3. That means if the Euclidean distance of the injected attack is smaller than 0.3, the Kalman Filter can not detect.

Considering a false data injection attack, we assume cyber-attacker has enough information of system model. The cyber-attacker can also have the ability to command some sensors in system. The FDI attack model is expressed as

$$y'(t) = C(t)x'(t) + v(t) + y_a(t) \tag{3.15}$$

Where y_a is the malicious data from the attacker.

For the system investigated in this part, it is the same as Figure 2-2. The Kalman Filter with the Euclidean-detector is obtained:

$$\hat{x}(k+1|k) = A\hat{x}(k|k) + Bu(k) \tag{3.16}$$

$$\mathrm{P(k+1|k)} = \mathrm{AP(k|k)}A^T + \mathrm{Q} \tag{3.17}$$

$$\mathrm{K(k+1)} = \mathrm{P(k+1|k)}C(\mathrm{CP(k+1\,|\,k)\ C\hat{}T + R)^{-1}} \tag{3.18}$$

$$\hat{\mathrm{x}}\mathrm{(k+1|k+1)} = \hat{\mathrm{x}}\mathrm{(k+1|k)} + \mathrm{K(k+1)(y(k+1)} - \mathrm{C}\hat{\mathrm{x}}\mathrm{(k+1|k))} \tag{3.19}$$

$$\mathrm{P(k+1|k+1)} = \mathrm{(I - K(k+1)C)P(k+1|k)} \tag{3.20}$$

$$|y(k+1) - \hat{x}(k+1|k+1)| \leq d \tag{3.21}$$

So if the FDI attack satisfy:

$$\mathrm{attack(k)} = (\big(1 - \mathrm{Ck(k+1)}\big) * \hat{\mathrm{x}}\mathrm{(k+1|k)} + \mathrm{randi}([-1{,}1] * \mathrm{d}))/(1 - \mathrm{k(k+1)}) \quad (3.22)$$

Substitute system state equation into the (3.16)~(3.21).

$$\hat{\mathrm{i}}\mathrm{(k+1|k)}_{\alpha} = Ts/L(v_{\alpha} - \hat{\mathrm{i}}\mathrm{(k)}_{\alpha} * (R - L/Ts)) \quad (3.23)$$

$$\hat{\mathrm{i}}\mathrm{(k+1|k)}_{\beta} = Ts/L(v_{\beta} - \hat{\mathrm{i}}\mathrm{(k)}_{\beta} * (R - L/Ts)) \quad (3.24)$$

$$\mathrm{p(k+1|k)} = \frac{\mathrm{Ts}}{\mathrm{L}} * \left(\mathrm{R} - \frac{\mathrm{L}}{\mathrm{Ts}}\right) * \mathrm{p(k)} * \frac{\mathrm{Ts}}{\mathrm{L}} * \left(\mathrm{R} - \frac{\mathrm{L}}{\mathrm{Ts}}\right) + \mathrm{Qc} \quad (3.25)$$

$$\mathrm{K(k+1)} = \mathrm{P(k+1|k)}/(\mathrm{P(k+1|k)} + Rc) \quad (3.26)$$

$$\hat{\mathrm{x}}\mathrm{(k+1\,|\,k+1)}_{\alpha} = \hat{\mathrm{x}}\mathrm{(k+1|k)}_{\alpha} + \mathrm{K(k+1)}(\mathrm{attack(k+1)}_{\alpha} - \hat{\mathrm{x}}\mathrm{(k+1|k)}_{\alpha}) \quad (3.27)$$

$$\hat{\mathrm{x}}\mathrm{(k+1\,|\,k+1)}_{\beta} = \hat{\mathrm{x}}\mathrm{(k+1|k)}_{\beta} + \mathrm{K(k+1)}(\mathrm{attack(k+1)}_{\beta} - \hat{\mathrm{x}}\mathrm{(k+1|k)}_{\beta}) \quad (3.28)$$

$$\mathrm{P(k+1|k+1)} = (\mathrm{I} - \mathrm{K(k+1)})\mathrm{P(k+1|k)} \quad (3.29)$$

$$|attack(k+1) - \hat{x}(k+1|k+1)| \leq d \quad (3.30)$$

For the system, the FDI attack should satisfy (3.30) to avoid the Euclidean detector

$$(\mathrm{attack(k+1)}_{\alpha} - \hat{\mathrm{i}}\mathrm{(k+1|k)}_{\alpha})^2 + (\mathrm{attack(k+1)}_{\beta} - \hat{\mathrm{i}}\mathrm{(k+1|k)}_{\beta})^2 \leq (\mathrm{d}/(1 - \mathrm{k(k+1)}))^2 \quad (3.31)$$

So for the MPC, the control steps of the whole inverter system that is injected with special attack is displayed in Figure 3-8.

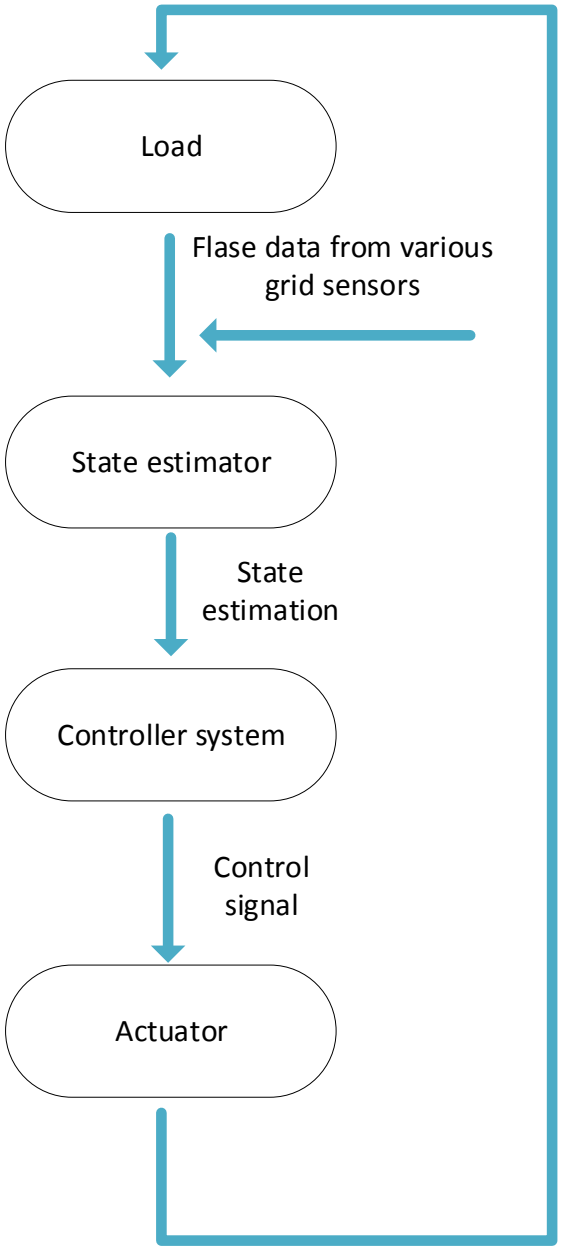


Figure 3-8 Block diagram of control steps

So as to demonstrate the correctness of attack model in this part, we get simulation results of the inverter system with the MPC strategy on the MATLAB/Simulink. The main circuit topology is the same as Figure 2-2. and the system parameters are the same as table 2-2.

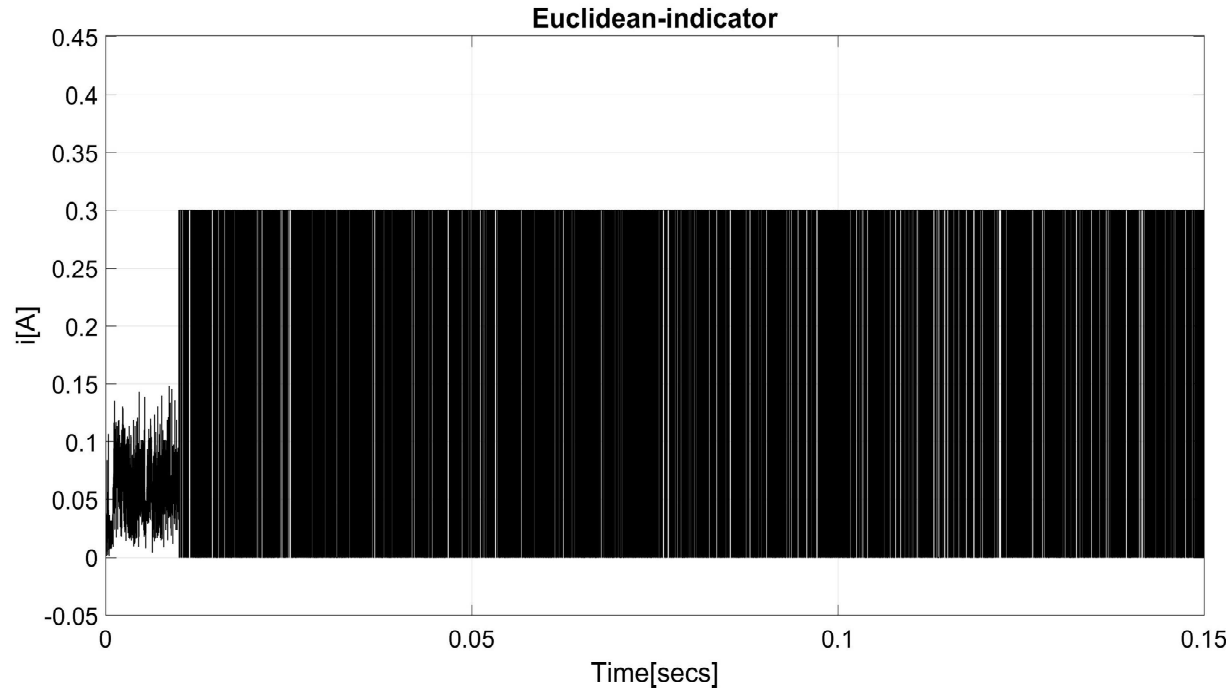


Figure 3-9 Euclidean indicator

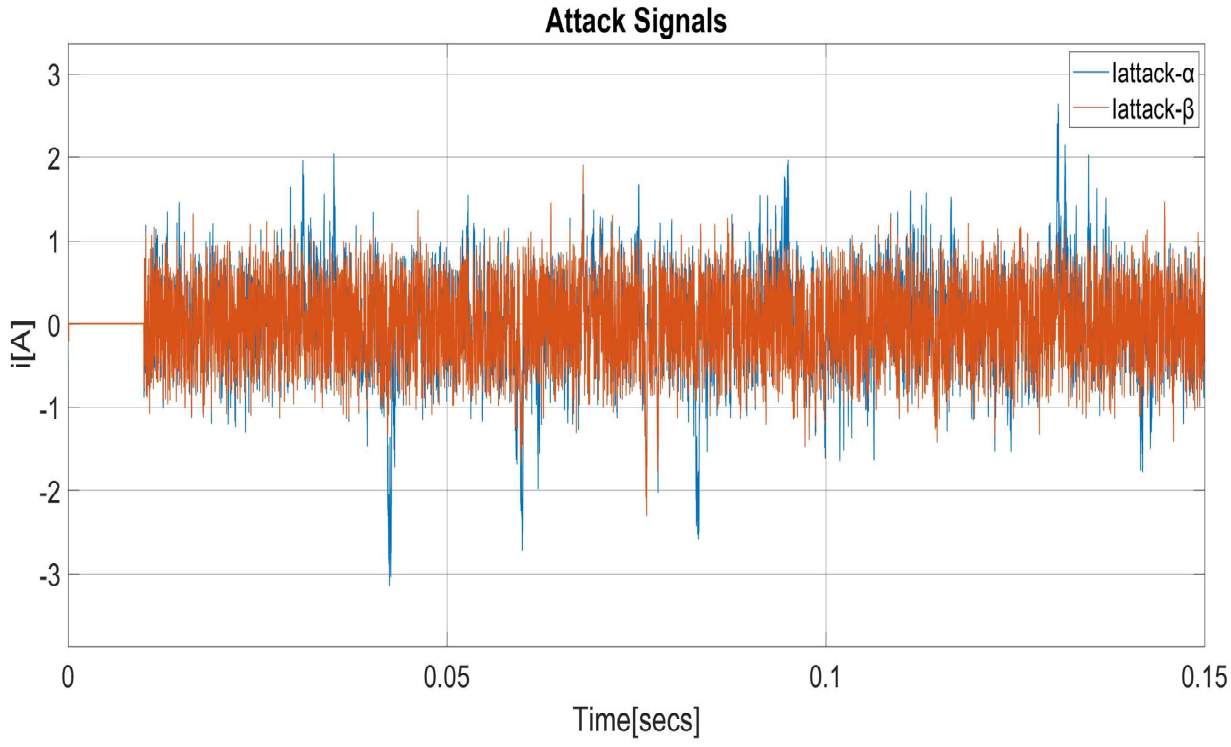
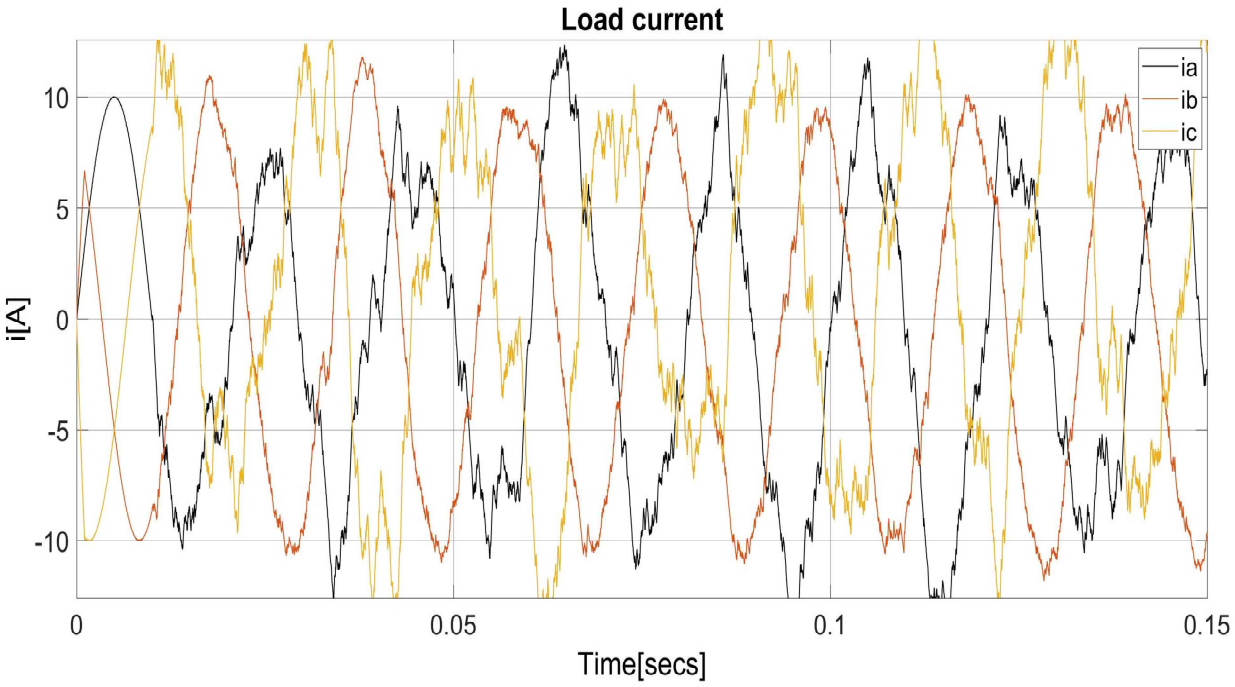


Figure 3-10 False data injecting attack



FFT analysis

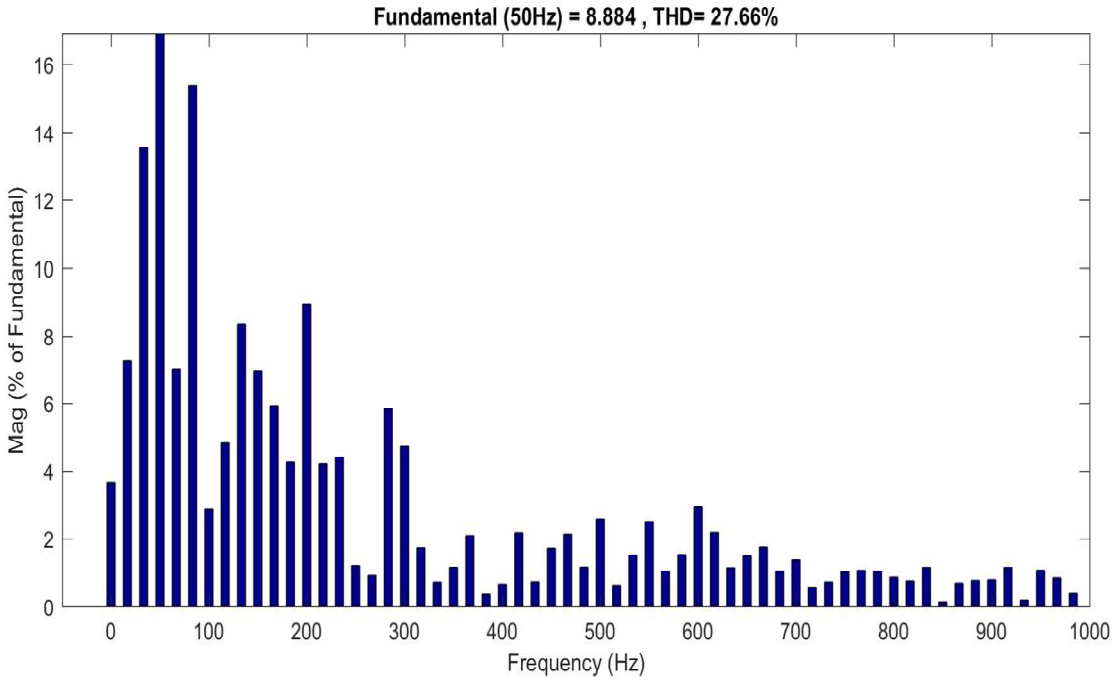


Figure 3-11 Model predictive control

From the Figure 3-9 it shows Euclidean-detector of Kalman Filter. From t=0.01 seconds, the false data is injected into system and indicator of Kalman Filter is defined below 0.3 which means the special attack can not trigger an alarm. Figure 3-10 shows the designed attack according to (3.31). We can see from Figure 3-11 that load current is unable to follow the reference current while the false data is considered into the inverter system. It shows the quality of the system output is bad with high THD.

3.5 Conclusion

The Gaussian noises on the feedback of the load current produced by the sensor is displayed in Figure 3-3. The inverter with the Kalman Filter shows the filtering ability in Figure 3-5. To some extend, the Kalman Filter can filter some noise in the system. From Figure 3-4 and Figure 3-5, the max noise amplitude reduce from 0.5 A to 0.38 A. Therefore, the Kalman Filter can filter some noise and the system with Kalman Filter shows better performance to track reference current when the noise exits in system.

In this chapter, firstly the basic Kalman Filter model is described and then the cascaded multilevel inverter with Kalman Filter is established. It can filter the noise in the system and increase the accuracy of current control. Then, the Euclidean-detector is defined whether the attacks can be detected and the alarm can be triggered. Finally, a special false data injection attack is designed though using the incomplete inverter system information which can not be detected by the Euclidean-detector of the Kalman Filter.

In general, Kalman Filter model are established and tested. For this model, first time updating and measurement equations are obtained from three-phase cascaded multilevel inverter system. Then, the noise which shows gaussian distribution from the sensors in the system is considered. The simulation results demonstrate the Kalman Filter can filter the noise in the system and increase the accuracy of current control. After that, based on the Kalman Filter model and the Euclidean-detector from the cyber-attacker perspective, a special attack model is designed that is undetectable. However, when the system injects the special attack, the simulation results show the conventional MPC can not keep the system stable and lose the ability to current control.

Future work can be focused on the following aspects: considering the impact of FDI attack and the bad data detection methods like the machine learning.

Chapter 4 Bad Data Detection

4.1 Introduction

Cyber-security has raised a lot of attention in the progress of smart grid. [22] proposed the measurements got from SCADA systems are faced with malicious false data injection (FDI) attacks. During the past years, various attack model and protection researches are done so as to understand the influence of FDI attacks. However, some special attacks are designed by cyber-attackers who have great information of the power network topology and system parameters so that these attacks are unbale to be distinguished by the conventional detectors such as the Kalman Filter.

For example, [22] demonstrated that if the cyber-attacker get enough information oft the network topology, it is possible to establish a set of special attacks that can dodge traditional bad data detection and enter the system. This kind of attack is defined as an unobservable cyber-attack [47].

Besides the traditional mathematical modeling research methods, FDIA detection approaches on account of artificial intelligence have been investigated in last years, such as neural network [49−50].Among them, some scholars think about machine learning methods for monitoring and controlling power systems [48-50]. [48] suggests an intelligent concept which is used for the system controller design, in which machine learning approaches make use of forecasting errors of the system. Vicious activity forecasting and intrusion detection issues have been analyzed by

considering machine learning techniques at the network layer of smart grid communication systems [49], [50].

In this chapter, we think about FDI attack and DOS attack aiming at sensor of the system and a deep-learning intelligent method is proposed to distinguish the FDI attack and DOS attack which is unable to be perceived by the Kalman Filter.

4.2 KNN Algorithm

The K-Nearest Neighbor (KNN) classification approach is one of the machine learning algorithms to make classification. The KNN algorithm first expresses the sample to be classified into a feature vector; then calculates the distance between the sample to be tested and each training sample according to the distance function, selects the K samples with the smallest distance as the neighbor samples; and finally according to the K neighbor samples determine the category of the sample to be classified. Among them, the definition of the sample distance mechanism directly affects the accuracy and efficiency of the KNN.

The principal idea of the KNN classification way is to first calculate distance between the sample to be classified and the training sample of the known category to find the nearest K neighbors; Then, according to the category which the K neighbor samples belong, the category of the sample data to be classified is determined: most of the K samples belong to a certain category, and the sample also belongs to this category.

Among them, the proximity of the sample mainly has two kinds of measurement methods: Euclidean distance and cosine similarity, and the calculation formula is as follows

$$\text{distance}(p_1, p_2) = \sqrt{\sum_{i=1}^{n}(p_{1i} - p_{2i})^2} \tag{4.1}$$

$$\cos(p_1, p_2) = \frac{\sum_{k=1}^{n} p_{1k} p_{2k}}{\sqrt{\sum_{i=1}^{n} {p_{1k}}^2}\sqrt{\sum_{i=1}^{n} {p_{2k}}^2}} \tag{4.2}$$

As a supervised learning algorithm, the KNN only needs to store training samples during the pattern learning phase, which is negligible. In the real-time classification stage, the entire pattern space needs to be traversed, and finally the type of the sample to be tested is obtained. If the pattern space is too large, the time required for each classification increases, and the demand for real-time classification cannot be satisfied. This is one of the inherent drawbacks in the supervised learning algorithm such as KNN compared to other active learning algorithms.

K-Nearest Neighbor (KNN) which is widely applied for classification assigns the S samples to the closest neighbors. The Euclidean distance is often made used to find the closeness

$$d_{i,j} = \|s_i - s_j\|, s_j \in s \tag{4.3}$$

For k =1, the forecasted class label y_i is given by the labeled sample closest to y_i:

$$y_i = argminy_i\{d_{ij}\} \tag{4.4}$$

For k>1, the majority voting is used to determine the eventual label from k nearest neighbors of s_i. K is the amount of closest neighbor that is chosen according to cross validation performance defined as 9.

Considering the circuit topology in Figure 2-2, for the training set, we get 2000*6 size of correct load current and bad load current from the system in order to have better performance of classification. First of all, the current data is obtained from the sensor $i_{current}$, and the estimation current data from pervious data can be expressed as

$$i_{current}(N-1) = \frac{Ts}{L} * (V(N+1) - \frac{Ts}{L} * \left(V(N-1) - i(N-1) * \left(R - \frac{Ts}{L}\right)\right) * \left(R - \frac{Ts}{L}\right) \quad (4.5)$$

$$i_{current}(N-2) = \frac{Ts}{L} * (V(N+1) - \frac{Ts}{L} * \left(V(N-1) - \frac{Ts}{L} * \left(V(N-2) - i(N-2) * \left(R - \frac{Ts}{L}\right)\right) * \left(R - \frac{Ts}{L}\right)\right) * (R - Ts/L) \quad (4.6)$$

$$i_{current}(N-3) = \frac{Ts}{L} * (V(N+1) - \frac{Ts}{L} * \left(V(N-1) - \frac{Ts}{L} * \left(V(N-2) - \frac{Ts}{L} * \left(V(N-3) - i(N-2) * \left(R - \frac{Ts}{L}\right)\right) * \left(R - \frac{Ts}{L}\right)\right) * \left(R - \frac{Ts}{L}\right)\right) * (R - Ts/L) \quad (4.7)$$

So the test data is defined as $[(i_{currenta\alpha} - i_{currenta\alpha}(N-1)), (i_{currenta\alpha} - i_{currenta\alpha}(N-2)), (i_{currenta\alpha} - i_{currenta\alpha}(N-3)), (i_{current\beta} - i_{current\beta}(N-1)), (i_{current\beta} - i_{current\beta}(N-2)), (i_{current\beta} - i_{current\beta}(N-3))]$.

If the data is correct that means it dose not include the attack, it will be labeled sample 1 and the data will be used by the MPC control. If the data is classified as bad information, it will be labeled sample 2 and the data that is used by the MPC control will from (4.8).

$$i_{current}(N) = 3i_{current}(N-1) - 3i_{current}(N-2) + i_{current}(N-3) \quad (4.8)$$

(4.8) is obtained from Lagrange's second-order extrapolation formula.

4. 3 Model Test

So as to demonstrate the correctness of the modified model predictive current control based on KNN, we get simulation results on the MATLAB/Simulink. Moreover, we also consider to FDI attack model in chapter 2.3 and chapter 3.4. The simulation results show the conventional MPC is hard to keep the system stable and the modified MPC based on KNN strategy can have a better performance to current control when the system suffers from the special FDI attack.

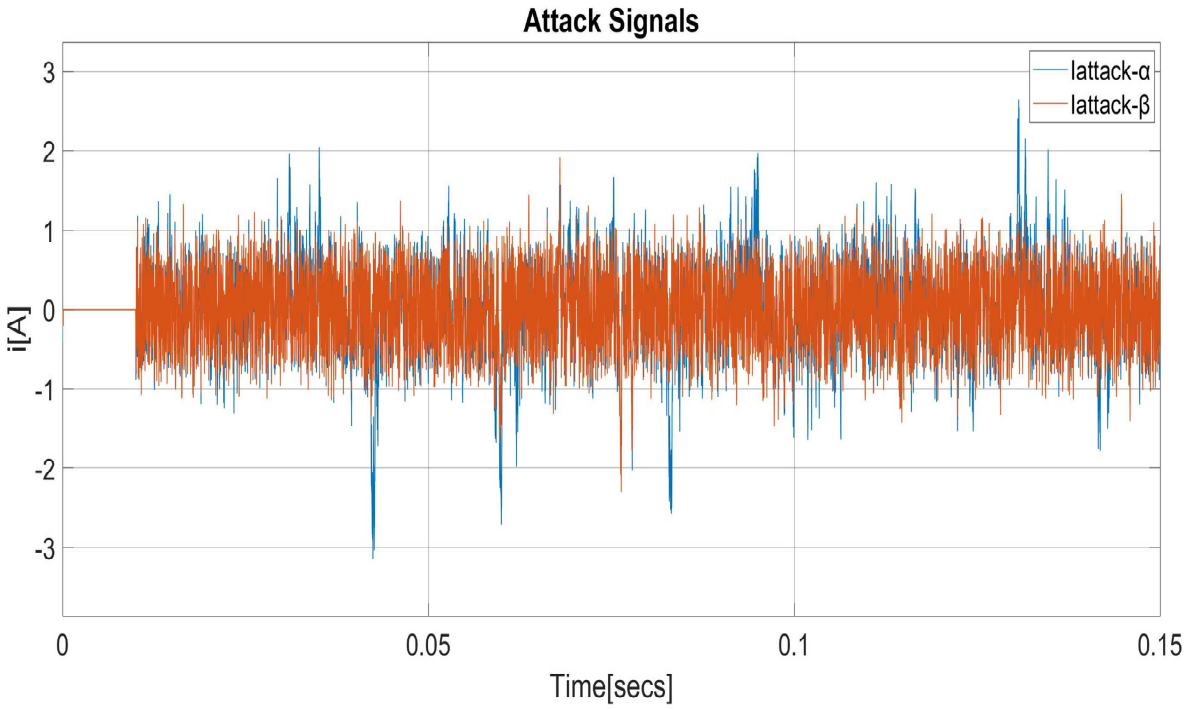


Figure 4-1 Attack model based on Kalman Filter

The system is injected with the special false data attack signal shown in Figure 4-1 on the sensors which is from 0.01 seconds which can not be detected by the Kalman Filter. Compare with the conventional MPC in chapter 3.4, the simulation results in Figure 4-2 demonstrate the load current can follow the reference current accurately with modified MPC based on KNN algorithm. The current control has better quality with low THD.

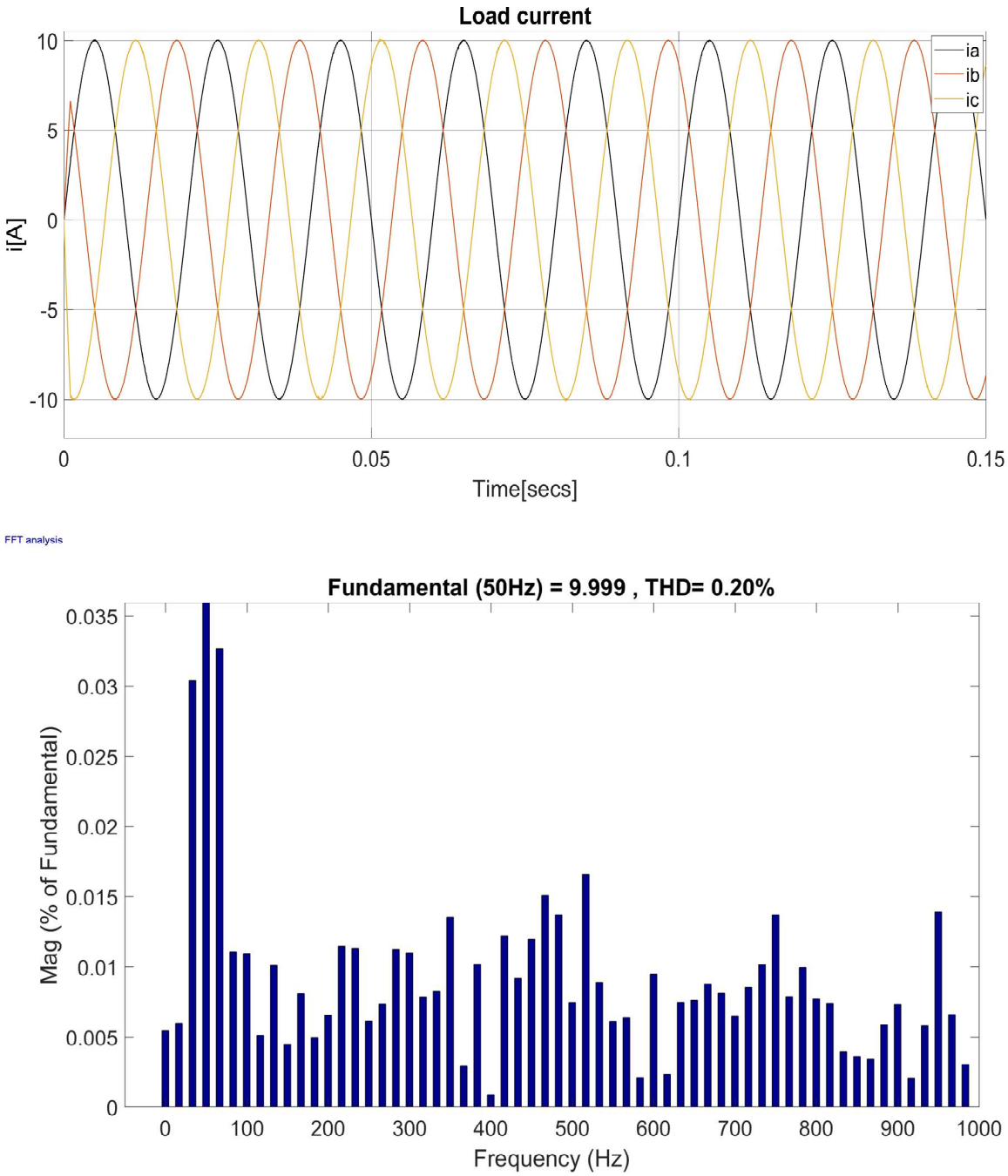


Figure 4-2 Modified model predictive control with KNN

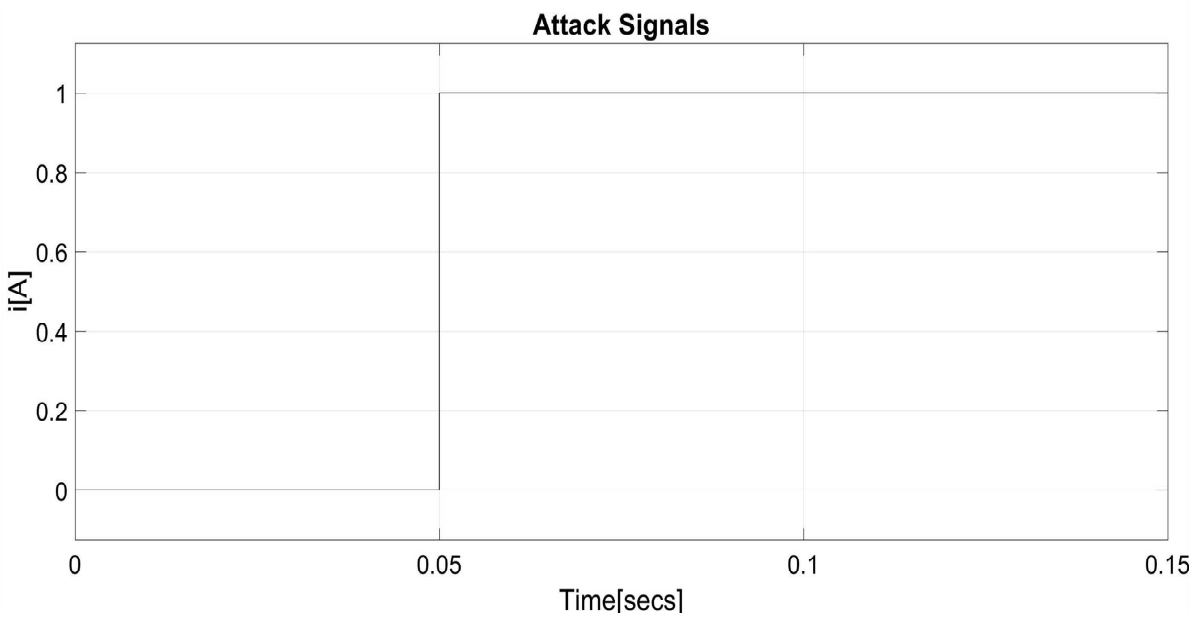


Figure 4-3 Step attack signals

The system is injected with the step attack signal shown in Figure 4-3 on the sensors which is from 0.05 seconds. Compare with the conventional MPC in chapter 2.2, the simulation results in Figure 4-4 demonstrate the load current can track the reference current accurately with the modified MPC based on KNN algorithm. The current control has better quality with low THD.

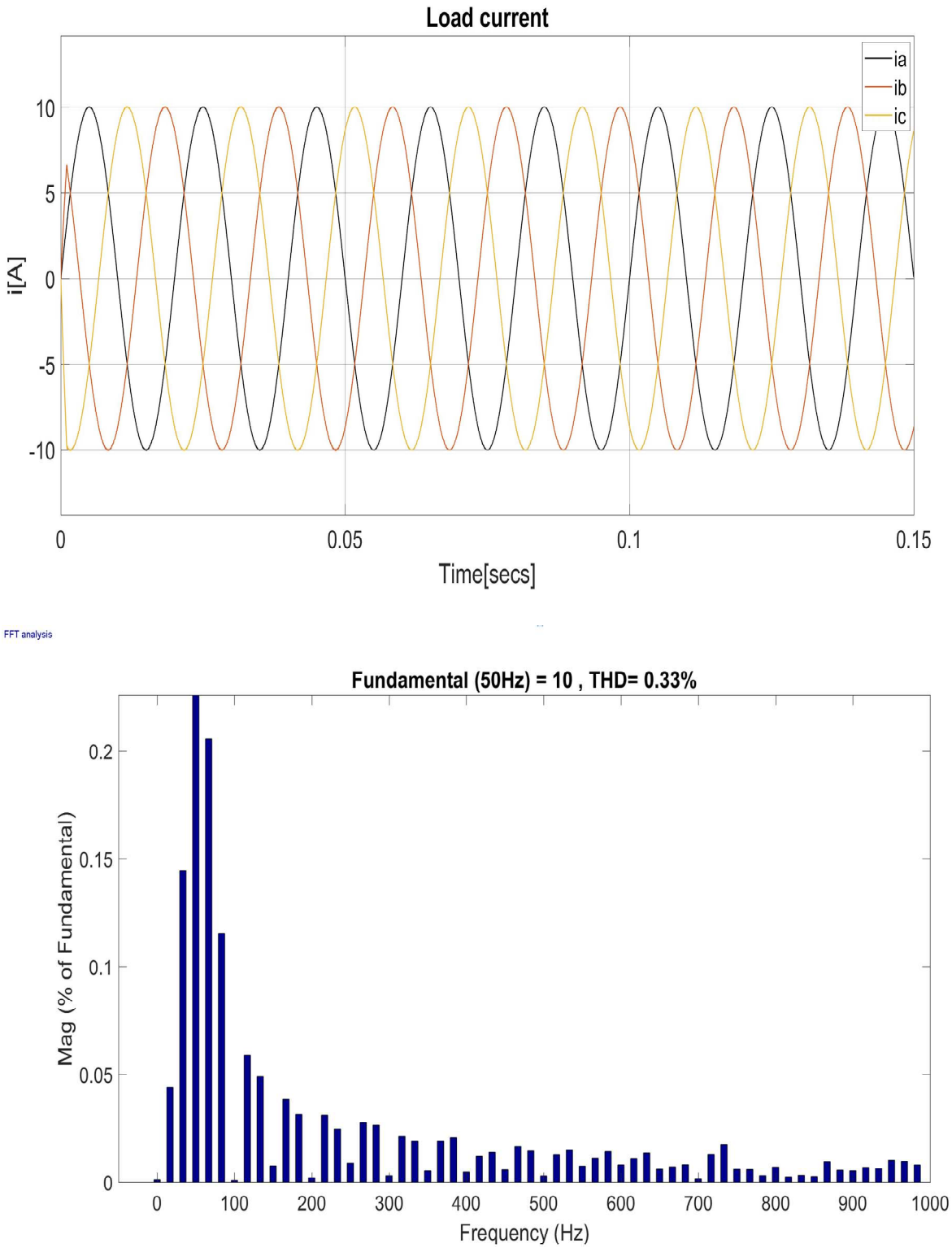


Figure 4-4 Modified model predictive control with KNN

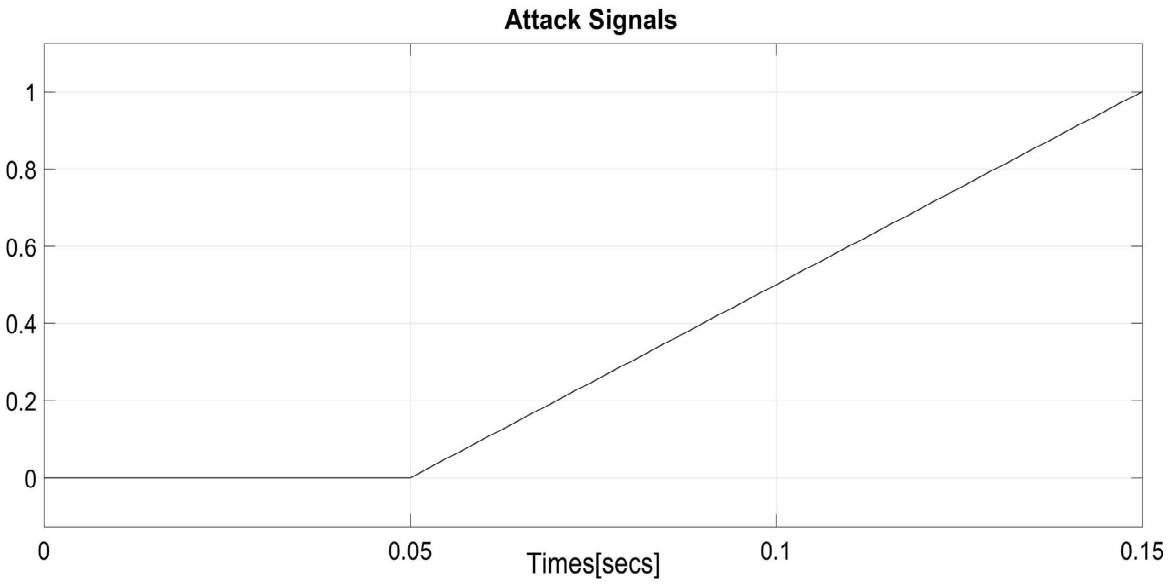


Figure 4-5 Ramp attack signals

The system is injected with the step attack signal shown in Figure 4-5 on the sensors which is from 0.05 seconds. Compare with the conventional MPC in chapter 2.2, the simulation results in Figure 4-6 demonstrate the load current can track the reference current accurately with the modified MPC based on KNN algorithm. The current control has better quality with low THD.

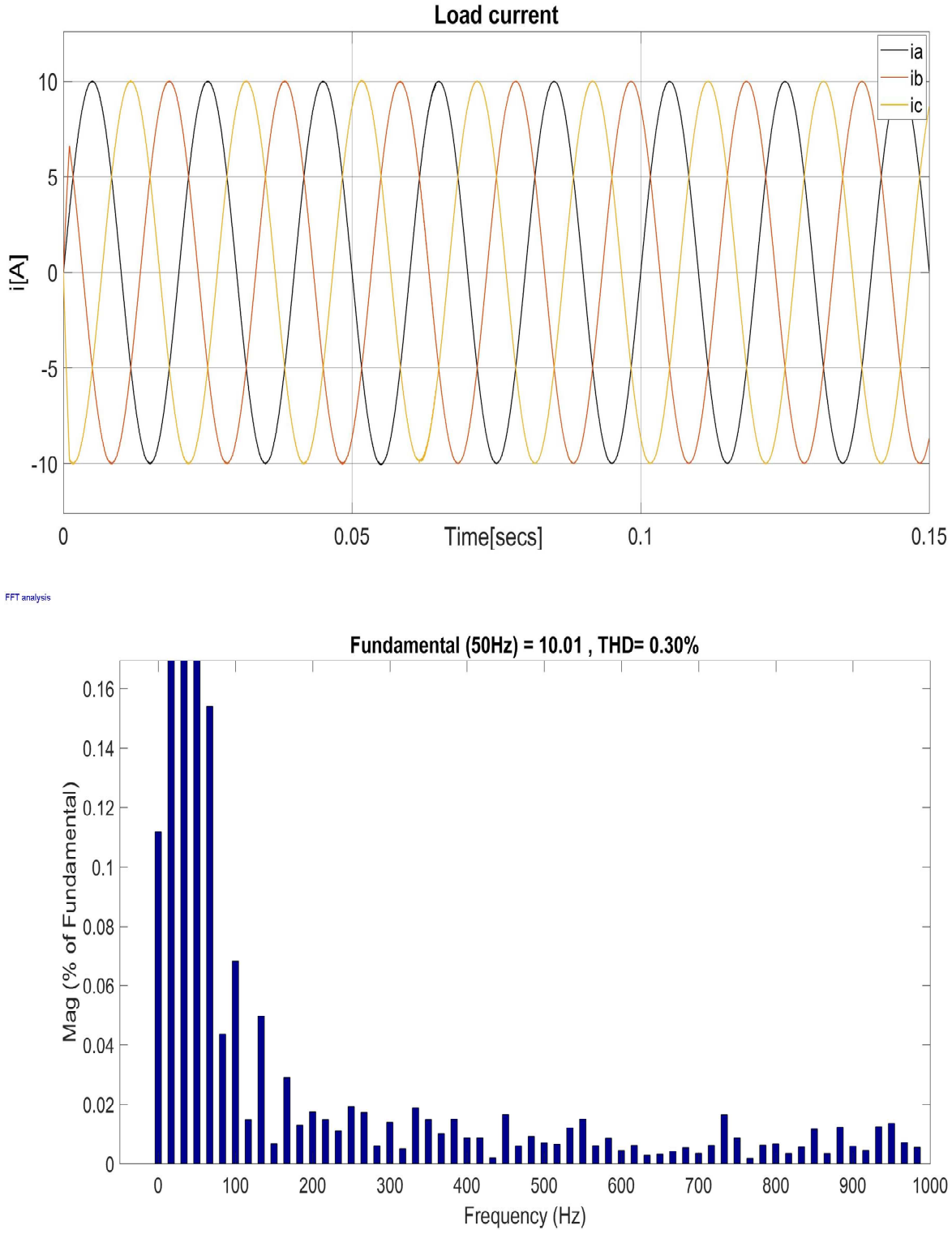


Figure 4-6 Modified model predictive control with KNN

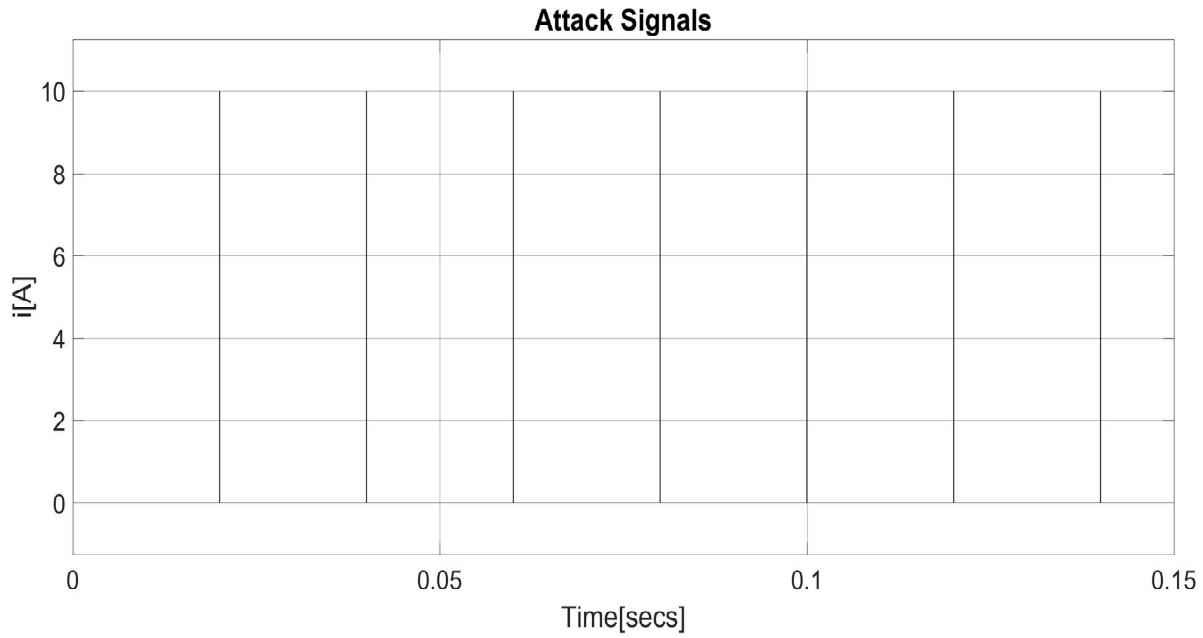


Figure 4-7 Pulse attack signals

The system is injected with the pulse attack signal shown in Figure 4-7 on the sensors which is from 0.05 seconds. Compare with the conventional MPC in chapter 2.2, the simulation results in Figure 4-8 demonstrate the load current can track the reference current accurately with the modified MPC based on KNN algorithm. The current control has better quality with low THD.

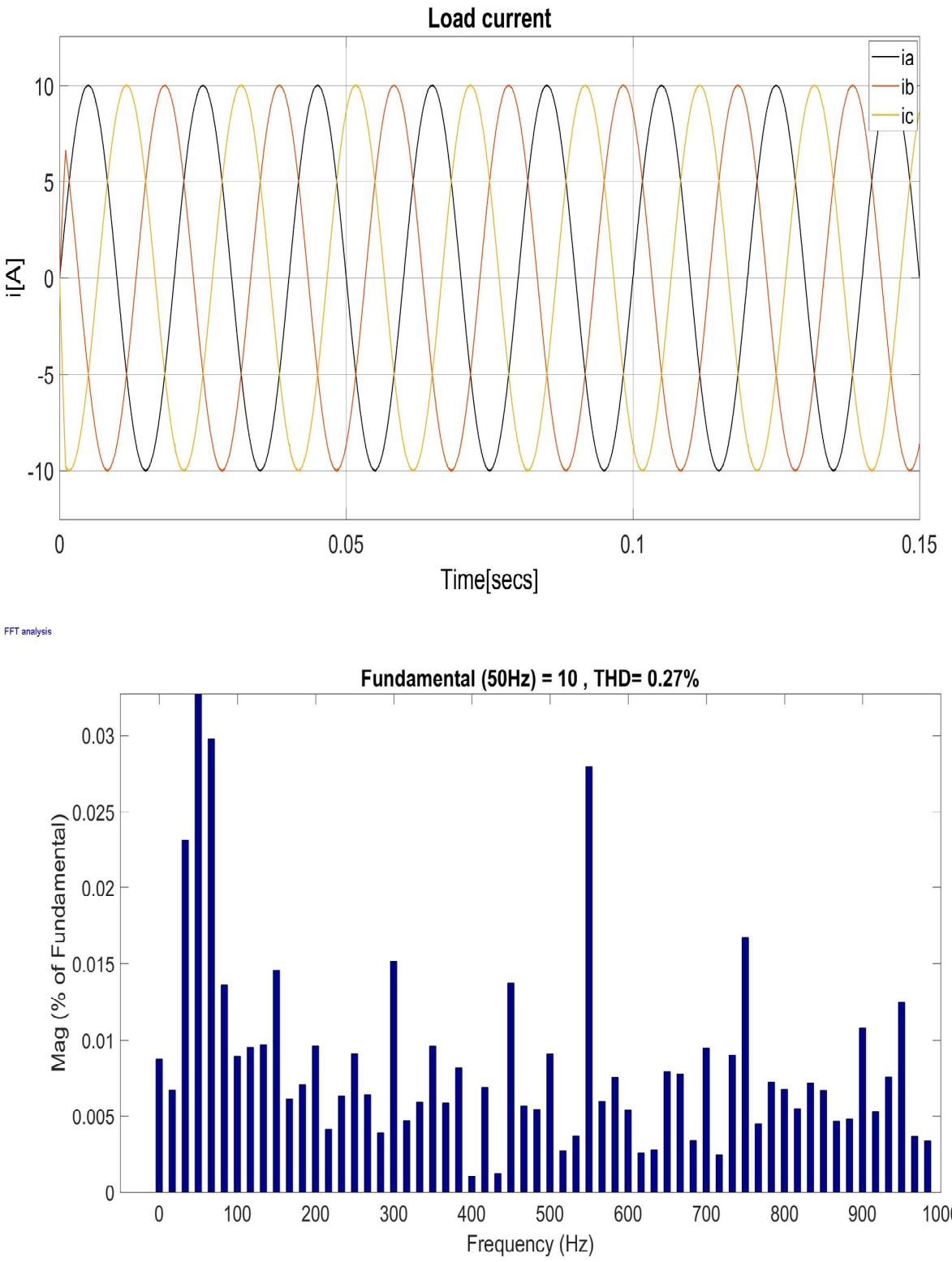


Figure 4-8 Modified model predictive control with KNN

4.4 Conclusion

In this chapter, KNN algorithm is considered to establish and a novel MPC strategy is proposed. For this strategy, firstly, the attack injected from sensors is detected by Kalman Filter using the Euclidean-distance indicator. If the attack is detected by the Euclidean-distance indicator of Kalman Filter, the system will make alarms. If the attack is undetectable and can enter the system, it can be firstly classified by the designed controller. The controller can distinguish the bad data and real data. After that, if the signal is detected as the bad data, the controller will use the previous data to make estimation for the current value; If the signal is correct, the controller will use the current value. The simulation results show the modified MPC based on KNN algorithm can achieve current control accurately when the system is injected various attack signals.

To test this model, we did the simulations in Simulink and consider four scenarios:

(1) By using the proposed MPC strategy for the CHB systems injected step false data to achieve the current control.

(2) By using the proposed MPC strategy for the CHB systems injected ramp false data to achieve the current control.

(3) By using the proposed MPC strategy for the CHB systems injected pulse false data to achieve the current control.

(4) By using the proposed MPC strategy for the CHB systems injected special false data designed in Chapter 3 to achieve current control.

In general, the proposed MPC strategy can perform well while the false data is injected into the inverter. The load current has high quality and the THD is less than 1%. The improved MPC shows great performance in current control of CHB systems, which can accurately forecast the future system response. Compared with the conventional MPC strategy, it can guarantee a better performance of current control when the FDI attack happens.

Chapter 5 Conclusion

This thesis investigates the cascaded multilevel system considered falsa data injection. A system model with Kalman Filter is established and a special attack model is designed. Finally, a modified MPC strategy that is developed based on the KNN algorithm in order to keep the system stable when FDIA happens on the sensors in the system.

Firstly, the three phase cascaded H-bridge system is established. So as to achieve the precise current control, the model predictive control is applied. The simulation results show the MPC method has fast response and achieves current control accurately. However, when considering some attacks such as pulse attack signals, step attack signals, the system using the generic MPC strategy is hard to keep a stable and effective current control. The case studies demonstrate that the generic MPC method does not have enough robust ability.

Then, Kalman Filter is designed for the state estimation in the three phase cascaded H-bridge system when the system has Gaussian noises. The Gaussian noises are the measurement noises on the feedback of the load current produced by though the sensor. The simulation results show the inverter system with the Kalman Filter has the filtering ability and the max noise amplitude reduces from 0.5 A to 0.38 A. Therefore, the Kalman Filter can filter some noise and the system with Kalman Filter shows better performance to track reference current when the noise exits in system.

After that, from the view of the cyber-attacker, it is assumed that cyber-attacker can manipulate the data transmitted by the target system in the network. A detection indicator is defined using the Euclidean-distance which means if the indicator exceeds the set value, the system will

trigger an alarm. A sophisticated FDI attack sequence is designed based on the Kalman Filter, its indicator and system parameters. The purpose is that the attack signal can bypass the detection of the Kalman Filter to make the object of the system controlled object deviate from the given reference signal. Moreover, the conventional MPC strategy loses the ability of current control when the sophisticated attack injected into system.

Lastly, considering machine learning approaches that are widely applied in the smart grid to monitor and control power systems, a modified MPC combined with the KNN algorithm is proposed in the thesis. The novel approach detects the bad data that can enter the system without triggering alarms. The case studies show the modified MPC based on the KNN algorithm can achieve current control accurately when the system is injected with various attack signals.

Future work can be focused on the following aspects:

1. Considering an unsupervised learning method to modify MPC strategy because the KNN algorithm which is a supervised learning method requires a lot of training set.
2. Considering the system uncertainty and the robust model predictive control methods such as the disturbance compensator, min-max control model.
3. The KNN algorithm sometimes can not recognize the bad data that is close to real data, therefore it is not sufficient for all the false data injection attacks and other methods can be taken into account to enhance the control accuracy.
4. Modifying the MPC strategy and reducing the computation burden of MPC. The computation time for the MPC strategy increases with the number of the voltage vectors. So for the multilevel cascaded inverters that have many voltage vectors, the computation

is heavier and it essential to investigate the ways to decrease the computation times.

References

[1] P. Qashqai, A. Sheikholeslami, H. Vahedi et al., "A review on multilevel converter topologies for electric transportation applications", Proc. VPPC 2015, pp. 1-6.

[2] Y. Yu, G. Konstantinou, B. Hredzak et al., "Power balance of cascaded H-bridge multilevel converters for large-scale photovoltaic integration", IEEE Trans. Power Electron., vol. 31, no. 1, pp. 292-303, 2016.

[3] S. Kouro, M. Malionowski, K. Gopakumar et al., "Recent advances and industrial applications of multilevel converters", IEEE Trans. Ind. Electron., vol. 57, no. 8, pp. 2553-2580, 2010.

[4] J. Rodriguez, J.-S. Lai, F. Z. Peng, "Multilevel inverters: A survey of topologies controls and applications", IEEE Trans. Ind. Electron., vol. 49, no. 4, pp. 724-738, Aug. 2002.

[5] L. Tolbert, F. Z. Peng, T. Habetler, "Multilevel converters for large electric drives", IEEE Trans. Ind. Electron., vol. 35, no. 1, pp. 36-44, Jan./Feb. 1999.

[6] J. Rodriguez, S. Bernet, B. Wu, J. O. Pontt, S. Kouro, "Multilevel voltage-source-converter topologies for industrial medium-voltage drives", IEEE Trans. Ind. Electron., vol. 54, no. 6, pp. 2930-2945, Dec. 2007.

[7] A. Marzoughi, R. Burgos, D. Boroyevich et al., "Investigation and comparison of cascaded H-bridge and modular multilevel converter topologies for medium-voltage drive application", Proc. IECON 2014, pp. 1562-1568.

[8] P. Antsaklis, "Goals and challenges in cyber-physical systems research editorial of the editor in chief", *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3117-3119, Dec. 2014.

[9] G. Liang, S. R. Weller, J. Zhao, F. Luo, Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks", *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317-3318, Jul. 2017.

[10] X. Fang, S. Misra, G. Xue et al., "Smart grid – the new and improved power grid: a survey", *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 944-980, 2012.

[11] Y. M. Atwa, E. F. El-Saadany, M. M. A. Salama, R. Seethapathy, "Optimal renewable resources mix for distribution system energy loss minimization", *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 360-370, 2010.

[12] P. Qashqai, A. Sheikholeslami, H. Vahedi et al., "A review on multilevel converter topologies for electric transportation applications", Proc. VPPC 2015, pp. 1-6.

[13] Y. Mo, T.H.J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig et al., "Cyber–physical security of a smart grid infrastructure", *Proc. IEEE*, vol. 100, no. 1, pp. 195-209, 2012.

[14] H. He, J. Yan, "Cyber-physical attacks and defenses in the smart grid: a survey", *IET Cyber-Phys. Syst. Theory Appl.*, vol. 1, no. 1, pp. 13-27, 2016.

[15] C. W. Ten, C. C. Liu, G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems", *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[16] C. Vellaithurai, A. Srivastava, S. Zonouz, R. Berthier, "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures", *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566-575, March 2015.

[17] G. N. Sorebo, M. C. Echols, Smart Grid Security: An End-to-End View of Security in the New Electrical Grid, Boca Raton, FL, USA:CRC Press, 2011.

[18] S. Amin, A. Cárdenas, S. Sastry, "Safe and secure networked control systems under denial-of-service attacks", *Hybrid Syst.: Comput. Control*, vol. 5469, pp. 31-45, Apr. 2009.

[19] O. Kosut, L. Jia, R. J. Thomas, L. Tong, "Malicious data attacks on the smart grid", *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[20] G. Liang, J. Zhao, F. Luo, S. R. Weller, Z. Y. Dong, "A review of false data injection attacks against modern power systems", *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630-1638, Jul. 2017.

[21] S. Sridhar, A. Hahn, M. Govindarasu, "Cyber–physical system security for the electric power grid", *Proc. IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012.

[22] Y. Liu, P. Ning, M. K. Reiter, "False data injection attacks against state estimation in electric power grids", *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, pp. 13:1-13:33, Jun. 2011.

[23] Y. Mo, E. Garone, A. Casavola, B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks", *Proc. 49th IEEE Conf. Dec. Control*, pp. 5967-5972, Dec. 2010.

[24] H. Li, L. Lai, W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid", *IEEE Trans. Smart Grid*, vol. 2, no. 3, pp. 476-486, Sep. 2011.

[25] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, X. Shen, "A lightweight message authentication scheme for smart grid communications", *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675-685, Dec. 2011.

[26] Q. Li, G. Cao, "Multicast authentication in the smart grid with one-time signature", *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 686-696, Dec. 2011.

[27] B. Sikdar, J. Chow, "Defending synchrophasor data networks against traffic analysis attacks", *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 819-826, Dec. 2011.

[28] K. Manandhar, X. Cao, F. Hu et al., "Detection of faults and attacks including false data injection attack in smart grid using kalman filter", *IEEE Trans. Control Netw. Syst.*, vol. 1, pp. 370-379, 2014.

[29] M. Govindarasu, A. Hann, P. Sauer, "Cyber-physical systems security for smart grid", *Future Grid Initiative White Paper*, 2012.

[30] Y. Liu, M. K. Reiter, P. Ning, "False data injection attacks against state estimation in electric power grids", *Proc. ACM Conf. Comput. Commun. Security*, pp. 21-32, 2009-Nov.

[31] Y. Liu, P. Ning, M.K. Reiter, "False data injection attacks against state estimation in electric power grids", *ACM Trans. Inf. Syst. Secur.*, vol. 14, pp. 13, 2011.

[32] Y. Huang, M. Esmalifalak, H. Nguyen et al., "Bad data injection in smart grid: attack and defense mechanisms", *IEEE Commun. Mag.*, vol. 51, pp. 27-33, 2013.

[33] Q. Yang, J. Yang, W. Yu et al., "On false data-injection attacks against power system state estimation: modeling and countermeasures", *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, pp. 717-729, 2014.

[34] Z. Hu, Y. Wang, X. Tian, X. Yang, D. Meng, R. Fan, "False data injection attacks identification for smart grids", *Third International Conference on Technological Advances in Electrical Electronics and Computer Engineering (TAEECE)*, pp. 139-143, April - May 2015.

[35] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, T. J. Overbye, "Detecting false data injection attacks on DC state estimation", *Proc. 1st Workshop Secure Control Syst.*, pp. 226-231, 2010.

[36] Y. Chakhchoukh, H. Ishii, "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations", *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4395-4405, Nov 2016.

[37] Y. Gu, T. Liu, D. Wang, X. Guan, "Bad data detection method for smart grids based on distributed state estimation", *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 4483-4487, Jun. 2013.

[38] M. Cramer, P. Goergens, A. Schnettler, "Bad data detection and handling in distribution grid state estimation using artificial neural networks", *Proc. IEEE Eindhoven PowerTech*, pp. 1-6, Jun. 2015.

[39] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks", *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580-1590, Jul. 2017.

[40] Li S, Yılmaz Y, Wang X D. Quickest detection of false data injection attack in wide-area smart grids. IEEE Transactions on Smart Grid, 2015, 6(6): 2725−2735

[41] H. M. Khalid, J.C.-H. Peng, "Immunity Toward Data-Injection Attacks Using Multi sensor Track Fusion-Based Model Prediction", *IEEE Trans. Smart Grid*.

[42] Y. He, G. J. Mendis, J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism", *IEEE Trans. Smart Grid.*, vol. 8, no. 5, pp. 2505-2516, Sep. 2017.

[43] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, H. V. Poor, "Machine learning methods for attack detection in the smart grid", *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773-1786, Aug. 2016.

[44] S. Vazquez, J. Leon, L.G. Franquelo et al., "Model predictive control: a review of its applications in power electronics", IEEE Ind. Electron. Mag., vol. 8, no. 1, pp. 16-31, 2014.

[45] J. Rodriguez, J. Pontt, C.A. Silva et al., "Predictive current control of a voltage source inverter", IEEE Trans. Ind. Electron., vol. 50, no. 1, pp. 495-503, 2007.

[46] M. Chaves, E. Margato, J. F. Silva, S. F. Pinto, J. Santana, "Fast optimum-predictive control and capacitor voltage balancing strategy for bipolar back-to-back NPC converters in high-voltage direct current transmission systems", IET Gener. Transmiss. Distrib., vol. 5, no. 3, pp. 368-375, Mar. 2011.

[47] R. Deng, G. Xiao, R. Lu, H. Liang, A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks impacts and defense: A survey", IEEE Trans. Ind. Informat., vol. 13, no. 2, pp. 411-423, Apr. 2017.

[48] C. Rudin et al., "Machine learning for the New York City power grid", *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 2, pp. 328-345, Feb. 2012.

[49] Z. M. Fadlullah, M. M. Fouda, N. Kato, X. Shen, Y. Nozaki, "An early warning system against malicious activities for smart grid communications", *IEEE Netw.*, vol. 25, no. 5, pp. 50-55, Sep./Oct. 2011.

[50] Y. Zhang, L. Wang, W. Sun, R. C. Green, M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids", *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796-808, Dec. 2011.