Replay Attack Detection in Smart Grids using Switching Multi-sine Watermarking

Harsh Rajnikant Patel

A Thesis in

The Department

of

Electrical & Computer Engineering

Presented in Partial Fulfillment of the

Requirements for the Degree of

Master of Applied Science (Electrical & Computer Engineering) at

Concordia University

Montreal, Quebec, Canada

September 2023

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: Harsh Rajnikant Patel

Entitled: Replay Attack Detection in Smart Grids using Switching Multi-sine Watermarking

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science (Electrical & Computer Engineering)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Luiz A. C. Lopes

_____ External Examiner
Dr. Wen-Fang Xie (MIAE)

_____ Examiner
Dr. Pragasen Pillay

_____ Supervisor
Dr. Shahin Hashtrudi Zad

Approved by _____
Dr Yousef R. Shayan, Chair
Department of Electrical & Computer Engineering

_____ 2023

_____
Mourad Debbabi, Dean
Faculty of Engineering and Computer Science

Abstract

Replay Attack Detection in Smart Grids using Switching Multi-sine Watermarking

Harsh Rajnikant Patel

Cyber-Physical Systems (CPS) are systems that include physical and computational components linked by communication channels. In a Smart Grid (SG), the power plants and loads communicate with supervisors (Central Controllers (CC)) for managing the power demand more efficiently. As such, a smart grid can be regarded as a CPS. The computational components and communication links of a CPS can be subject to cyber-attacks. Researchers have been exploring detection and mitigation strategies for various types of cyber-attacks.

An important type of attack is the replay attack for which various strategies based on watermarking signals have been proposed. One such scheme is based on switching multi-sine waves as the watermarking signal. This thesis adapts this scheme and develops a design procedure for detecting replay attacks for smart grids. Specifically, it examines the places in a grid where the watermarking signal can be injected and presents guidelines for choosing the amplitude and frequencies of sine waves that suit smart grids.

One of the drawbacks of using a watermarking signal is the additional control cost (i.e., decrease in performance). In the context of smart grids, watermarking results in small fluctuations in delivered power. This thesis extends the single-input-single-output watermarking to a two-input-two-output watermarking scheme for smart grids in such a way to considerably lower grid power fluctuations due to watermarking. The proposed method is verified using a simulated grid connected inverter-based plants. Simulation results show that using the suggested strategy, the effect of watermarking on the overall grid power reduces significantly.

Acknowledgements

I would like to express my gratitude to my supervisor Dr Shahin Hashtrudi Zad for giving me the opportunity to work under his guidance at Concordia University. His support and advice carried me through all the stages of research and writing this thesis. I would also like to thank Dr Antonio Carlos Zambroni de Souza and Dr Luiz A. C. Lopes for the continuous discussions throughout the research. Moreover, I must thank my family for their unconditional love and encouragement. This work is dedicated to them. My special thanks to my friend and colleague Alok Patel for the help.

I can never forget one of the Hindu devotional songs (*bhajan*) which gave me constant hope and encouraged throughout my life. It also helped me during my thesis in every possible aspect. One of the lines from that *bhajan* says:

હરિ હળવે હળવે હંકારો મારું ગાડું ભરેલ ભારે,
મેં તો લગામ દીધી હાથ હરિને પ્રભુ ચાહે તો પાર ઉતારો...

(Hari haḷve haḷve hankāro mārū gāḍu bharel bhāre,
Me to lagām dīdhī hāth Harine Prabhu chāhe to pār utāro...)

Oh Lord Hari, drive gently, my cart is full,

I let go of the reins to you, now its up to you…

Table of Contents

List of Figures

List of Tables

Abbreviations

CPS	Cyber-Physical System
CC	Central Controller
SG	Smart Grid
SISO	Single-Input Single-Output
LTI	Linear Time Invariant
MIMO	Multi-Input Multi-Output
ARMAX	Autoregressive–Moving-Average model with exogenous inputs
MPC	Model Predictive Control
IBR	Inverter Based Resources
MSC	Machine Side Converter
GSI	Grid Side Inverter
PV	Photovoltaic
KVL	Kirchhoff's Voltage Law
PMSG	Permanent Magnet Synchronous Generator
VSI	Voltage Source Inverter
PLL	Phase Locked Loop

SVPWM Space Vector Pulse Width Modulation

PoM Point of Measurement

Chapter 1

Introduction

Cyber-Physical Systems (CPS) incorporate cyber and physical layers. A CPS contains physical devices such as sensors and actuators which are linked to the central computational device (for example, Supervisory Control and Data Acquisition system, SCADA) through communication links.

Basically, a CPS integrates and coordinates between several components to form a reliable system and runs its tasks more efficiently. In a CPS, a large-scale system is created in which several components are interconnected with each other through a cyber layer and interact with the physical world. Nowadays, CPS are used in many applications including air traffic control, intelligent transportation, Internet of Things (IoT), medical monitoring etc. Smart grid (SG) is one of the best examples of a CPS in a power grid. A SG integrates several plants and loads that are physically far away from each other. This can be helpful in managing electric power efficiently, so that there would be less waste of energy and resources. Additionally, through smart meters, measuring energy consumption and dealing with fault detection becomes easier and more efficient.

Despite the advantages and importance of using CPS, the use of CPS gives rise to some challenges. The complexity of integrating conventional systems requires years of research for analysis and design. More importantly, forming a link between physical layers through cyber layer can pose security threats which can affect the entire system connected to it. This could cause a major harm to economy, national security and even worse, could result in injury or death. In smart grids, while controlling and managing all the plants unattended by using central controller (CC)

can provide flexibility, it also gives attackers similar flexibility and opportunity to harm the widespread systems easily. As all the plants and loads are connected to a central controller and causing harm to single or a group of plants and loads or CC can quickly transfer the attack to the whole power grid. This could result in a blackout for an entire region.

The attacks against CPS are known as Cyber-Physical attacks. Based on available system knowledge and resources, attackers can create different types of attacks, such as **False Data Injection attack (FDI)**, **Denial of Service attack (DoS)**, **Covert attack** and **Zero Dynamics attack**. All these attacks require either full or some knowledge of the system, which makes them more difficult to implement. In **Replay attack**, however, attackers do not need the knowledge of the system, but they need sensor measurements data. In this type of integrity attack, attackers know when the system is expected to be in steady state. At first, an attacker records the data for a certain period and then in the next phase, the attacker replays the same data recorded at the measurement devices while manipulating the inputs of the system. This attack is not detectable by the controller using passive methods which determine the abnormalities in the system through monitoring sensor outputs. The reason is that the data received by the controller is the same healthy data from the past. Therefore, replay attack can be stealthy and difficult to detect. In 2011, Stuxnet worm clearly indicated the importance of taking replay attacks more seriously. That was the first known attack, where attackers used the replay attack method. Stuxnet modified the data for the SCADA system of the uranium enrichment facilities in Iran. Attackers manipulated pressure inside the centrifuges and changed the speed of it, causing damage to approximately 1000 of centrifuges [1]. To stay undetectable, the attacker first recorded the data of normal operation for hours and then repeated the same data on measurement sensors during the attack phase.

The smart grid is widespread and not all the plants, substations and measurement points can be under strict physical security all the time, which provides attackers more opportunities to implement replay attacks.

To stop replay attacks, the system should be able to detect and be resilient at the same time. One way to detect a replay attack is by adding a watermarking signal (also called an authentication signal) into measurement data being sent through communication lines. Thus, attackers will not be able to filter out the actual signal easily and use it for replay attack. In CPS, especially smart grids, there are many interconnected transmission and communication lines. This makes it difficult to

efficiently watermark all the communication channels, not to mention problems that can come while using watermarking. Researchers suggested many optimal authentication methods to detect the replay attack while minimizing the undesirable effects of watermarking on the system. This thesis is concerned with the case of watermarking for the detection of replay attacks in smart grids. We begin in the next section with a brief review of several proposed methods.

1.1 Literature Review

1.1.1 Cyber-physical Attacks

Over the years, researchers have been studying the concept of CPS in different areas. While doing so, many authors explored the possible security attacks and proposed different solutions to different attacks in related fields (see, e.g. [2]–[4]).

An attack can be targeted on various components and signals. Depending on the target, the attacks can be divided into different types. Here we briefly review various types of attacks on control systems. Attacks are grouped to DoS and deception attacks.

In DoS attack, an attacker prevents the data, transferring from controller to actuator and/or sensors to controller. The attacker does not need to read the data or know the system dynamics. In 2015, using Cyber-Physical attack known as Disrupted Denial of Service (DDoS) on Ukraine power grid, attackers managed to disrupt the power systems in 3 regions [5]. This caused a power loss of approximately 130 MW. Roughly, 225,000 consumers faced power outage for almost 6 hours.

Next, we review deception attacks.

In FDI attack, attackers try to inject maximum error while being careful of not getting detected by the detector [6]. By injecting error, attackers try to push the system dynamics into unstable mode. The target of the attack could be actuators and/or sensors. For this, the attacker needs to have a knowledge of system parameters and detection mechanisms.

In Covert attack, attackers have flexibility to read and manipulate the input while managing the output in a way that the effect of the attack is cancelled in the output and hence, it cannot be detected by the detector. Of course, attackers need to know the system dynamics and have access to the sensors.

Using the system states and model, attackers create Zero Dynamics attack by injecting an attack in the input such that it makes the system state unbounded. It is an open-loop FDI which uses the knowledge of the system to produce zero effect on the output y.

The last type of deception attack is the replay attacks which will be discussed in the next section. The summary of each attack is given in Table 1.1. The sources where the attacker can read the information are called **Disclosure resources**. **Disruptive resources** are the channels where the attacker has the ability to inject or modify the data.

Table 1.1 Types of attacks with requirements (in terms of access)

Types of Attack	**Access**
Denial of Service	Disruptive or Disclosure resources
False Data Injection	System knowledge, Disruptive and Disclosure resources
Covert Attack	System knowledge, Disruptive and Disclosure resources
Zero Dynamics Attack	System knowledge and Disruptive resources
Replay attack	Disruptive and Disclosure resources

1.1.2 Replay attacks

Just before Stuxnet attack was discovered in 2010, Mo and Sinopoli formulated the replay attack and presented the countermeasures [7]. To the best of our knowledge, that was the first time a formal method to detect the replay attack was proposed. They considered an LTI system with Linear Quadratic Gaussian (LQG) controller and χ^2 detector to detect any abnormalities in the plant. First, [7] defines a replay attack. Then, it proposes to add an Independent and Identically

Distributed (IID) Gaussian watermarking signal with zero mean along with the control signal u so that, there will always be a different and unpredictable small watermarking signal available at the output which can be detected by any conventional detectors such as χ^2. They also investigate the control loss of performance, detection rate and false alarm rate due to watermark with different variances. In a subsequent work [8], a noisy watermarking method for milt-input multi-output systems (MIMO) while decreasing the control loss of performance and false alarm rate. Later, in [9], it is shown that the system is susceptible to replay attacks if certain condition is met. Using this information, [9] optimizes more parameters that can guarantee possibility of detection while minimizing control loss. At the end, the results are compared with those of [8] by using the same example of chemical plant model. Mo et al. in [10] uses a stationary and Gaussian watermarking signal with Neyman-Pearson detector. Moreover, they propose a more optimal method to select the properties related to watermarking signal to balance between detection rate and control performance.

To decrease the control loss of performance and achieve better detection possibility, many other authors modified of adding the IID gaussian watermark. Irita and Namerikawa in [11] use a bargaining game method to reach certain detection rate and control performance. Using a finite horizon, zero-sum, nonstationary stochastic game approach an optimal watermarking method was presented in [12]. During replay attacks, to minimize the performance cost and have certain detection rate, this method switches between cost-centric and secure-centric controllers. To determine the parameters for the game, knowledge of the system dynamics and controller is needed. Tran et. al. in [13] use a smart grid model to formulate the replay attack and propose to the use of watermarking signal sporadically (instead of continuously) to decrease the power loss in the grid. When there is no replay attack, applying the watermarking signal continuously will only result in an increase in control cost. Using the replay attack model like Stuxnet worm, the authors in [14] and [15] derive an optimized periodic watermarking strategy that can give better control performance and detection rate. Khazraei et. al. in [16] used IID Gaussian watermarking signal in a homogeneous multiagent dynamic system. They show that by letting interconnected agents share watermarking signals among themselves, the performance could be better for the same degraded controller performance compared with using single watermarking signal for each agent. When the Gaussian distributed watermark is used, using an information-theoretic metric,

Hosseini et. al. in [17] present a one-step version of the problem. They explain that the optimality of degrading the control performance is maximum, when the attacker of any level of stealthiness also uses Gaussian distributed in control input. They also show that using the Gaussian random variable for watermarking signal, the stealthiness of Gaussian attacker can be minimized. Using the cumulative sum analysis technique, [18] examines the optimal method to use IID gaussian watermarking with less detection delay.

Attackers can always improvise and so many explored different kinds of attack models. Weerakkody et. al. in [19] formulated a replay attack assuming attackers have the knowledge of the system and has access to a subset of measurement output and control inputs to attack while being undetected. They proposed a semidefinite program for designing the watermarking while using Neyman-Pearson detector. They presented and compared the results using the proposed detection technique on formulated attack model where attackers have different level of access to the inputs. Rubio-Hernan et. al. in [20] assumed the almost similar attack model. They showed that attackers with knowledge of the system can bypass the detector more easily. Hence, they proposed that in that case, switching between N different multi-watermark signals of different co-variance and mean would be better at detecting the replay attack. The method was able to detect cyber, non-parametric cyber-physical adversaries and parametric cyber-physical adversaries who have access to a limited set of control inputs.

By changing the properties of the watermarking signal on every step, attackers can be stopped from adapting to the situation. In [21], authors presented a dynamic watermarking method for single-input single-output, linear time invariant (SISO LTI) systems with partial state observations and MIMO LTI systems with a full rank input matrix and full state observations. Later, in [22], they extended dynamic watermarking for general ARMAX model (Autoregressive–moving-average model with exogenous inputs) with colored noise. Hespanhol et. al. in [23] further extended their work of dynamic watermarking for the general LTI systems using a more general attack model than replay attack. They proposed a method to compensate the persistent disturbances using the internal model principle. Authors, in [24], introduced dynamic watermarking for the system with several nonlinearities. They experimentally demonstrated their work on the nonlinear railway transportation model and successfully detected the replay attack. Khazraei et. al. in [25] derived design parameters so that defenders could have more degree of freedom to optimize the

dynamic watermarking for better control performance and detection rate. Many authors tested the reliability and robustness of dynamic watermarking into the smart grid system [26]–[28]. Their experiments were able to detect the replay attack using dynamic watermarking without disturbing the performance of power beyond specified limits. Meanwhile, [29] and [30] investigated the security weaknesses related to dynamic watermarking detection method using different generalized replay attack models. [30] explored the limitations of dynamic watermarking for event triggered state estimation based networked control systems, then presented a linear event triggered solution to the similar watermarking method for detecting generalized replay attack. In [31], authors used moving target approach to stop attackers getting used to the watermarking signals. They used the extraneous states which depend on the plant model and have linear time-varying dynamics. By comparing output signals from the actual plant and extended plant (proposed method) they could successfully detect not only replay attack but also FDI and zero dynamics attacks.

Many authors proposed different strategies to detect replay attacks. Using the frequency response of the plant, the authors in [32] utilized the white Gaussian noise available in communication channels for the authentication. They proposed a new state estimation technique to detect those noises. But this method is only applicable to networked control systems involving the additive white Gaussian noise channels. In [33], the authors used packet drops into the control system as an authentication. By dropping the packets according to IID Bernoulli sequence, they analyzed the control performance and detection rate trade-offs. Abdelwahab et. al. in [34] used model predictive control (MPC) and feedback compensation with packet drops to mitigate performance loss and achieve the bounded stability of the system. Using the concept of package drops, [35] developed a watermarking strategy for active sensors to detect replay attack and passive eavesdropping attacks.

A random stochastic watermarking input can lead to undesirable consequences. Model inversion watermarking could give defenders freedom to detect the replay attacks while staying in the desirable behavior [36]. [36] used feedforward input watermarking using pseudo-inversion. [37] used harmonic oscillations (limit cycles) as nonlinear watermarking but did not study the loss in the performance.

The performance can be optimized by manipulating the control cost. In [38], [39] zonotopic Kalman filter is used to develop a watermarking signal accordingly for better performance and detection possibilities. Another way to get better control performance is by stopping the watermarking signal from travelling further in the loop through controller. In [40], authors used virtual actuating scheme to eliminate the watermarking signal from the sensing signal, so that the signal will not be in the control loop. [41] uses random sine signal as an authentication signal and cascade observers to detect the watermarking signals in the feedback. In normal conditions, the observer will eliminate the watermarking signal on the other side, preventing it from moving further in the loop and giving better performance.

All the work mentioned so far requires a knowledge of the plant. In the case of the system with unknown parameters, it would be hard to optimize the watermarking signal parameters to trade-off between control performance and detection rate. In that case, an online learning approach was used to determine the optimal watermarking signals [42]–[44]. Although, in this case, defenders will have to rely on the almost sure convergence rate of an algorithm and not the perfectly known performance.

In smart grid, there are numbers of plants and loads. Gaining a precise knowledge of all components and controllers can be very difficult, and even if we manage to do so, there will always be some amount of power loss due to fluctuations in watermarking signal. Additionally, adding random watermark signal in the smart grid plants means making the generator and power electronics work randomly which can put more burden on power electronics and measurement system. Ghamarilangroudi in [45] proposed a watermarking using switching sine waves which utilize very minimum model knowledge i.e., the knowledge of frequency responses of the plant for the frequencies that was used for the watermark. The frequency response information could be obtained experimentally, and mathematical model of the plant is not required. [45] shows that a multi-sine wave can be constructed in such a way that the transient due to switching can be suppressed. Also, sine waves change gradually (not abruptly), which means less burden on the actuating systems.

Table 1.2 A brief Summary on different methods for detecting replay attacks

	Location of Watermark	**Type of Method**	**References**
1	With control signal u	IID Gaussian Noise	[7], [8], [9]
2		Stationary Gaussian Noise + Neyman-Pearson detector	[10]
3		Gaussian Noise + Game Approach	[11], [12]
4		Periodic Gaussian Noise	[13], [14], [15]
5		Switching between Multiple Watermarking Signals	[20]
6		Dynamic Watermarking	[21]–[30]
7		Moving Target	[31]
8		Packet Drops	[33], [35]
9		Packet Drops + MPC	[34]
10		Model Inversion	[36]
11		Harmonic Oscillations as Watermark	[37]
12		Using Zonotopic Kalman Filter	[38], [39]
13		Eliminating Watermark from the loop	[40], [41]
14		Optimization using Online learning	[42]–[44]
15		Multi-Sine Watermark	[45]
16	-	Utilizing channel noise as watermark	[32]
17	At the sensor signal	By using Coder and Decoder	[46]–[48]
18		Only Coder	[49]
19		Moving Target	[50]
20		Switching between Multiple Watermarking Signals	[51]–[53]

To eliminate the loss in control performance completely due to watermarking signal, some authors used coded sensors to put authentication signals into the sensor measurement and then decoder or the remover on the other side before feeding to the controller [46]–[48]. In [49], authors used a coding matrix for the measurements which does not need any decoder and can be directly utilized into the estimator to estimate the system states. Ghaderi et. al. in [50], used the similar approach with the moving target strategy to make harder for the attackers to implement the attack. [51], [52] used multiplicative watermarking schemes to each sensor's output which keeps switching between different signals, making harder for attackers to decipher the security protocols. Later, [53] developed similar strategy for the generalized replay attack model and explained the construction of parameters of the multiplicative watermarking to achieve certain detectability. These methods also help catch the stealthy FDI attacks. Another advantage is that it does not put additional burden on sensors. But since attackers could hack the sensors to perform the attack, then, additional security would be required to stop attackers defeating those approaches.

1.2 Thesis Objectives and Contributions

The thesis aims to develop a design procedure for replay attack detection. In particular, the procedure is to be derived from the switching multi-sine watermarking scheme in [45]. The reasons for choosing this scheme are that,

i. it relies on frequency response data which are not difficult to obtain for circuits,
ii. the impact of the watermarking scheme on the plant output can be analytically calculated and kept bounded, and
iii. the detection of watermarking signal in the received sensor data does not require an observer/estimator. The above properties make the approach easier to implement in the existing grids.

The contribution of the thesis can be summarized as follows:

- The thesis presents a design procedure for choosing watermarking signal for smart grid that contains inverter-based power plants. Specifically, it extends the guidelines of [45] and
    i. discusses suitable locations for adding watermarking,
    ii. presents guidelines for choosing frequencies and amplitudes of sine waves for watermarking in smart grids.
- The procedure of [45] for single-input-single-output systems has been extended to two-input-two-output systems for specifically smart grids in such a way to minimize the impact of watermarking on the grid.

Simulation of inverter-based power plant is used to illustrate the results.

1.3 Thesis Outline

Chapter 2 contains a brief review of background material on replay attack, the switching multi-sine watermarking method and voltage sensitivity to active and reactive power change. In Chapter 3, after introducing the problem, a solution is presented for designing watermarking signal for a single plant connected to grid. Chapter 4 explores the effects of adding the watermarking on the grid and then proposes a method to almost eliminate the undesirable effects of watermarking on the grid. Using two different plants connected to a grid, simulation results are used to illustrate the proposed solution. Finally, Chapter 5 concludes the work and discusses directions for possible future work.

Chapter 2

Background

In this chapter, we briefly review replay attacks in control systems and multi-sine watermarking method for detecting replay attacks. At the end, we discuss voltage sensitivity at different places in electric power grids with respect to active and reactive power changes. These results will later be used in the thesis.

2.1 Replay Attack

The replay attack is generally carried out when the system is in a steady state. The attacker records the sequence of measurement data from the sensors and later replays the same data on the communication channels of the respective sensors while manipulating control signals in a way that it would cause harm to the system or group of systems. By replaying the same data, the attacker can easily manage to remain undetected by diagnosis/observation system.

In this attack, the adversary does not need the information about either the plant model or controller but knows when and for how long the system will remain in steady state.

Consider the feedback system in Fig. 2.1 [7,10]. The plant is the linear time-invariant system.

$$x_{k+1} = Ax_k + Bu_k + w_k \tag{2.1}$$

$$y_k = Cx_k + v_k \tag{2.2}$$

where $x_k \in \mathcal{R}^n$ and $w_k \in \mathcal{R}^n$ are the vectors of state variables and process noise at time k. The sensor reads the measurement data $y_k \in \mathcal{R}^n$ with noise v_k. Let us suppose the controller is an observer-based controller. The observer/estimator receives the output signal y_k.

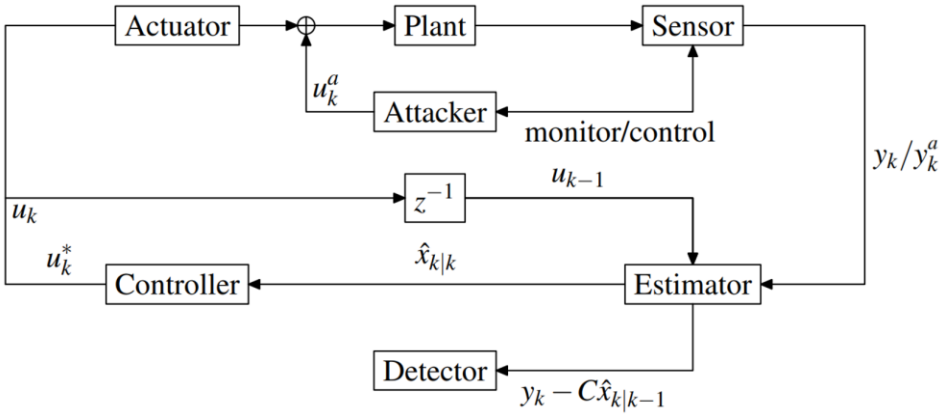

Figure 2.1 Replay attack model used in [7]

Next the estimator calculates the state estimate $\hat{x}_{k|k}$ from measured data y_k and previous input u_{k-1}. Using estimated state variables $\hat{x}_{k|k}$, controller sends control input u_k to the plant/actuator.

Here, it is assumed that the attacker has access to all the sensor signals and can manipulate the control signal. Before initiating attack, during Phase 1, the attacker makes sure to record the measurements for enough time, say N samples, so that later during the attack phase, the stored measurements can be played for a significantly long time.

Suppose the attack starts at $k = 0$. During attack (Phase 2), the attacker replaces sensor data with recorded data y_k^a from time 0 to $N - 1$, where $y_k^a = y_{k-N}, 0 \leq k \leq N - 1$. So, even if the system is equipped with failure detectors like χ^2, it will not be able to detect the attack as the new modified measurements and states seem healthy. In the meantime, the attacker can modify the control input supplied by the controller to u^a to perform the attack.

Figure 2.2 shows the attack phase. Instead of the actual sensor data y, the attacker replays previously recorded sensor data y_a. At the same time, the attacker replaces the control signal u^* with another signal u_a.

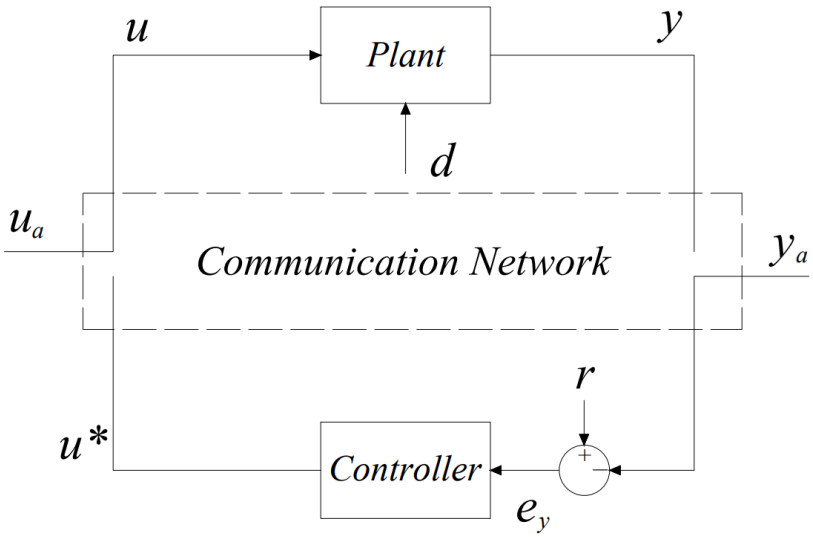

Figure 2.2 Typical plant model under replay attack [37]

2.2 Detection using Multi-Sine Watermarking

In [45], a method is introduced for detecting replay attacks which involves sinusoidal signals for watermarking. To prevent the attacker from adapting to watermarking, the frequency of sinusoidal signals is changed. To prevent transients in the plant output as a result of the watermarking switching, a multi-sine wave is used. To derive the watermarking signal, only the order of the transfer function from control signal to output and frequency response at the frequencies used for watermarking is needed.

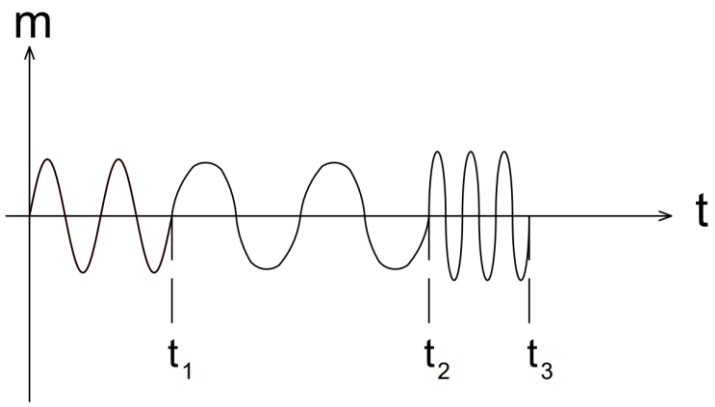

Figure 2.3 Different frames of watermarking

Figure 2.3 shows the watermarking signal:

between 0 and t_1: frequency ω_1,

between t_1 and t_2: frequency ω_2,

between t_2 and t_3: frequency ω_3 and so on.

For each interval $[t_i, t_{i+1}]$ where frequency does not change is called a frame.

Figure 2.4 shows the linear model of the system operating at the steady state.

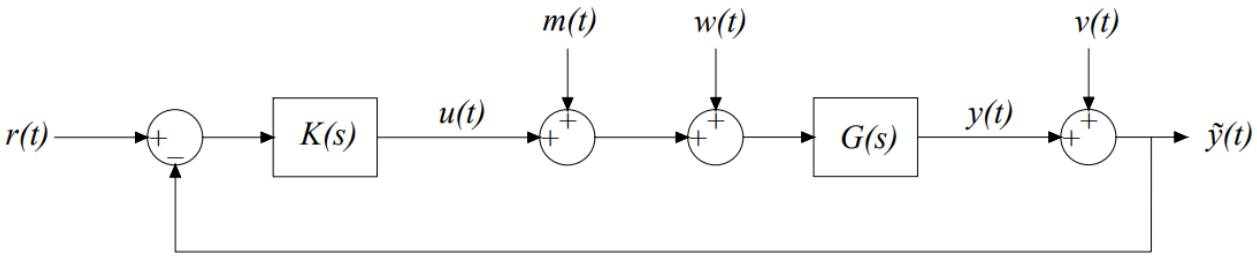

Figure 2.4 Linear system model used in [45]

where,

$K(s)$ is the transfer function of the controller,

$G(s)$ represents transfer function of the plant,

$r(t)$ is the reference signal,

$u(t)$ as the control signal,

$w(t)$ is the plant input disturbance,

$y(t)$ is the actual plant output and

$\tilde{y}(t)$ is the output signal measured by the sensor which has $v(t)$ sensor noise.

The proposed watermarking signal $m(t)$ in [45] can be represented as,

$$m(t) = \sum_{i=1}^{n_m} A_i \sin(\omega_i t + \phi_i) \tag{2.3}$$

where,

$n_m = number\ of\ sinusoidal\ signals$

$A_i = amplitude\ of\ i^{th}\ sine\ signal$

$\phi_i = phase\ of\ i^{th}\ sine\ signal$

$\omega_i = frequency\ of\ i^{th}\ sine\ signal$

Given the order of the transfer function $G(s) = Y(s)/M(s)$, the parameters (mentioned above) are chosen in such a way that there will be no transient response due to the watermarking signal. The summary for selecting these parameters for the plant with different orders is given below. First the results for the first, second and third order systems are provided and next the process for a general n^{th} order system is reviewed.

1. First order systems:

For the first order system, to prevent transients the parameters of the multi-sine watermark can be chosen as:

$$n_m = 1 \tag{2.4}$$

$$\phi_1 = -\angle G_{my}(j\omega_1) + 2l\pi \tag{2.5}$$

where, $l = 0, 1, 2, \ldots$ and $\angle G_{my}(j\omega_1)$ is the phase of the first order system $G_{my}(j\omega)$ at frequency ω_1.

A_1 and ω_1 can be chosen arbitrarily. Other considerations for choosing A_1 and ω_1 will be reviewed later.

2. Second order systems:

For the second order system, 2 sinusoidal signals are needed. Hence, $n_m = 2$.

A_1 and A_2 must be chosen such that,

$$A_1|G(j\omega_1)| = A_2|G(j\omega_2)| \tag{2.6}$$

Furthermore,

$$\alpha_1 = \frac{\pi}{2}, \alpha_2 = -\frac{\pi}{2} \quad or \quad \alpha_1 = -\frac{\pi}{2}, \alpha_2 = \frac{\pi}{2} \tag{2.7}$$

where,

$\alpha_1 = \phi_1 + \angle G(j\omega_1)$ and

$\alpha_2 = \phi_2 + \angle G(j\omega_2)$.

ω_1 and ω_2 ($\omega_1 \neq \omega_2$) can be chosen arbitrarily (as far as avoiding transient is concerned).

3. Third order systems:

For the 3rd order system, we need 2 sinusoidal signals to suppress transients. The parameters of $m(t)$ must satisfy the following:

$$\frac{A_1|G(j\omega_1)|}{A_2|G(j\omega_2)|} = \frac{\omega_2}{\omega_1} \tag{2.8}$$

$$\alpha_1 = 0, \alpha_2 = \pi \quad or \quad \alpha_1 = \pi, \alpha_2 = 0 \tag{2.9}$$

ω_1 and ω_2 ($\omega_1 \neq \omega_2$) can be chosen arbitrarily (as far as avoiding the transient is concerned).

4. Procedure for n^{th} order transfer function

Consider an n^{th} order plant $G(s)$ shown by the following differential equation:

$$\frac{d^n y}{dt^n} + a_{n-1}\frac{d^{n-1}y}{dt^{n-1}} + \cdots + a_0 y(t) = b_{n-1}\frac{d^{n-1}u}{dt^{n-1}} + \cdots + b_0 u(t) \tag{2.10}$$

Hence,

$$G(s) = \frac{b(s)}{a(s)} = \frac{b_{n-1}s^{n-1} + \cdots + b_1 s + b_0}{s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0} \tag{2.11}$$

The watermarking signal $m(t)$ from (2.3) can be shown as:

$$M(s) = \frac{p_m(s)}{(s^2 + \omega_1^2) \ldots \left(s^2 + \omega_{n_m}^2\right)} \tag{2.12}$$

where,

$$p_m(s) = c(s)a(s) \tag{2.13}$$

It follows from (2.13) that,

$$n = \deg\left(a(s)\right) \leq \deg\big(p_m(s)\big) \leq 2n_m - 1 \tag{2.14}$$

Therefore, we must have

$$n_m \geq \frac{n+1}{2} \tag{2.15}$$

For a given n_m, $c(s)$ must be chosen such that such that (2.14) is satisfied. Frequencies $\omega_1, \omega_2, \dots, \omega_{n_m}$ can be chosen arbitrarily as far as transient suppression is concerned.

Next, let us discuss some general considerations on the choice of frequencies.

For all the cases mentioned above,

$$f_i = \frac{\omega_i}{2\pi} = \frac{1}{T_i} \tag{2.16}$$

where, f_i is frequency in Hz and T_i is period of the i^{th} component.

[45] suggests that the frequencies of the sinusoidal signals must be chosen such that for some integers $p_1, p_2, \dots, p_{n_m}$

$$\frac{f_1}{p_1} = \frac{f_2}{p_2} = \cdots = \frac{f_{n_m}}{p_{n_m}} \tag{2.17}$$

Here, integers are relatively prime, i.e., $\gcd\big(p_1, p_2, \dots, p_{n_m}\big) = 1$ but $p_{i+1} - p_i \neq 1$.

This will ensure that $m(t)$ is a periodic signal with the period of

$$T_{combined} = p_1 T_1 = p_2 T_2 = \cdots = p_{n_m} T_{n_m} \tag{2.18}$$

and the frame size of the watermarking signal will be,

$$T_{frame} = kT_{combined} \tag{2.19}$$

where,

$k\ is\ some\ positive\ integer.$

The total amplitude of the watermarking signal is usually determined based on the ability of the detector to detect the specific frequency despite the available noise in the signal (explained in the next section). So, for the watermarking signal (2.3),

$$Total\ amplitude\ of\ the\ watermarking\ signal\ A_{wm} = \sum_{i=1}^{n_m} A_i |G_{my}(j\omega_i)| \tag{2.20}$$

2.3 Power Spectral Density using Periodogram

A Periodogram is an estimation function that gives a Power Spectral Density (PSD) of a signal. In time-series data, periodogram calculates the significance of different frequencies in terms of power. In signal processing, PSD around the frequency f is given as,

$$P_{xx}(f) = \frac{\Delta t}{N} \left| \sum_{n=0}^{N-1} x(n) e^{-j2\pi f n} \right|^2 = \frac{1}{N} |X(f)|^2 \tag{2.21}$$

For sampling time $\Delta t = \frac{1}{f_s}$, f is defined as,

$$-\frac{1}{2\Delta t} < f < \frac{1}{2\Delta t} \tag{2.22}$$

There are many methods to calculate the PSD of a particular signal. Welch's method uses a method of average periodograms, in which a long sequence of the time-series data is divided into shorter and possibly overlapping parts [54]. For each part, the periodogram is calculated and later, using the average of corresponding element of all the windowed periodograms the final PSD result is obtained.

Using the periodogram with confidence bounds, we can determine the detectability of a periodogram for detecting specific signal despite the available noise. At any specific frequency and amplitude (of the signal of that frequency), if the power density of the lowest bound is higher than upper bound of any other frequencies that means, that frequency is available in that signal and periodogram can successfully detect it.

To understand this, consider a signal consisting of 120Hz and 200Hz sine waves in additive white $N(0,1)$ noise. The signal can be expressed using (2.23).

$$\cos(2\pi 120t) + \sin(2\pi 200t) + v(t) \tag{2.23}$$

where,

$v(t) = white\ noise\ N(0,1)$

In the above signal, the amplitude of both sine waves is one.

Figure 2.5 shows a periodogram with 95% confidence bounds for a signal mentioned in (2.23).

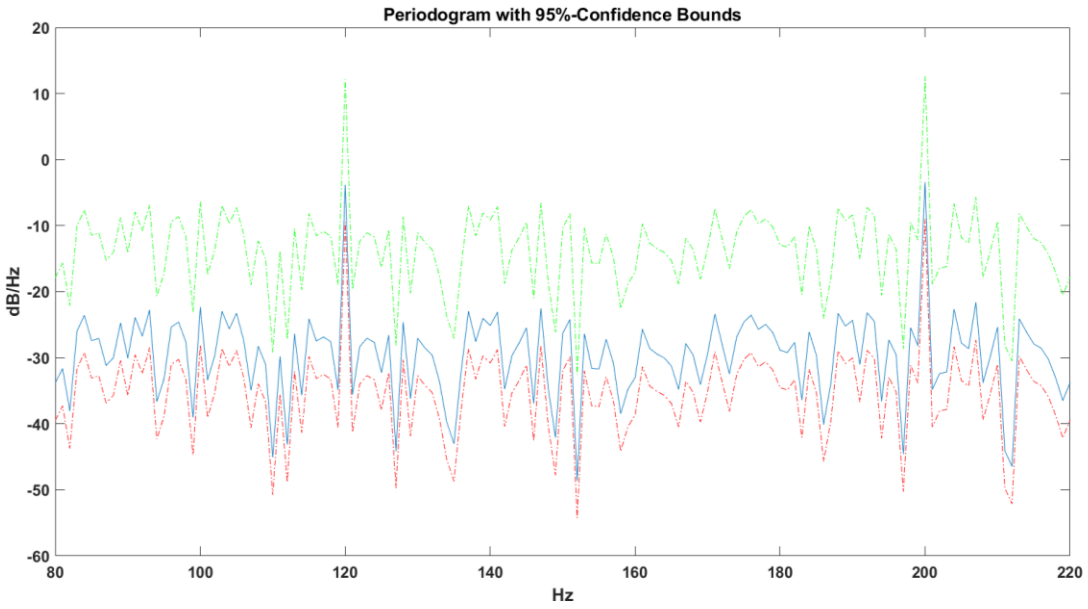

Figure 2.5 Detection of signal (2.23) using Periodogram with 95% confidence bounds

In figure 2.5, at frequencies 120Hz and 200Hz, the power density of the lowest bound (red) is much higher than upper bound (green) at any other frequencies. That means, the periodogram can successfully detect the frequencies which have amplitude of 1. In other words, the frequencies of amplitude of 1 is detectable by the periodogram.

Now consider the same signal with 2 sine waves and additive noise. But this time, the amplitude of sine wave with frequency 200Hz is 0.3. The signal can now be shown using (2.24).

$$\cos(2\pi 120t) + 0.3\sin(2\pi 200t) + v(t) \tag{2.24}$$

Figure 2.6 shows the periodogram with 95% confidence bound for a signal (2.24). At 200Hz, the power density of lowest bound (red) is much lower than the power density of upper bound at any other frequencies. That means that, periodogram cannot successfully detect frequency of the amplitude 0.3 even though it is available in the signal. The amplitude 0.3 is not detectable by the periodogram.

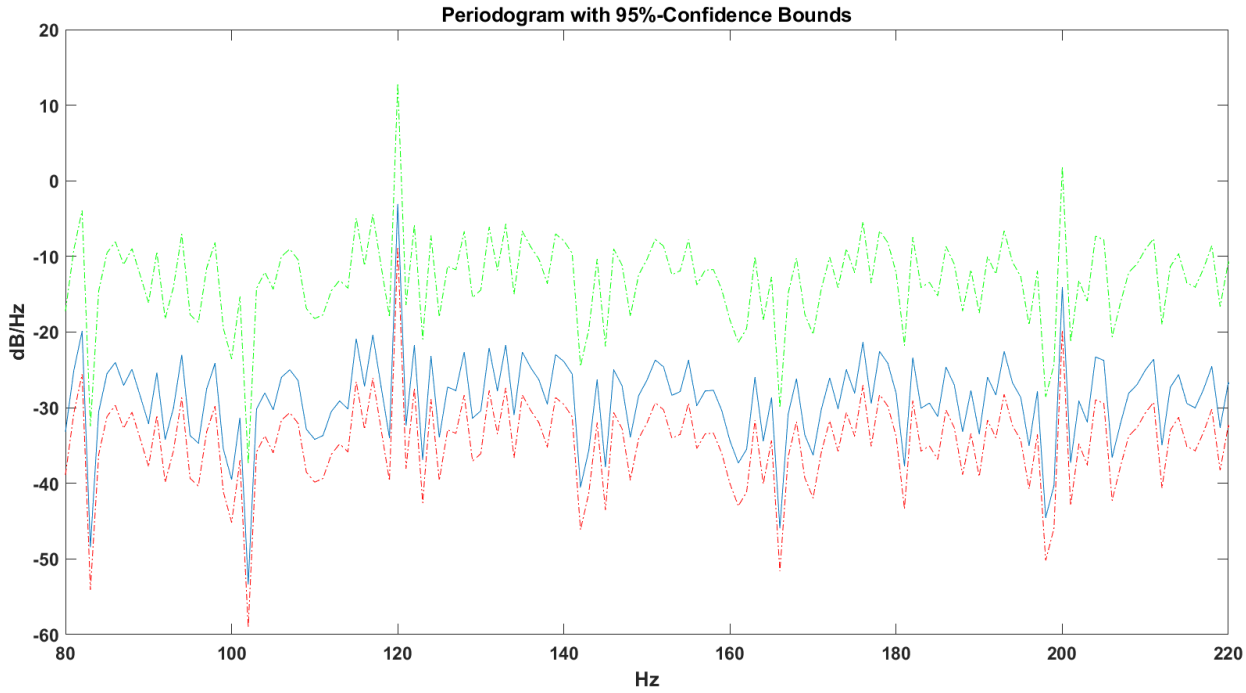

Figure 2.6 Detection of signal (2.24) using Periodogram with 95% confidence bounds

2.4 Voltage Sensitivity

In this thesis we study replay attacks in smart grids. A topic of interest for us will be the impact of changes of power on voltage.

In power systems, any power generating/consuming center can be represented by a bus. From a total of n buses available in a power system, Figure 2.7 shows two buses i and j.

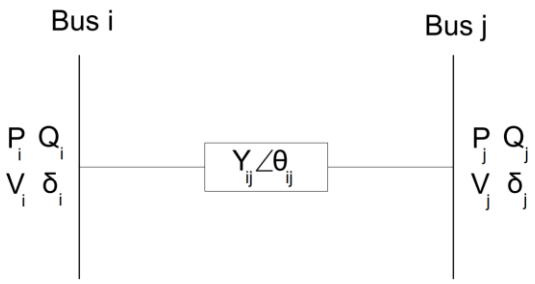

Figure 2.7 Buses i and j with admittance in between them

For bus i,

$$P_i = \sum_{j=1}^{n} |V_i||V_j||Y_{ij}| \cos(\theta_{ij} - \delta_i + \delta_j) \tag{2.25}$$

$$Q_i = -\sum_{j=1}^{n} |V_i||V_j||Y_{ij}| \sin(\theta_{ij} - \delta_i + \delta_j) \tag{2.26}$$

where, P_i and Q_i are total available active and reactive power respectively at bus i. (V_i, δ_i) and (V_j, δ_j) are the voltage magnitudes and phase angles at buses i and j respectively. The admittance of the line from bus i to bus j is shown as $Y_{ij}\angle\theta_{ij}$ (inverse of line impedance Z_{ij}).

By solving nonlinear equations (2.25) and (2.26), say using the Newton-Raphson method, the following expression can be derived which relates small changes in active and reactive powers to small changes in voltage magnitudes and phases:

$$\begin{bmatrix} \Delta\delta_1 \\ \vdots \\ \Delta\delta_k \\ \vdots \\ \Delta\delta_n \\ \hline \Delta V_1 \\ \vdots \\ \Delta V_k \\ \vdots \\ \Delta V_n \end{bmatrix} = \boldsymbol{S} \begin{bmatrix} \Delta P_1 \\ \vdots \\ \Delta P_k \\ \vdots \\ \Delta P_n \\ \hline \Delta Q_1 \\ \vdots \\ \Delta Q_k \\ \vdots \\ \Delta Q_n \end{bmatrix} \tag{2.27}$$

$\boldsymbol{S}$ is the voltage sensitivity matrix and is the inverse of the Jacobian matrix. Eq. (2.27) allows a quantitative analysis of the change in voltage due to change in power. $\boldsymbol{S}$ can be partitioned as,

$$\boldsymbol{S} = \begin{bmatrix} S^{\delta P} & S^{\delta Q} \\ S^{VP} & S^{VQ} \end{bmatrix} \tag{2.28}$$

where, $S^{\delta P}$ and $S^{\delta Q}$ are the sensitivities of the voltage phase angles with respect to the active and reactive powers, respectively. Similarly, sensitivities of the voltage magnitudes to the change in active and reactive power is shown as S^{VP} and S^{VQ}, respectively.

Chapter 3

Replay Attack Detection in Smart Grids

The objective of this thesis is to develop a watermarking scheme for detecting replay attacks in smart grids. In this chapter, we start by introducing the problem. Later, we propose a solution using a simulated grid connected plant.

3.1 Problem Statement

Smart grids consist of a Central Controller (CC), generating units, loads, different electric devices, and communication channels. The CC manages power flow from the power plants to the consumers. It gathers the measurement data such as current, voltage, phase angle, frequency, active power, and reactive power from the smart meters and substations situated at various locations in the grid. The goal of the central controller is to keep the electrical quantities within limits specified by IEC, IEEE, or any other local/national standards. According to these standards and using collected measurement data, CC sends reference signals (set points, for example reference active power P_{ref} and reactive power Q_{ref}) to different plants for producing electricity. Fig. 3.1 shows the typical structure of the smart grid.

In the smart grids, the central controller plays a part of a supervisor which coordinates between all the plants through communication links. These plants then have their own individual controllers. This makes the smart grid one of the biggest widespread cyber physical MIMO

systems which has multiple controllers, plants, complex communication network and multiple non-linear quantities.

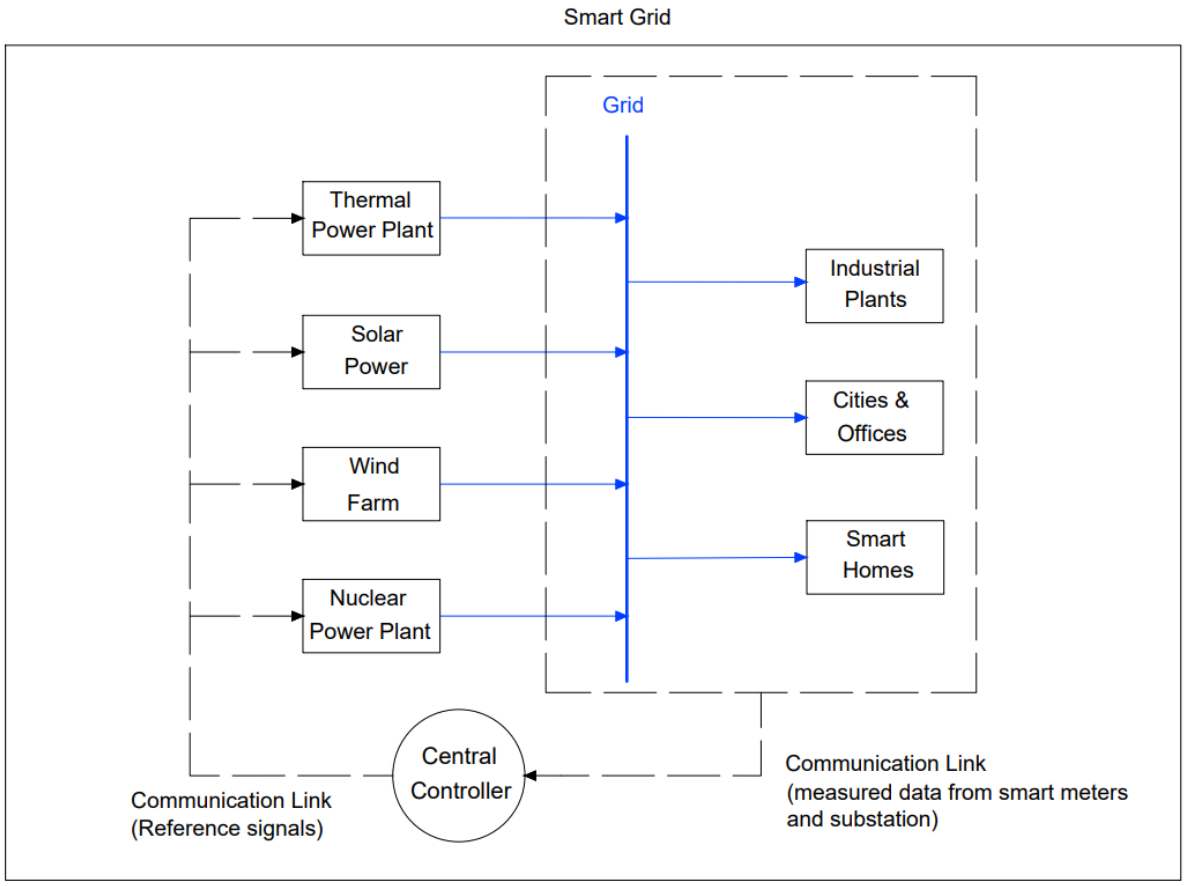

Figure 3.1 Typical structure of the smart grid system (blue lines represent electric power flow)

The basic and general task of the central controller is to balance the active and reactive power within the grid. In normal conditions, the power demand changes according to the needs of the consumers. But a major change in power demand occurs every few hours. Hence, the operation of smart grid stays in the steady state most of the time (considering the ideal operation without any fault and/or unbalance). Due to the higher number of communication lines and longer steady state period, it makes the smart grid more vulnerable to security attacks, especially to the replay attacks. Also, it gives attackers more than just one place where they can execute replay attacks as shown in Figure 3.2.

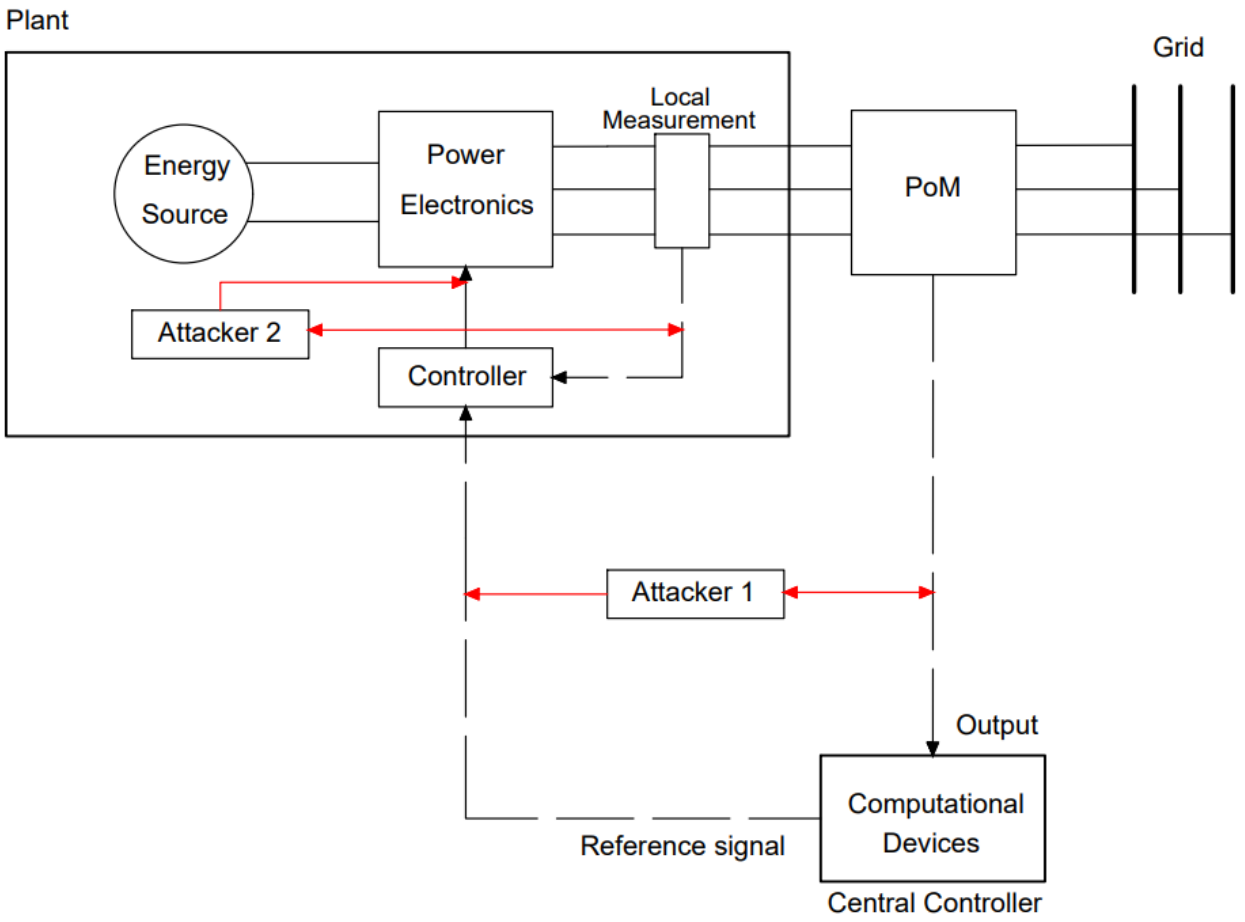

Figure 3.2 Replay attacks in the smart grid

As shown in Figure 3.2, Attacker 1 can implement the replay attack in between a plant & the CC. Attacker 1 can read and record the output from the Point of Measurement (PoM) and later the same recorded output can be replayed on the communication line and feed it to the CC while altering the reference signal. Similarly, Attacker 2 can place the replay attack within the plant by recording the data from the local measurement. In this case, attacker 2 can change the control signal from the controller (local) while replaying the recorded data.

Here are some of the assumptions that are considered though out the work:

1. The power plants are inverter-based resources (IBRs) as they are easy to control through a local controller. And it also gives freedom to use different control strategies.
2. As the general task of the CC is to balance active and reactive power within the grid, the CC sends the reference set points of active and reactive power to the local controllers and the local controllers make sure to deliver the electricity according to those reference set points. Hence, the local controllers are considered to be working in a PQ control mode.
3. The communication between the plants and CC is in real time. The CC sends reference signals and receives measured signals continuously without any delay in the communication channels.
4. As the replay attack usually happens when the plant is operating in steady state, the watermarking signal is also added when the plant has reached a steady state.
5. There is no fault and/or unbalance happening in the plant and grid. The electrical faults can be detected by the separate protection system.

Remark 1: The delay in the communication links can be eliminated using the time stamps.

Remark 2: The period in which the power plant operates in a steady state varies according to the types of plants. This could be in minutes or hours. The base load power plants remain in a steady state for a longer period (for hours), on the other hand some plants operate in a quasi-steady state. In this work, plants are considered to be operating in a steady state all the time.

The objective of this thesis is to develop a design procedure for watermarking in smart grids so that it can be used to detect replay attacks. In this chapter, we discuss a case of one power plant and in the following chapter, a more general case of multiple power plants is considered. In the next section, first we review the communication structure between a grid connected plant and CC. Then by using a case of a simulated single power plant, we propose a solution.

3.2 Proposed Solution

Using replay attack and by changing the active and reactive power reference signals (P_{ref} and Q_{ref}), attackers can easily cause blackouts through cascade failures while being undetected. To detect the replay attack occurring in between the plant & the CC, the watermarking can be placed in the reference signals (P_{ref} and Q_{ref}) transmitted by the central controller as shown in Fig. 3.3.

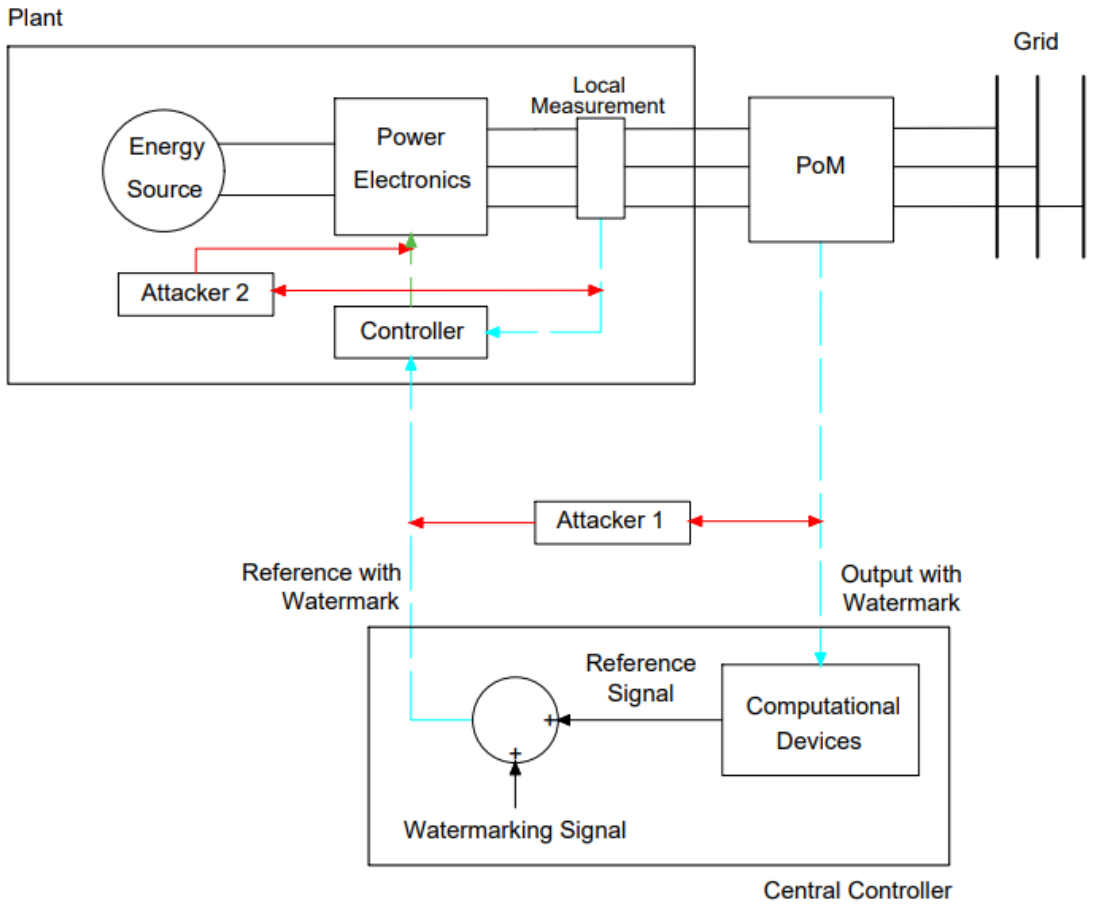

Figure 3.3 Replay attack detection in the smart grid

The PoM measures the delivered active and reactive power (P and Q) and sends it to CC. Detection happens in the CC. Since the watermark is added to the reference signal of the plant, the effect of the watermark can be seen in the output as well as control signals (Fig 3.3, shown in blue) of the plant (shown in green).

Remark 3: Plant and PoM are physically separated but are near to each other. Plant and CC usually have a significant distance in between them.

Next, we will review the attack model using a single power plant and provide a solution. In the following chapter, we consider the case of multiple power plants.

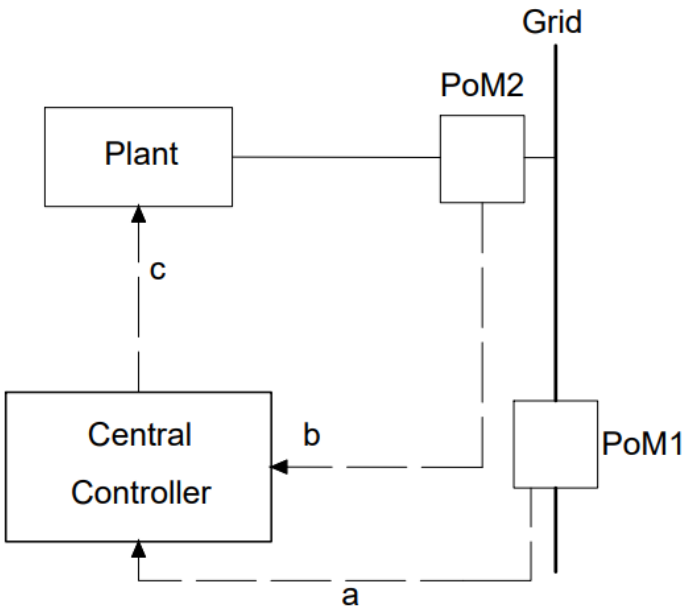

Figure 3.4 Communication structure between plant and central controller (dashed lines: communication links; solid lines: electric transmission lines)

Remark 4: The CC usually has the information of power demand from the consumers throughout the day. The CC can also calculate the changing power demands from the received present measured data from various parts of the grid.

To meet the demand, the CC calculates P and Q that are required at present and asks specific plants to generate certain P and Q. Here in Figure 3.4, CC communicates with the plant using the communication line 'c'. The CC then checks whether sent references (P_{ref} and Q_{ref}) were generated by the plant or not from PoM2 via line 'b'.

Let us assume, a replay attack occurs on lines 'b' and 'c'. The attacker will read & save enough data of line 'b' in the first phase (Fig. 3.5) & then in the next phase (Fig. 3.6), attacker will repeat the same data on line 'b' while altering reference signals on line c.

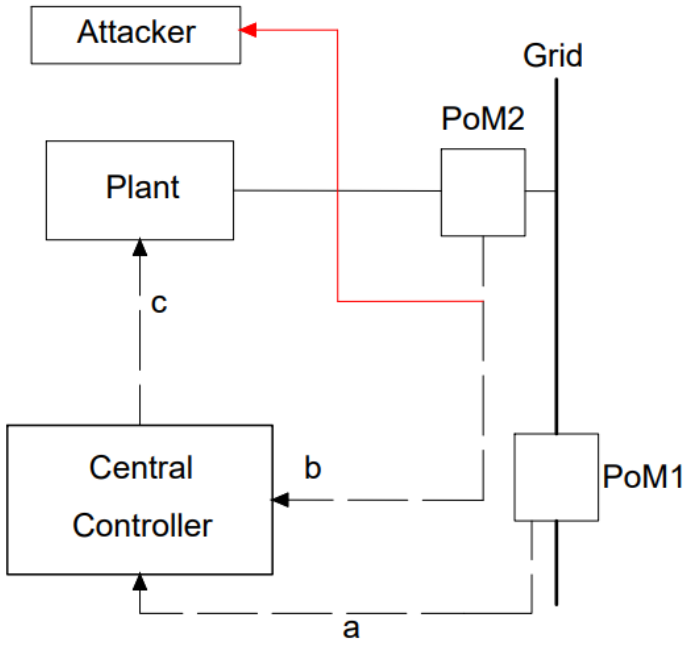

Figure 3.5 Replay attack in the smart grid; Phase 1: Attacker reads and records the data

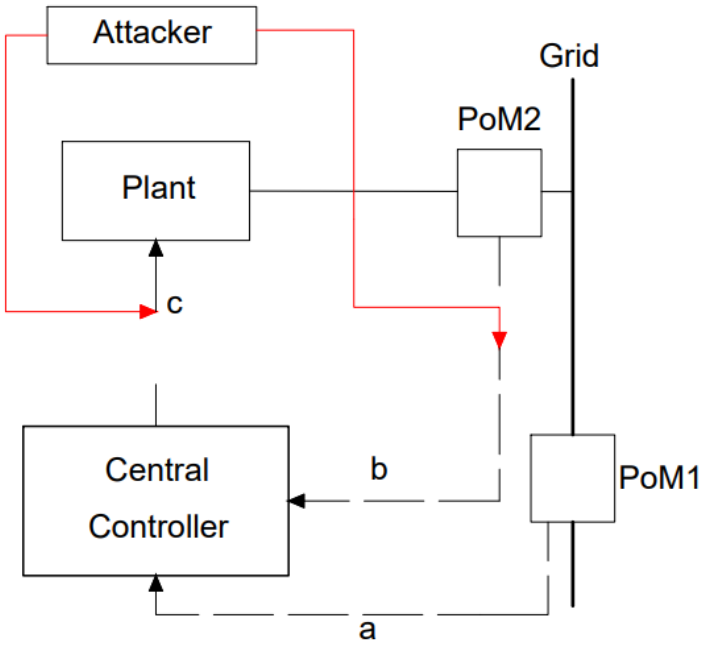

Figure 3.6 Replay attack in smart grid; Phase 2: Attacker replays the recorded data while changing the reference signal

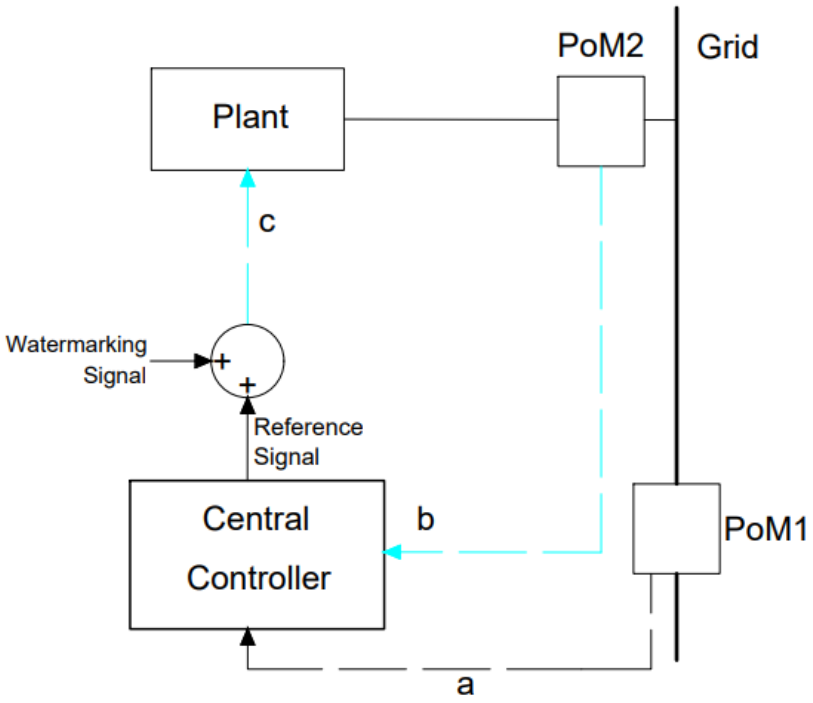

Figure 3.7 Watermark added in the reference signal

To detect the replay attack, a proper watermarking signal can be added to the reference signal as shown in Fig. 3.7. In normal conditions (absence of replay attack), the effect of watermarking can be seen at PoM2. If it is not available at PoM2, that means there is a replay attack happening within the plant or in between plant & CC.

In this thesis, multi-sine wave signal is used as a watermark. One of the advantages of using it as a watermarking signal is that it is smooth and there is no sudden change in magnitude because of the sinewaves. Hence, it does not put any instant burden on the power electronics, transmission lines, measurement components, etc.

Using the attack model explained above, we now develop a method for deriving a multi-sine wave watermarking signal for a single power plant. To help us develop the design procedure, we will use a running example. We start by modelling the power plant. Next, after adding the watermarking signal in a simulated grid connected plant, we will develop the design guidelines. Furthermore, we will also investigate the effects of watermarking on current harmonics and control signals.

3.2.1 Modelling of the Power Plant

Nowadays, almost all plants are connected to the grid through inverters. These plants are called Inverter Based Resources (IBRs). Except for the fuel cells and Photovoltaic (PV) arrays, generators are connected to back-to-back converters as shown in Fig. 3.8. This back-to-back converter consists of a machine side converter (MSC), grid side inverter (GSI), and DC link. PV arrays and fuel cells are directly connected to the grid through DC link and GSI. Hence, in terms of dynamics and physical structure, all the IBRs are similar from DC link to the grid.

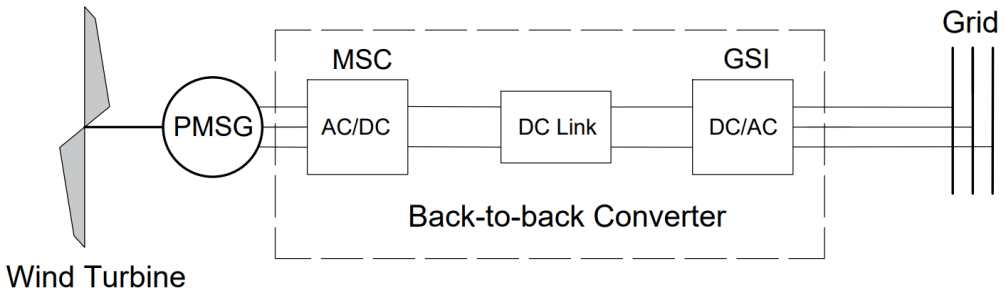

Figure 3.8 Permanent Magnet Synchronous Generator (PMSG) connected to the grid through back-to-back converter

In our work, we are not going to control any parameters of the MSC and DC link. Also, both the DC link capacitor and the battery banks can be considered as DC power sources. Hence, to simplify the modelling, an ideal DC voltage power source can be connected to the GSI as shown in Fig. 3.9. Moreover, the lumped impedance is used which can be represented as the total impedance of filter, transmission lines, cables, transformer (if there is any) etc. These assumptions will not affect the overall operation and dynamics of the plant. The diagram of the power plant with the above assumptions can be shown using Fig. 3.9.

Remark 5: An ideal voltage power source provides the constant voltage at every instant of time.

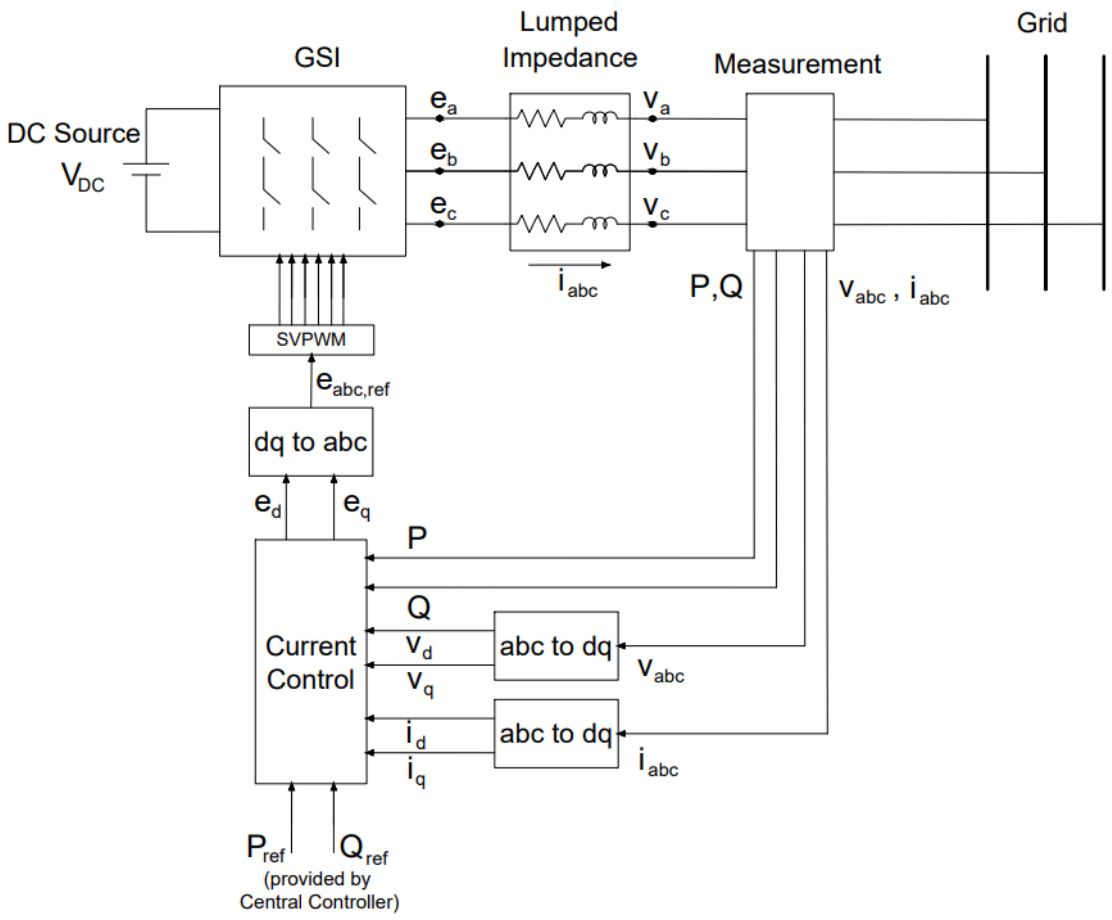

Figure 3.9 Modelling of a Power Plant

Remark 6: In electrical system, instantaneous quantities are usually shown using small fonts (for example instantaneous voltage v) except for the active and reactive power. They are denoted using the capital alphabets P and Q respectively.

Remark 7: Any three phase quantities r_a, r_b and r_c (where $r = i, v$ or e) can be shown using the term r_{abc}.

Central controller sends the reference instantaneous active and reactive power values (P_{ref} *and* Q_{ref}) to the power plant. Usually, to control active and reactive power, the current control method is used [55]. Using P_{ref}, Q_{ref}, measured instantaneous active power P, measured instantaneous reactive power Q, instantaneous voltage v_{abc} and instantaneous current i_{abc}, controller calculates and sends control signal $e_{abc,ref}$ to the pulse generator.

On one side, GSI is connected to the DC source of voltage V_{DC}. Pulse generator will trigger all the six switches of the power electronics in a specific manner that the three-phase voltage e_{abc} is generated on the other side of the GSI as shown in Figure 3.9. As SVPWM (Space Vector Pulse Width Modulation) gives 15.5% more utilization of DC link voltage and lesser switching losses than the other conventional PWM methods, in our case, SVPWM is used as a pulse generator to give pulses to the power electronic switches of GSI.

Applying Kirchhoff's Voltage Law (KVL) on Fig. 3.9:

$$e_{abc} = Ri_{abc} + L\frac{di_{abc}}{dt} + v_{abc} \tag{3.1}$$

where,

$e_{abc} = instantaneaous\ three\ phase\ voltages\ at\ the\ inverter\ terminal$

$v_{abc} = instantaneaous\ three\ phase\ grid\ voltages$

$i_{abc} = instantaneaous\ three\ phase\ current\ from\ GSI\ to\ grid$

$R\ and\ L\ are\ the\ lumped\ resistance\ and\ inductance\ respectively$

Equation (3.1) shows that power converter needs to generate voltage e_{abc} to overcome losses due to impedance (in our case lumped impedance) and give voltage v_{abc} at the grid while controlling the current i_{abc} according to the active and reactive power requirements.

Generally, for better controlling, three phase quantities (abc) are converted into the dq0 quantities [56], [57].

Three phase quantities can be transformed into dq0 quantities using Clarke-Park transformation [55]:

$$\begin{bmatrix} r_d \\ r_q \end{bmatrix} = \frac{2}{3}\begin{bmatrix} \cos(\omega t) & \cos(\omega t - 2\pi/3) & \cos(\omega t + 2\pi/3) \\ -\sin(\omega t) & -\sin(\omega t - 2\pi/3) & -\sin(\omega t + 2\pi/3) \end{bmatrix}\begin{bmatrix} r_a \\ r_b \\ r_c \end{bmatrix} \tag{3.2}$$

where,

$r = some\ vector\ (v, e\ or\ i)$

$\omega = 2\pi f; f = grid's\ voltage\ frequency$

Remark 8: To obtain ω, Phase Locked Loop (PLL) is generally used [58].

The inverse Clarke-Park transformation can be shown using (3.3) [55]:

$$\begin{bmatrix} r_a \\ r_b \\ r_c \end{bmatrix} = \begin{bmatrix} \cos(\omega t) & -\sin(\omega t) \\ \cos(\omega t - 2\pi/3) & -\sin(\omega t - 2\pi/3) \\ \cos(\omega t + 2\pi/3) & -\sin(\omega t + 2\pi/3) \end{bmatrix} \begin{bmatrix} r_d \\ r_q \end{bmatrix} \tag{3.3}$$

So, after Clarke-Park transformation (3.1) can be written as:

$$e_d = Ri_d + L\frac{di_d}{dt} - \omega L i_q + v_d \tag{3.4}$$

$$e_q = Ri_q + L\frac{di_q}{dt} + \omega L i_d + v_q \tag{3.5}$$

where,

$e_d, e_q = \ instantaneaous\ dq\ axes\ voltages\ at\ the\ inverter\ terminal$

$v_d, v_q = instantaneaous\ dq\ axes\ grid\ voltages$

$i_d, i_q = instantaneaous\ dq\ axes\ currents\ from\ GSI\ to\ grid$

Remark 9: As this plant (shown in fig. 3.9) is VSI (voltage source inverter), ideally the voltage (e_{abc}) will be constant and only current will be changed according to active and reactive power demand from the CC.

The instantaneous active and reactive power can be shown as [55]:

$$P = \frac{3}{2}(v_d i_d + v_q i_q) \tag{3.6}$$

$$Q = \frac{3}{2}(v_q i_d - v_d i_q) \tag{3.7}$$

where,

$P = instantaneous\ active\ power\ delivered\ by\ the\ plant$

$Q = instantaneous\ reactive\ power\ delivered\ by\ the\ plant$

If the d axis is perfectly aligned with the grid voltage $v_q = 0$, (3.6) and (3.7) can be written as

$$P = \frac{3}{2} v_d i_d \tag{3.8}$$

$$Q = -\frac{3}{2} v_d i_q \tag{3.9}$$

In our case, active power P and reactive power Q are the reference quantities given by CC. Hence, reference i_d and i_q can be calculated using (3.10) and (3.11):

$$i_{d,ref} = \frac{2}{3}\frac{P_{ref}}{v_d} \tag{3.10}$$

$$i_{q,ref} = -\frac{2}{3}\frac{Q_{ref}}{v_d} \tag{3.11}$$

Writing (3.4) and (3.5) again,

$$e_d = u_d - \omega L i_q + v_d \tag{3.12}$$

$$e_q = u_q + \omega L i_d + v_q \tag{3.13}$$

where,

$u_d = Ri_d + L\frac{di_d}{dt}$ & $u_q = Ri_q + L\frac{di_q}{dt}$

Based on the requirements of the P and Q, i_d and i_q can be calculated using (3.10) and (3.11). Then, using (3.12) and (3.13) e_d and e_q can be derived. Inverse Clarke-Park transformation is used to convert e_d and e_q quantities into $e_{abc,ref}$. Then, $e_{abc,ref}$ can be given to GSI using SVPWM as shown in Figure 3.9.

Remark 10: In controller design, the linearized (small signal) model is used, and the inverter (GSI) is considered ideal. Using the given $e_{abc,ref}$, GSI generates e_{abc}. Hence, in this case, $e_{abc} = e_{abc,ref}$.

Using (3.10) to (3.13), open loop controllers can be shown as:

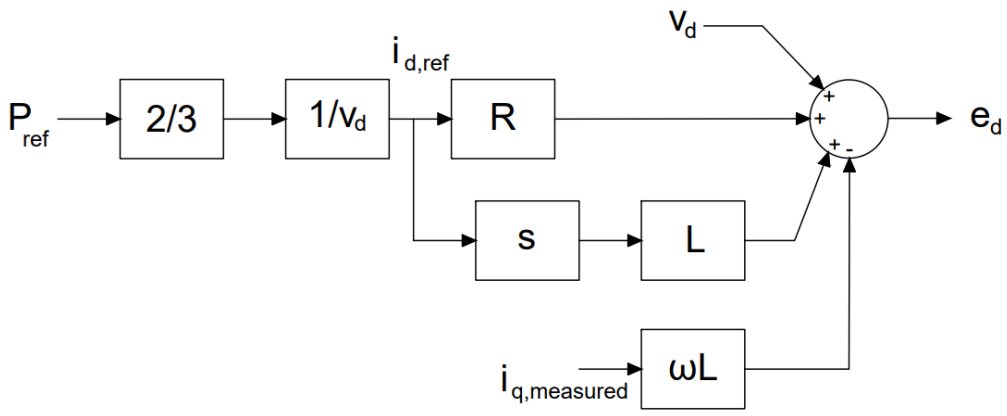

Figure 3.10 Open loop control with the reference P

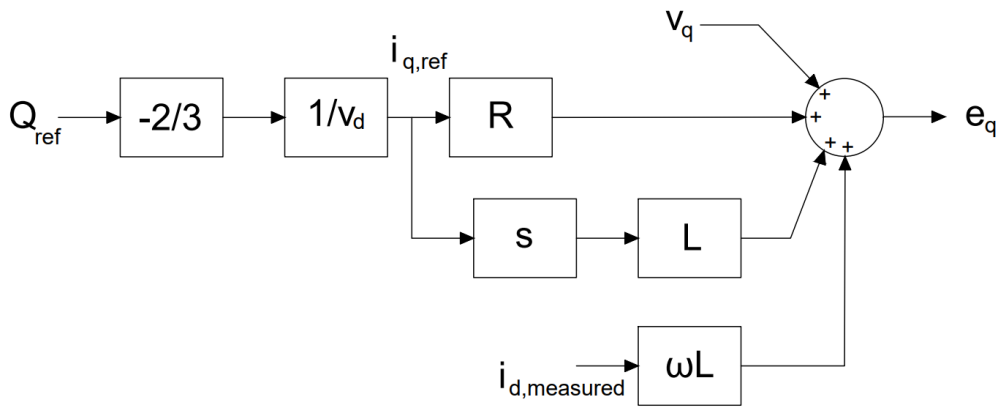

Figure 3.11 Open loop control with the reference Q

To achieve certain transient specifications and zero steady state error for the step input, closed loop controls with PI controllers are used:

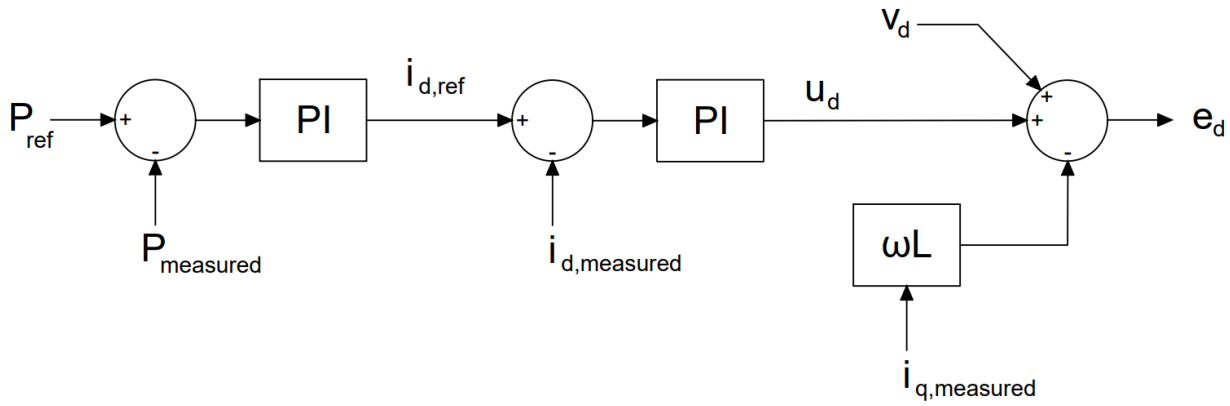

Figure 3.12 Closed loop control with the reference P

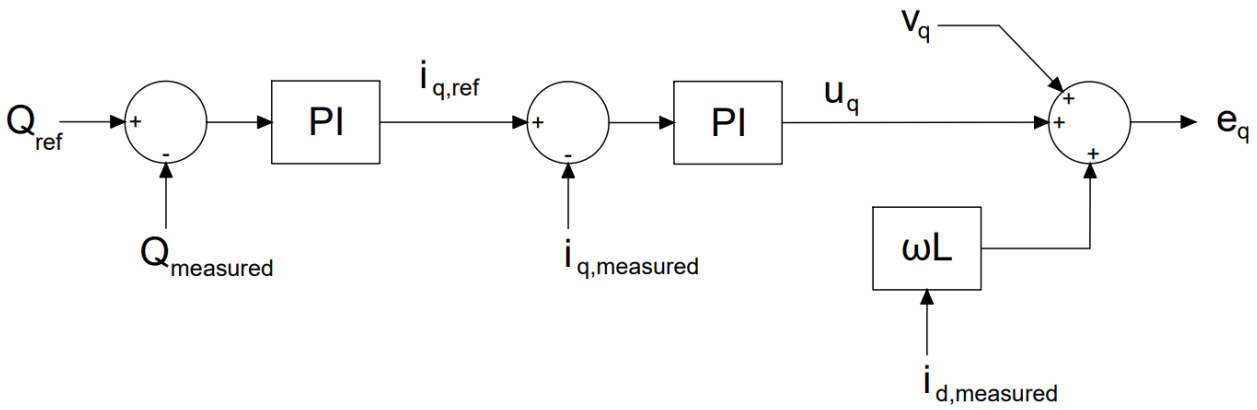

Figure 3.13 Closed loop control with the reference Q

The PI controllers can be defined as:

$$i_{d,ref} = \left(k_{pd1} + \frac{k_{id1}}{s}\right)(P_{ref} - P_{measured}) \tag{3.14}$$

$$i_{q,ref} = \left(k_{pq1} + \frac{k_{iq1}}{s}\right)(Q_{ref} - Q_{measured}) \tag{3.15}$$

$$u_d = \left(k_{pd2} + \frac{k_{id2}}{s}\right)(i_{d,ref} - i_{d,measured}) \tag{3.16}$$

$$u_q = \left(k_{pq2} + \frac{k_{iq2}}{s}\right)(i_{q,ref} - i_{q,measured}) \tag{3.17}$$

The closed loop controls with plant and PoM can be shown using Figures 3.14 and 3.15.

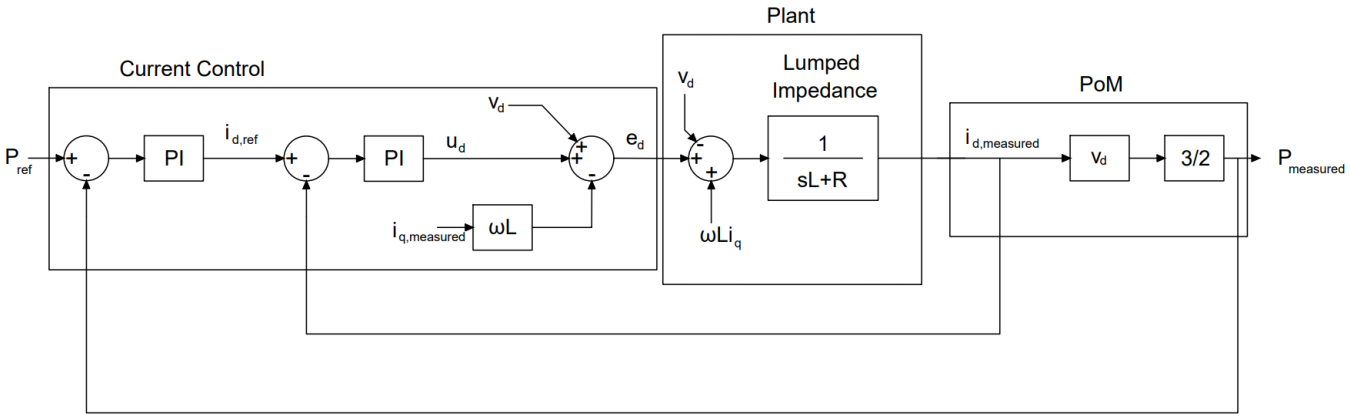

Figure 3.14 Current control of active power P with plant and PoM

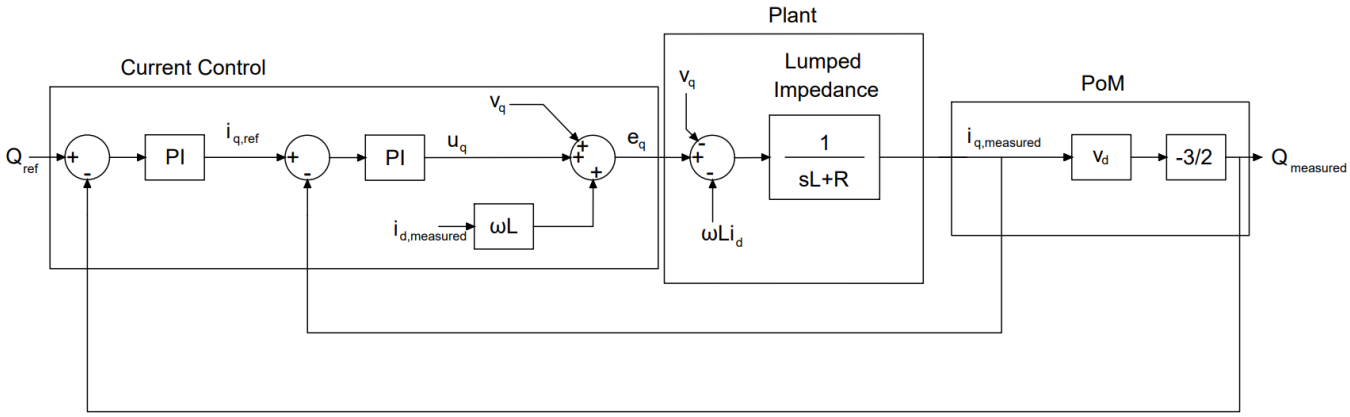

Figure 3.15 Current control of reactive power Q with plant and PoM

Now that we have reviewed the modelling of a power plant, the next step would be to define values for our simulation. Usually, generators or PV arrays can generate power in kW or MW. In our case, 100kW is chosen as the maximum power generation capacity (active power P) of the plant.

The other parameters that were used for the model shown in the Figure 3.9 are:

Grid's phase to phase, rms voltage $v_{ph-ph,rms}$: $400V$

(This voltage can be converted to any other value using a transformer)

Frequency f: $60Hz$

Reference inputs from the CC:

$$P_{ref} = 90kW \; and \; Q_{ref} = 15kVAR$$

Lumped impedance (resistance R & inductance L) can be considered as a total impedance from inverter terminals to PoM. This contains impedance of filters, transformer, cables etc. In our case, first R and L were calculated according to the filter design calculations [59], and then the lumped impedance was taken around that value:

$$R\text{: } 0.01\Omega \text{ and } L\text{: } 1.3mH$$

According to [59],

$$V_{DC} \geq \sqrt{3} v_{ph-ph,peak} \tag{3.18}$$

$$\therefore V_{DC} \geq \sqrt{3} \times \sqrt{2} \times v_{ph-ph,rms} = \sqrt{6} * 400 \cong 979.8V$$

Hence, $V_{DC} = 1000V$ is taken.

We are adding power (P_{ref} and Q_{ref}) into the grid. Hence, the value of i_d and i_q will change according to (P_{ref} and Q_{ref}) at the constant grid voltage (v_d and v_q). Inverter voltages (e_d and e_q) will be equal to the summation of voltage drop due to lumped impedance and a grid voltage (v_d and v_q). Although, the voltage dop due to lumped impedance is usually much smaller than grid voltages. Hence, Inverter voltages (e_d and e_q) are approximately the same as grid voltages (v_d and v_q).

For the values defined above,

$v_d = e_d = 326.6V$

$v_q = e_q = 0V$

$i_d = 183.7A$

$i_q = -30.6A$

While given step input, the transient specifications for the outer loop shown in Figures 3.12 and 3.13 could be different according to different standards, type of plant and control strategy used. Here, the following specifications were used for both inner and outer loops, which cover most of the standards such as IEEE, IEC, etc.:

$rise\ time\ t_r = 0.2s$

$settling\ time\ t_s = 0.6s$

$Percentage\ of\ overshoot\ = 3\%$

$steady\ state\ error\ for\ step\ input\ e_{ss} = 0$

PI controllers can be tuned using simple pole placement or any other method. The gains of the PI controllers are:

P loop: $k_{pd1} = 0.001$, $k_{id1} = 0.05$; $k_{pd2} = 10$, $k_{id2} = 100$

Q loop; $k_{pq1} = -0.001$, $k_{iq1} = -0.05$; $k_{pq2} = 6$, $k_{iq2} = 70$

In the next section, the multi-sine watermark is derived for the MIMO system presented in this section.

3.2.2 Watermarking Signal Design and Considerations

To develop a multi-sine watermarking signal as explained in section 2.2, the order of the transfer function and frequency response for the frequencies that is used for the watermarking are needed. In our case, we are going to apply watermark in the reference signals P_{ref} and Q_{ref}, and we want to see the effects of watermarking in the generated P & Q. Hence, the transfer function should be from reference signals (P_{ref} & Q_{ref}) to measured signals ($P_{measured}$ & $Q_{measured}$), i.e., combined transfer functions of plant (with controller & lumped impedance) and point of measurement (PoM) shown in Figures 3.14 and 3.15. PoM calculates instantaneous P and Q according to (3.8) & (3.9).

The terms $\omega L i_q$ & v_d in Figure 3.14 and $\omega L i_d$ & v_q in Figure 3.15 are decoupling terms that are cancelling the effect of coupling which is already there due to Clark-park transformation. Hence, the overall transfer functions of both the cases (Figures 3.14 & 3.15) are independent of each other. The simplified block diagram of Figures 3.14 and 3.15 around the operating point can be shown using Figures 3.16 And 3.17.

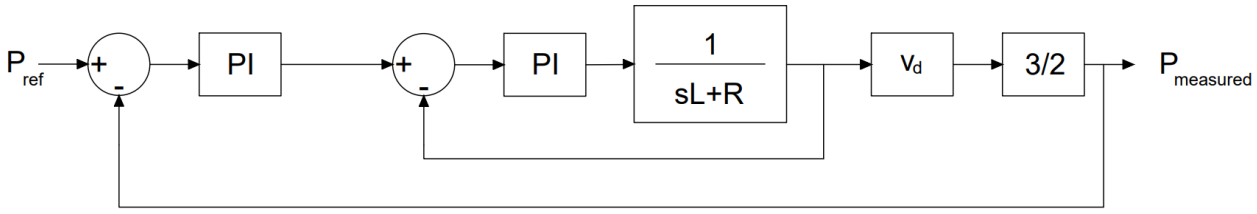

Figure 3.16 Simplified block diagram of control loop P

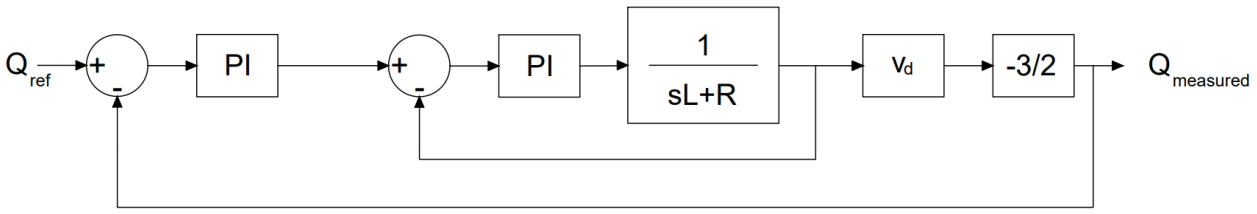

Figure 3.17 Simplified block diagram of control loop Q

The systems shown in fig. 3.16 and 3.17 are of order three. The transfer function for Fig. 3.16 can be shown as,

$$G_P(s) = \frac{P_{measured}(s)}{P_{ref}(s)} = \frac{4.9s^2 + 293.9s + 2450}{0.0013s^3 + 4.91s^2 + 294s + 2450} \tag{3.19}$$

Similarly for Fig. 3.17,

$$G_Q(s) = \frac{Q_{measured}(s)}{Q_{ref}(s)} = \frac{2.94s^2 + 181.3s + 1715}{0.0013s^3 + 2.95s^2 + 181.2s + 1715} \tag{3.20}$$

The bode plots of these systems are:

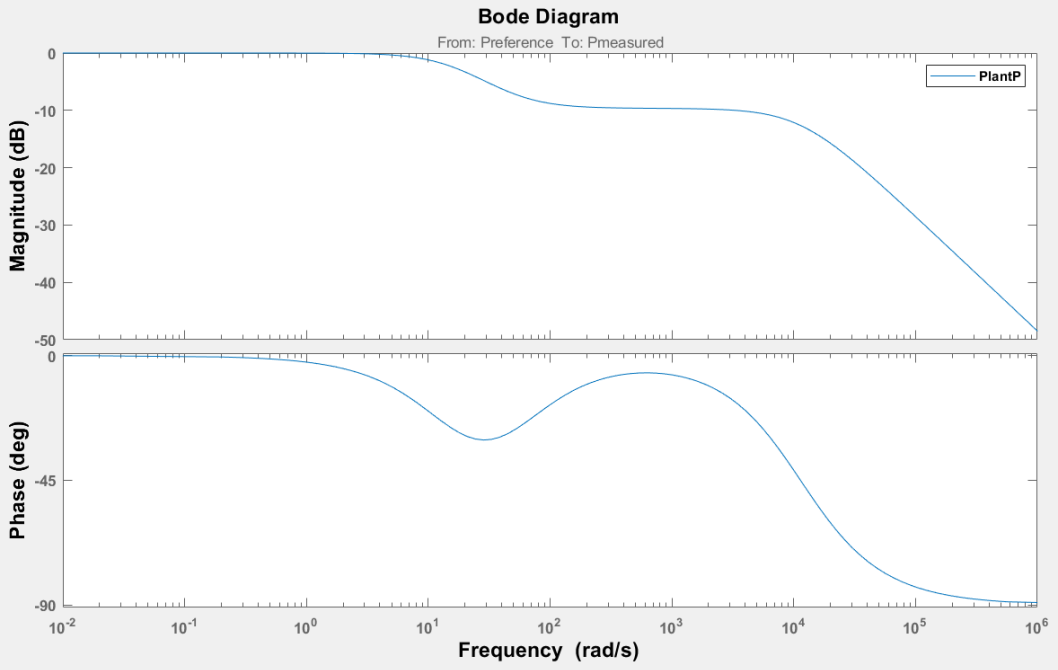

Figure 3.18 Bode plot of system shown in Fig. 3.16

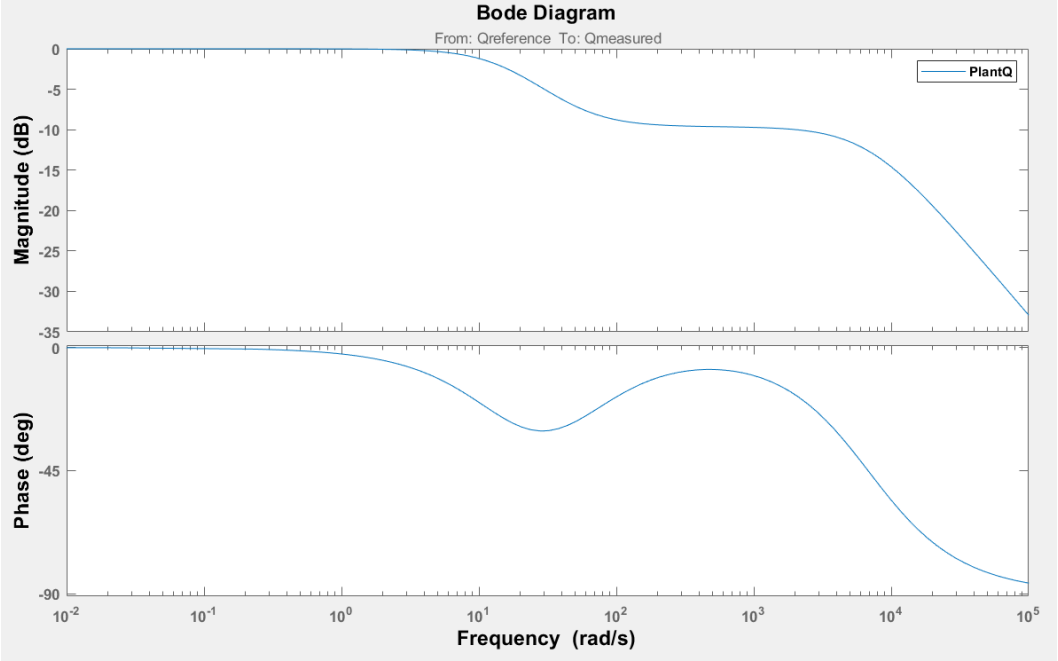

Figure 3.19 Bode plot of system shown in Fig. 3.17

For the 3rd order system, the watermarking signal needs two sine waves to suppress the transient. For both the reference signals P_{ref} and Q_{ref}, the watermark can be shown as:

$$WM_P = A_{P1}sin(\omega_{P1}t + \emptyset_{P1}) + A_{P2}sin(\omega_{P2}t + \emptyset_{P2}) \tag{3.21}$$

$$WM_Q = A_{Q1}sin(\omega_{Q1}t + \emptyset_{Q1}) + A_{Q2}sin(\omega_{Q2}t + \emptyset_{Q2}) \tag{3.22}$$

Now we present the guidelines for choosing the parameters mentioned in (3.21) and (3.22).

- **Choosing range of frequencies**

From the Bode plots, frequencies between 0.1Hz (0.63rad/s) to 6Hz (37.7rad/s) can be used because of the following reasons:

1. Frequencies of the watermarking signals must be significantly lower than switching frequency. It may add harmonics in the current and place an extra burden on power electronics and other electrical devices. It may also increase switching losses and trip protective devices unnecessarily.
2. Furthermore, frequencies should be considerably lower than the grid frequency. For the grid frequency $f = 60Hz$, the frequencies of the watermarking signals should be smaller than $f/10 = 6Hz$.
3. The sensors should be able to detect and communicate the watermarking signals to the CC. As the time-period of watermarking signals with higher frequencies is smaller, this may require faster sensing and more frequent communication between plants and CC.
4. Control systems are less accurate on higher frequencies.
5. There will always be some fluctuations and noises present in the output due to switching harmonics and sensing devices. These noises are usually of higher frequencies. To distinguish watermarking from these noises, the watermarking with lower frequencies should be chosen.
6. According to the bode plots, magnitude (dB) should be relatively higher. In our case the highest magnitude is around 0dB. If magnitude is less, that means in the reference signal we will have to give watermarking of the higher magnitude for the same signal that is detectable at the output.
7. Frequency should not be too low. Low frequency means a higher time-period (higher $T_{combined}$ & T_{frame}) of the signal. That would give attackers more time to figure out the watermarking and artificially replicate it into the measurement signals.
8. The range of frequencies should be wide enough to allow watermarking frequencies in different frames that are sufficiently apart for later detection through PSD methods.

Guidelines 6, 7 and 8 were adapted from [45]. Other guidelines were introduced here for smart grids.

- **Choosing total amplitude**

For smart grids, the total amplitude of the watermarking should be kept as low as possible. Although, it depends on two factors:

1. Power generation capacity of the plant and

2. Ability of the detector to detect, despite fluctuations (fluctuations are mostly due to power electronics switching)

The flowchart shown in Figure 3.20 represents the trial-and-error method to determine the total amplitude of watermarking.

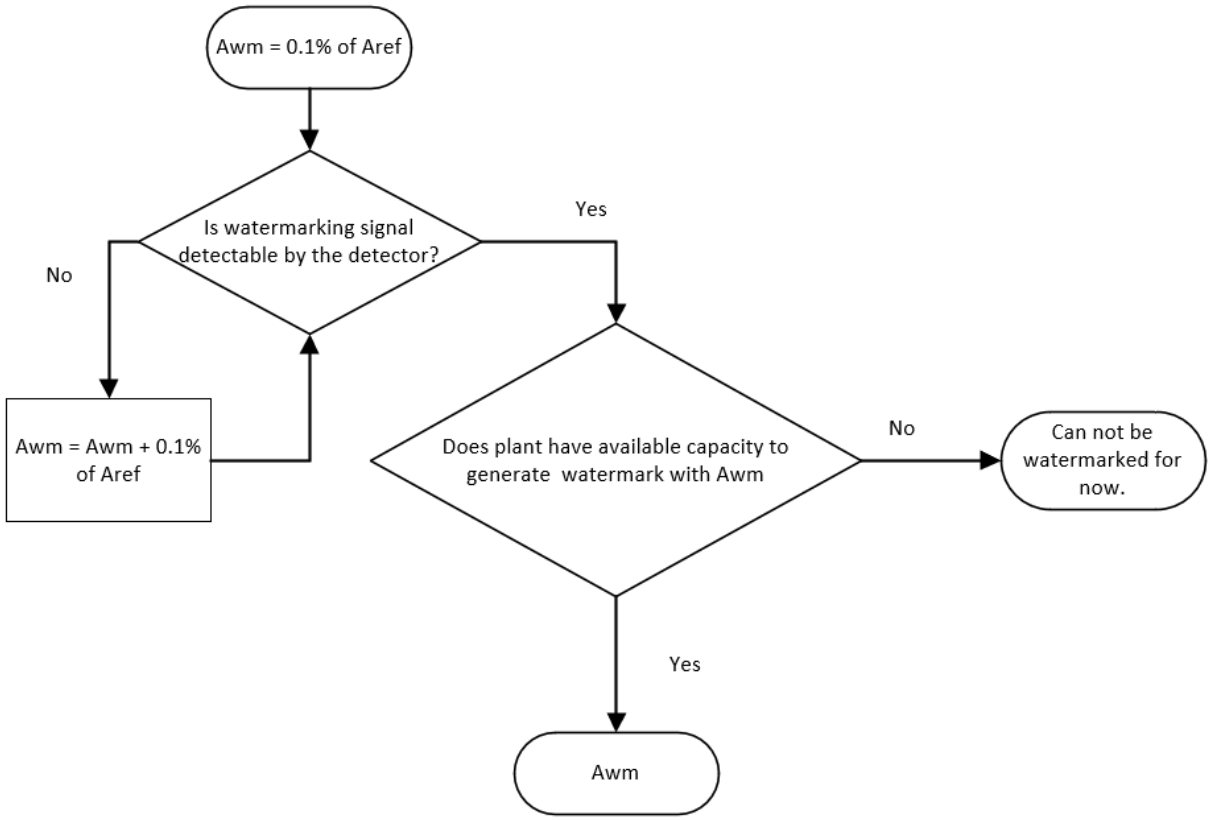

Figure 3.20 Flowchart for selecting total amplitude of the watermark

Notations used:

$A_{WM} = Total\ amplitude\ of\ watermarking\ signal\ (A_P\ or\ A_Q)$

$A_{ref} = Amplitude\ of\ reference\ signal\ (P_{ref}\ or\ Q_{ref})$

Starting from lowest amplitude, we can check at which amplitude the watermarking is detectable using the periodogram with 95% confidence bounds and then at next step, we can see if the plant has enough capacity to generate watermarking or not. If not, then for now, CC will focus on generating watermarking for other plants. The method to check the detectability of the watermarking signal at specific amplitude is covered in section 2.3.

To prevent the attackers from getting used to the watermarking signal, the following methods can be used:

1. The frame of the watermarking can be kept minimum i.e., $Number\ of\ frames\ k = 1$.
2. The frequencies $\omega_1\ and\ \omega_2$ can be chosen randomly every time.
3. In [45], the watermark was applied continuously while changing the frequencies of the signals. Continuous watermarks can affect the grid (explained in the next chapter) and can result in power fluctuations. To prevent this, intermittent watermarking can be used by adding the frames of watermarking (with different but random $\omega_1\ and\ \omega_2$) at a random period. It will also stop attackers from figuring out the watermarking.

For our case, watermarking frequencies

$\omega_{P1} = 0.6283\ rad/s\ (f_1 = 0.1Hz)$,

$\omega_{P2} = 1.885\ rad/s\ \ (f_2 = 0.3Hz)$ were used for P control loop and

$\omega_{Q1} = 0.942\ rad/s\ (f_1 = 0.15Hz)$

$\omega_{Q2} = 2.826\ rad/s\ \ (f_2 = 0.45Hz)$ were used for Q control loop.

In both cases, $\frac{f_1}{f_2} = \frac{p_1}{p_2} = \frac{1}{3}$. Also,

$$T_{frameP} = kT_{combinedP} = 1 * T_{combinedP} = p_1 T_{P1} = 1 * 10 = 10s$$

$$T_{frameQ} = kT_{combinedQ} = 1 * T_{combinedQ} = p_1 T_{Q1} = 1 * 6.67 = 6.67s$$

The magnitude and phase angle of each system shown in Figures 3.16 and 3.17 are:

$$\angle G_P(j\omega_{P1}) = 0.02512\, rad \qquad \angle G_Q(j\omega_{Q1}) = 0.036116 rad$$
$$\angle G_P(j\omega_{P2}) = 0.07536\, rad \qquad \angle G_Q(j\omega_{Q2}) = 0.11411\, rad$$
$$|G_P(j\omega_{P1})| = 1 \qquad |G_Q(j\omega_{Q1})| = 0.999$$
$$|G_P(j\omega_{P2})| = 0.9925 \qquad |G_Q(j\omega_{Q2})| = 0.99$$

Following (2.8) and (2.9) with $\alpha_1 = 0$ and $\alpha_2 = \pi$ results in,

$$\phi_{P1} = -\angle G_P(j\omega_{P1}) = -0.02512\, rad \qquad \phi_{Q1} = -\angle G_Q(j\omega_{Q1}) = -0.036116\, rad$$
$$\phi_{P2} = \pi - \angle G_P(j\omega_{P2}) = 3.06464\, rad \qquad \phi_{Q2} = \pi - \angle G_Q(j\omega_{Q2}) = 3.02589\, rad$$

Remark 11: In this document, the total amplitude of the watermarking signals is taken to be 1% of the reference value assuming that it is the lowest possible value of the watermarking signal that can be detected by the detector after doing the analysis on periodogram with 95% confidence bounds. Also, it is assumed that the plants have enough capacity to generate watermarking signal of such amplitudes.

The total amplitude of watermarking signal for reference P = $1\%\ of\ P_{ref} = 900W$ and amplitude of watermarking signal for reference Q = $1\%\ of\ Q_{ref} = 150W$. According to (2.20), the amplitude of each sinusoidal will be:

$$A_{P1} = 675 \qquad A_{Q1} = 112.61$$
$$A_{P2} = 226.7 \qquad A_{Q2} = 37.88$$

Now (3.21) and (3.22) can be written as:

$$WM_P = 675sin(0.6283t - 0.02512) + 226.7sin(1.885\,t + 3.06464) \quad (3.23)$$

$$WM_Q = 112.61sin(0.942\,t - 0.036116) + 37.88sin(2.826t + 3.02589\,) \quad (3.24)$$

Using the information so far, the plant with watermarking was simulated using Simulink:

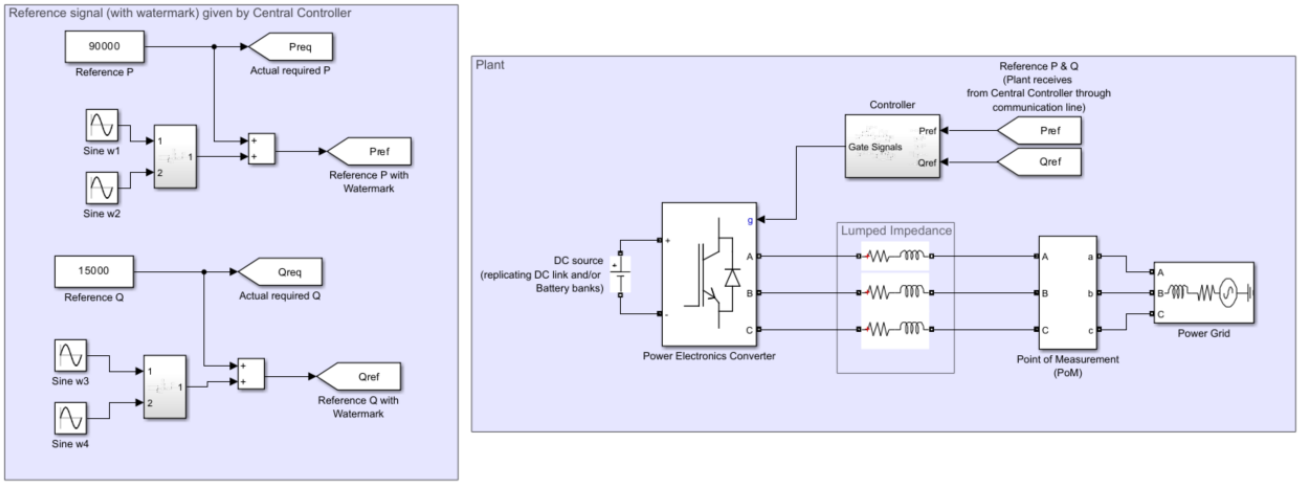

Figure 3.21 Single plant model with watermarking - simulated using Simulink

Remark 12: The communication should be in real time. The delay in the communication lines should be considered while detecting the watermark in the measured signal. According to [60]*, the communication channel delay could be from 100ms to 2s depending on the communication method. If the readings are time-stamped, then it should not be an issue. In our case, for simplicity, this delay is not considered.*

Watermark WM_P was applied between 6s to 16s. Note that, at the start and end of the frames there are no transients.

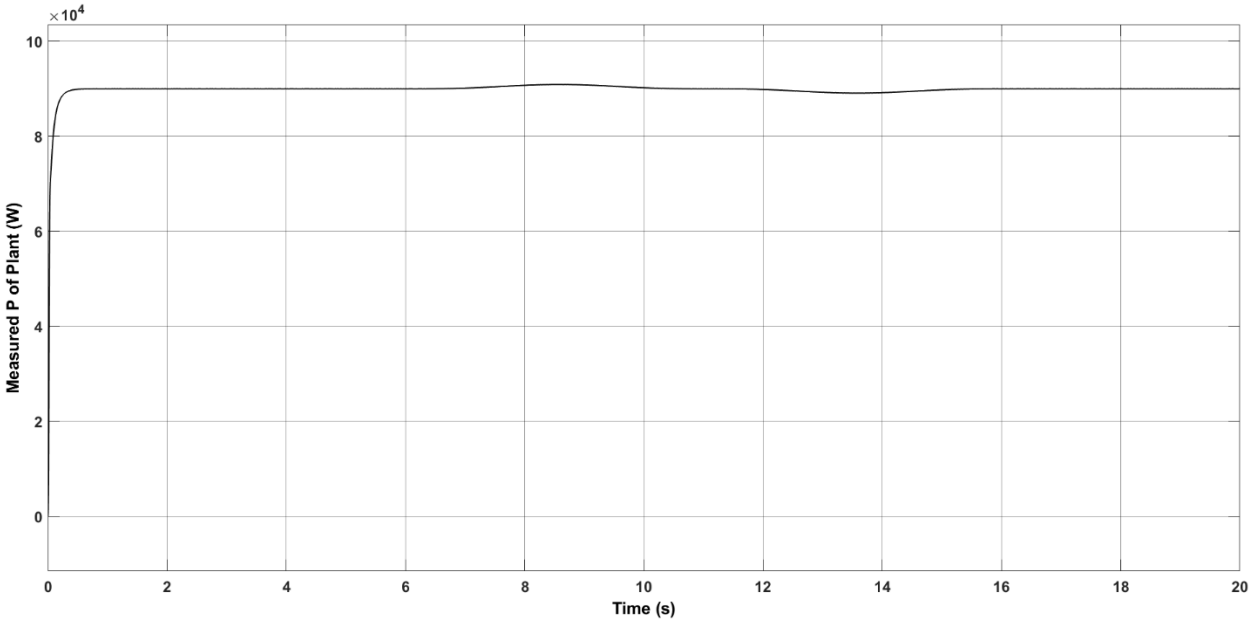

Figure 3.22 Measured P with watermarking

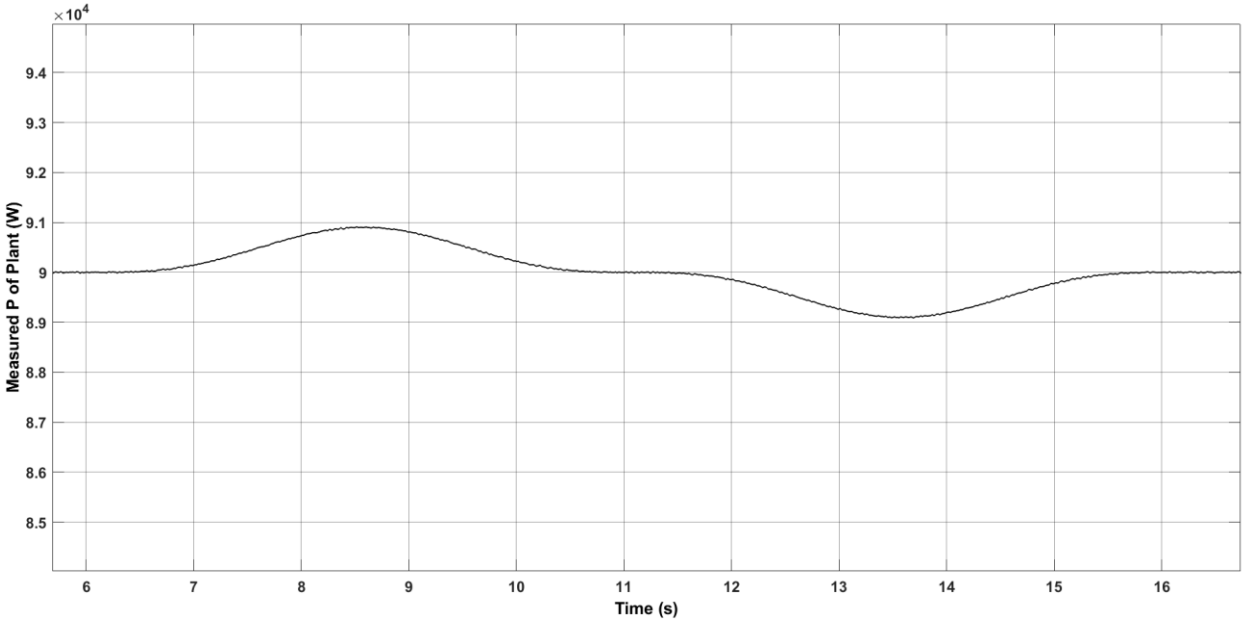

Figure 3.23 Measured P with watermarking (zoomed in)

The watermark can be detected by Power Spectral Density estimates using periodogram. As CC knows in which time interval the watermarking would be available in the measured signal (considering communication delay), it will only consider data within that time for PSD estimation.

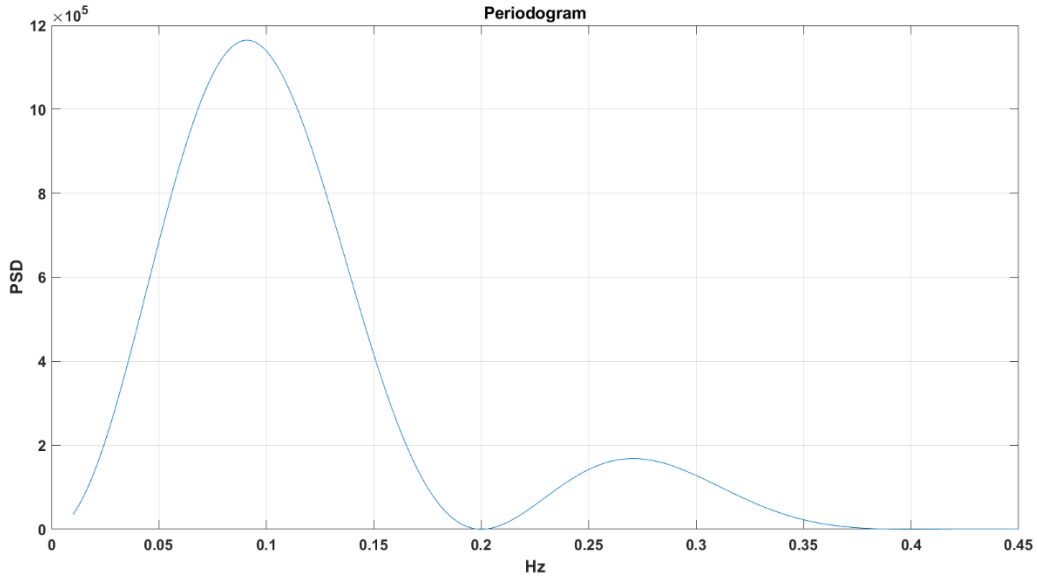

Figure 3.24 Detection of watermarking in reference P using Periodogram

Fig. 3.24 shows the periodogram of P signal between $t = 6s$ and $t = 16s$ after the DC component has been removed. There is a higher power density near the frequencies of 0.1Hz and 0.3Hz because of the watermark. As the amplitude of sine with frequency 0.1Hz is larger, the periodogram shows a higher power density around frequency 0.1Hz than any other frequencies.

For reference Q, WM_Q was applied between 10s and 16.67s.

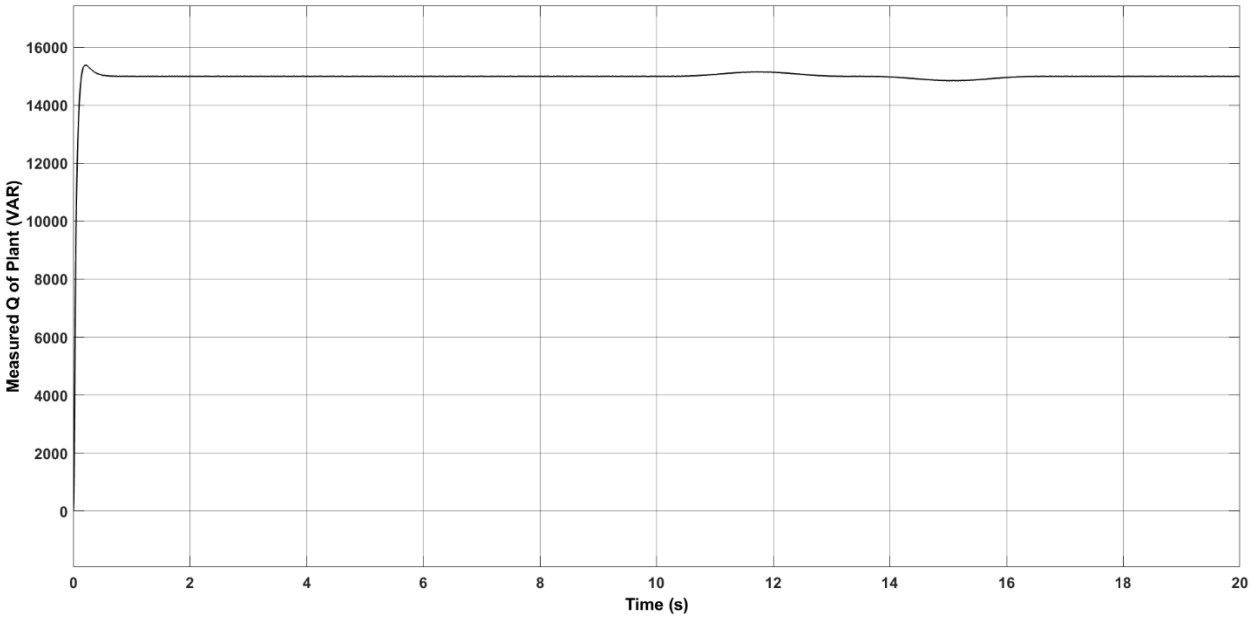

Figure 3.25 Measured Q with watermarking

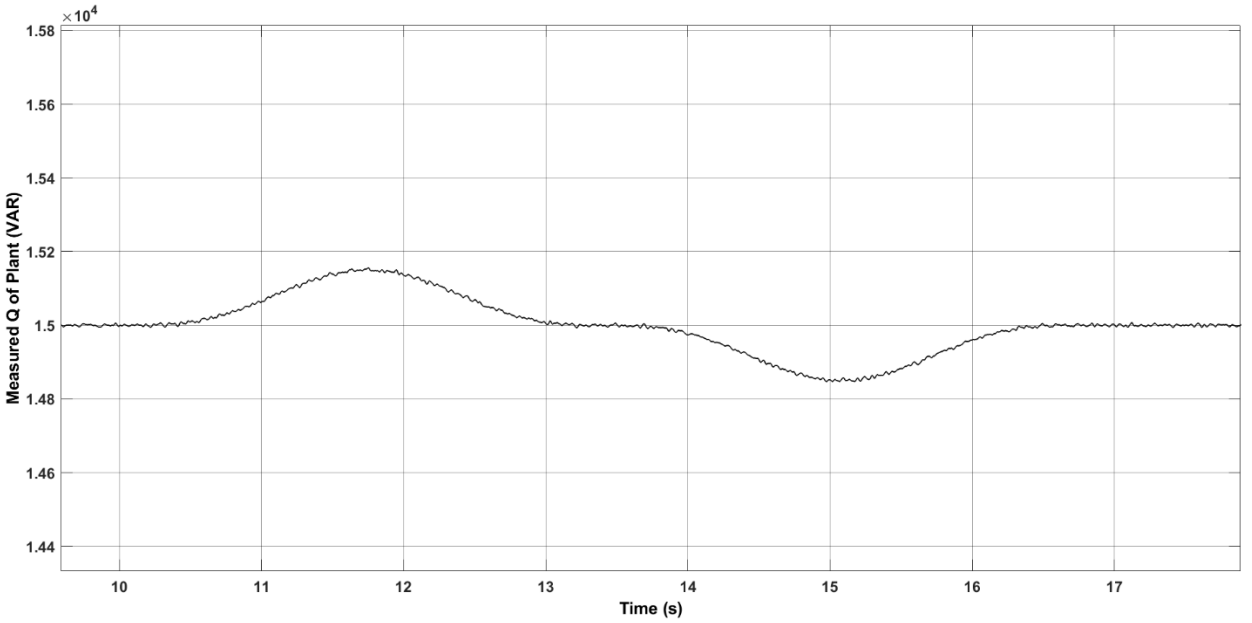

Figure 3.26 Measured Q with watermarking (zoomed in)

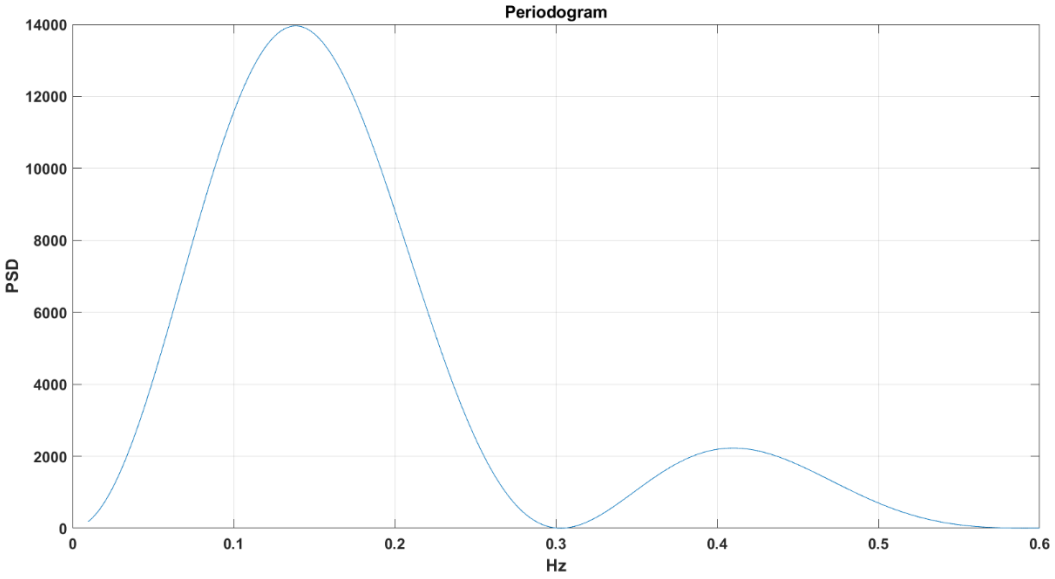

Figure 3.27 Detection of watermarking in reference Q using Periodogram

The periodogram in this case shows the estimation of higher power density around frequencies of 0.15Hz and 0.45Hz which were used for the watermarking in signal Q.

In both cases, if periodogram cannot detect the watermarking frequencies that means there is a replay attack happening within the plant or in between plant & CC.

The harmonics in the current without watermarking are shown in Fig. 3.28.

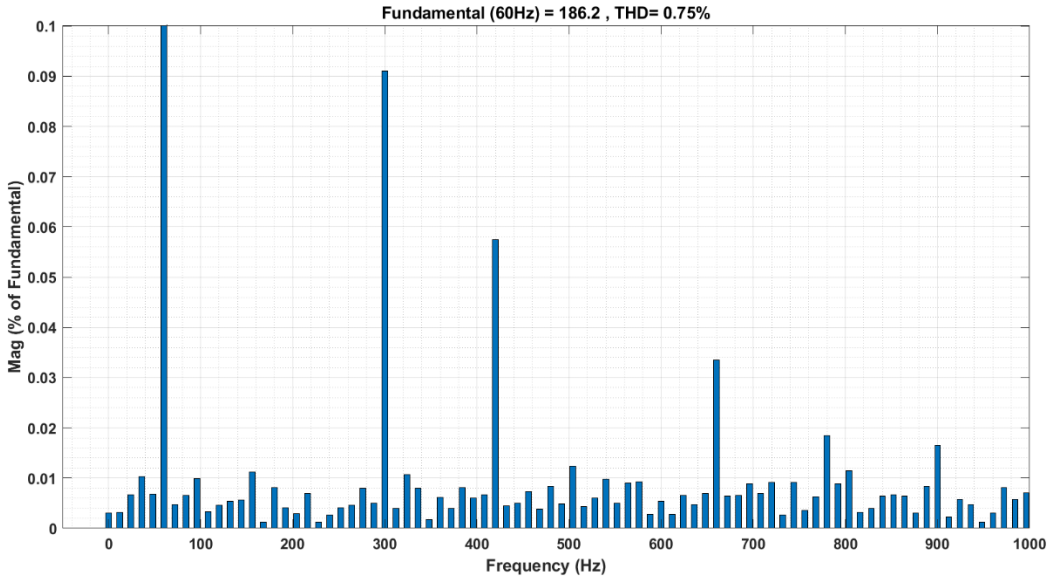

Figure 3.28 Harmonics in the current without watermarking

The harmonics in the current while watermarking was applied in signal P are shown in Fig. 3.29.

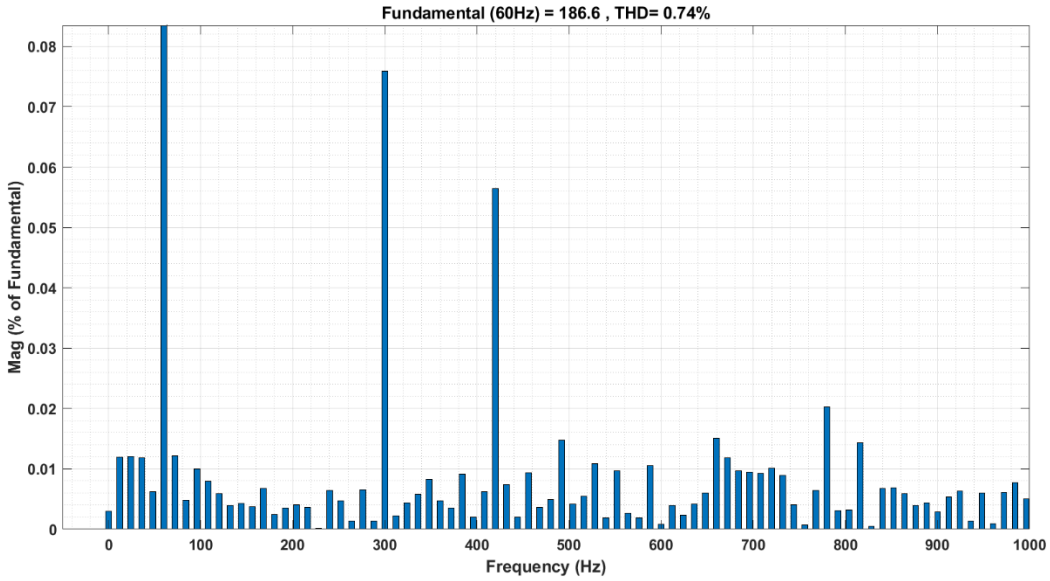

Figure 3.29 Harmonics in the current with watermarking in P

Hence, watermarking does not create any major harmonics in the current. This could be because of the following reasons:

1. Sinewaves are smooth and there is no sudden change in the watermarking.
2. Frequency of sinewaves are lower than switching frequency (in our case, switching frequency is 2kHz).

According to (3.10) and (3.11), $i_{d,ref} \propto P_{ref}$ and, $i_{q,ref} \propto Q_{ref}$, if the watermarking was added in reference signals P and Q, the effects of watermarking can be seen in measured i_d and i_q as well. That is why, if there is a replay attack happening within the plant, it can also be detected using the proposed method.

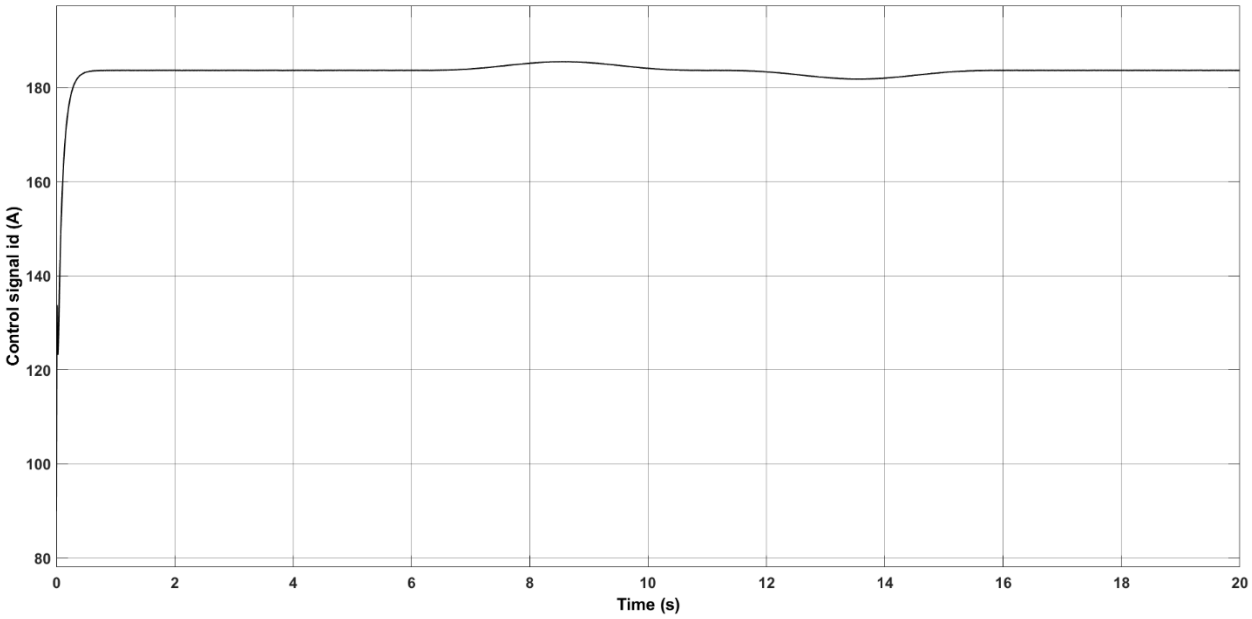

Figure 3.30 Measured control signal id

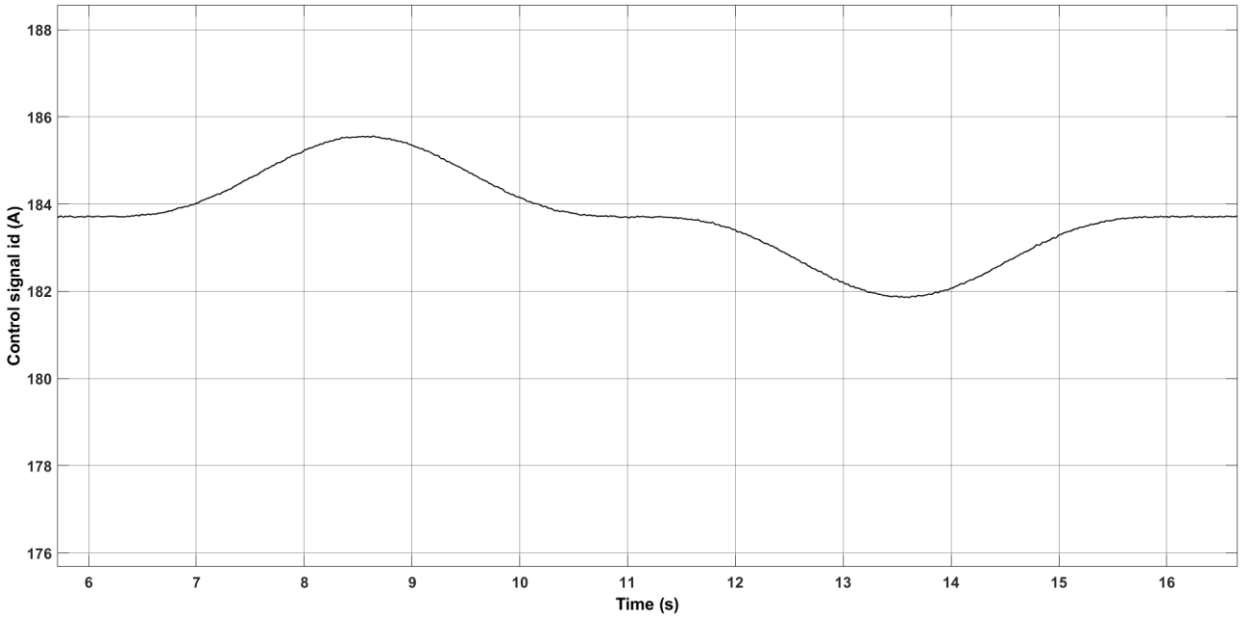

Figure 3.31 Measured control signal id (zoomed in)

Just like signal P, the watermark in control signal i_d can also be seen between 6s to 16s.

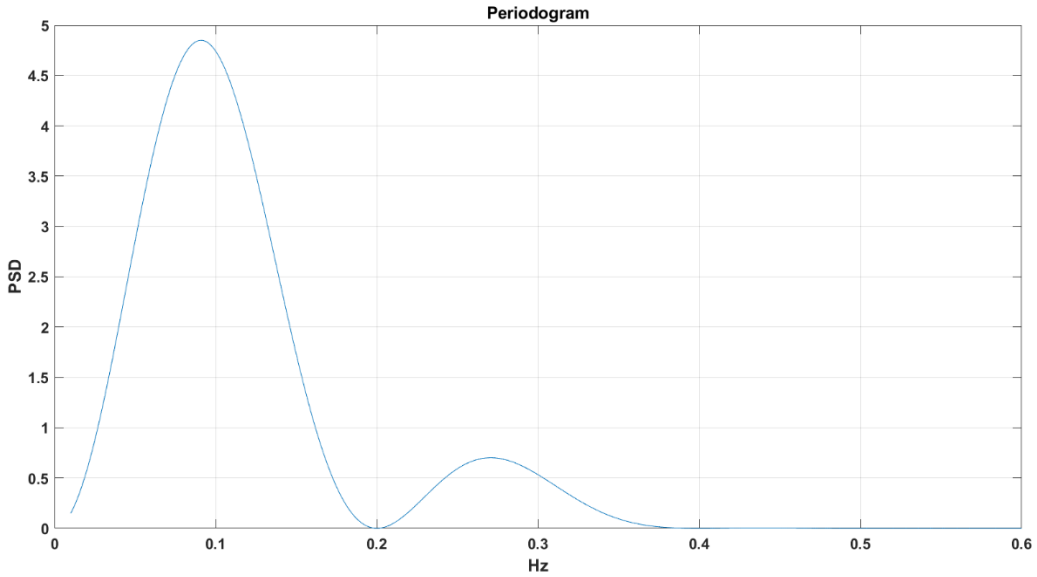

Figure 3.32 Detection of watermarking in control signal id using Periodogram

As shown in fig. 3.32, the same watermarking of 0.1Hz and 0.3Hz can be detected in control signal i_d using periodogram.

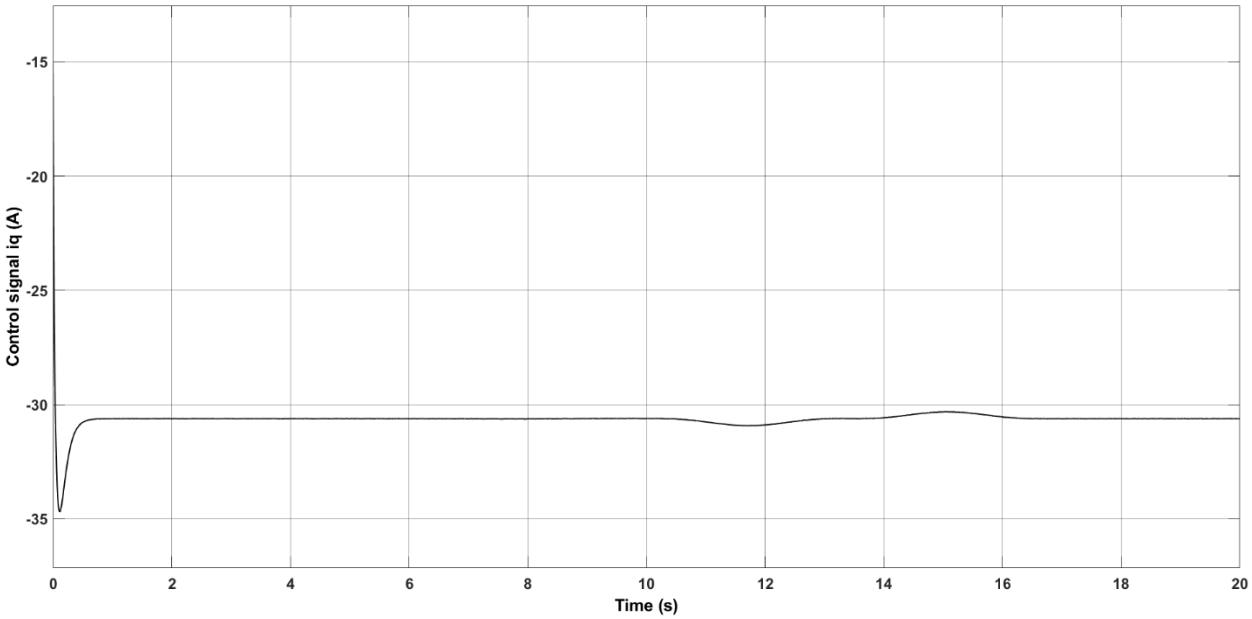

Figure 3.33 Measured control signal iq

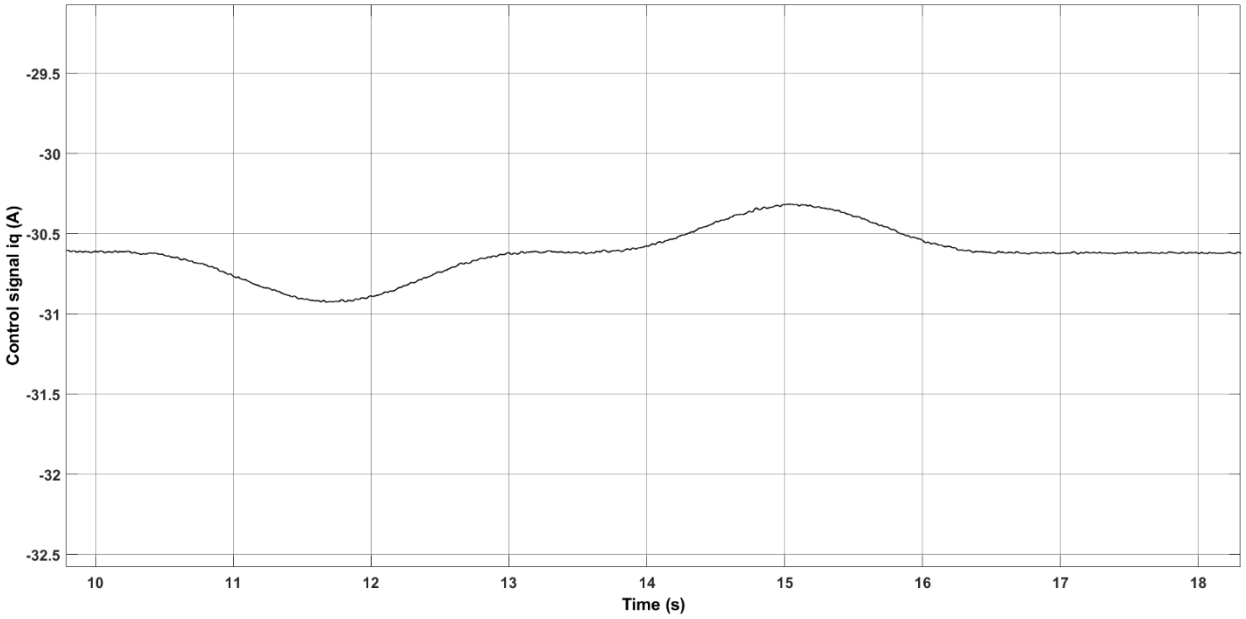

Figure 3.34 Measured control signal iq (zoomed in)

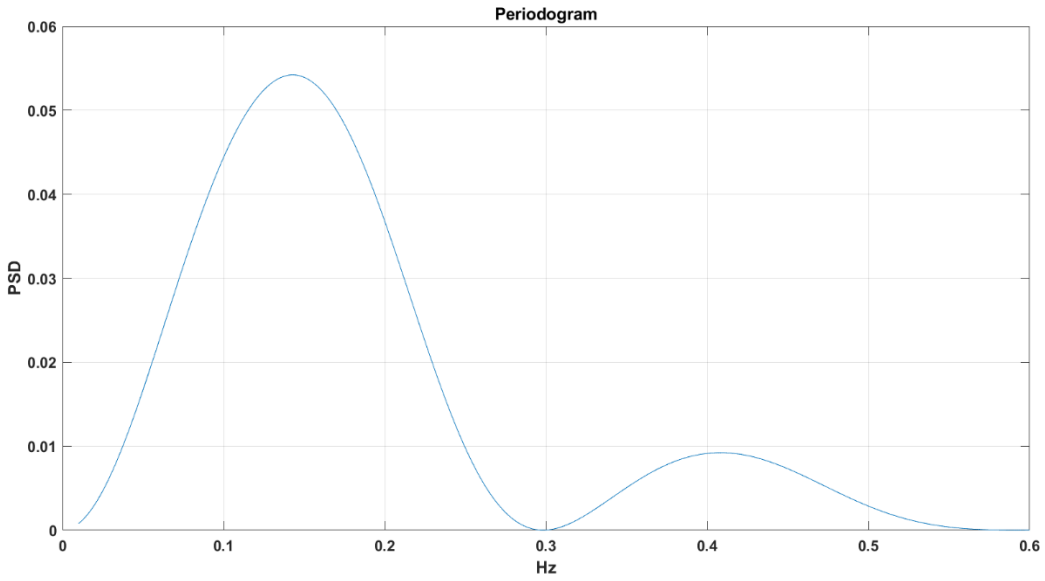

Figure 3.35 Detection of watermarking in control signal iq using Periodogram

Like signal Q, control signal i_q also has the watermarking between 10s to 16.67s with the frequencies of 0.15Hz and 0.45Hz. If these frequencies cannot be detected, that means, there is a replay attack present withing the plant.

In summary, if watermark cannot be detected in P and/or Q that means there is a replay attack occurring within plant or in between plant & CC. To check if the replay attack is happening within the plant, one should check the availability of watermarking in the measured signals i_d and i_q. In this case, the local controller can sense the attack sooner than the CC. If the effect of the similar watermarking is available in i_d and i_q but not P and/or Q that means replay attack should be in between the plant & CC.

3.3 Conclusion

In this chapter, we formalized a method to derive a watermarking signal for detecting replay attacks in smart grids. This scheme helps to detect replay attacks happening within the plant and in between the plant and the CC. The multi-sine watermarking signal does not create any harmonics in the line current. Additionally, it does not place any extra burden on the electrical equipment. Because of this, the possibility of false tripping the protective relay decreases. To implement this method, one of the essential requirements is that communication between the plant and the CC must be faster.

Chapter 4

Mitigating Power Fluctuations

There are a lot of parameters to consider while using a watermarking signal to detect replay attacks in the smart grid. To detect the replay attack successfully and not give attackers enough time to collect healthy data that is without the watermark, the watermarking signal should be added in the reference signal more often. Hence, when the number of plants is higher, the watermarking cannot be added to each plant at a time. Because, then the attackers will have sufficient time to record healthy data while the watermarking is added in the other plants. Suppose the watermarking was applied to all the plants in the grid randomly (at random time and with random amplitude). Then there might come a time when some or all plants are generating watermarking at the same time. So, the effect of fluctuations due to watermarking will be added on the grid. This can affect the grid to a significant level.

In this section, first we will review the problems for using a watermarking in the grid, then we propose a solution to resolve the issue. Later, the suggested solution is verified using the results of a simulation of two grid connected plants.

4.1 Effects of Watermarking on the Grid

The change in the quantities of a group of plants can affect the whole grid. Watermarking signal gives us security against replay attacks, but it also increases the power fluctuations and leads to many problems that can affect an entire power grid. In this section, we begin by evaluating the effects of change in active and reactive power on the overall grid and then, in the next section, a scheme to apply the watermarking is proposed so that watermarking has minimum impact on the grid.

4.1.1 Effects of Active and Reactive Power Change on the Grid

A change in the active power can affect the power (phase) angle δ [61],[55]. Similarly, the change in a reactive power can change the voltage magnitude.

The brief explanation is given using Figure 4.1:

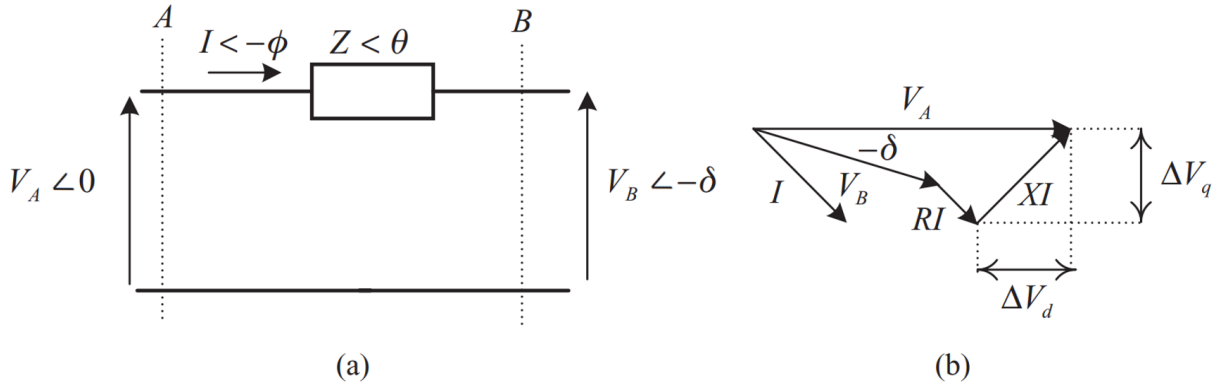

Figure 4.1 Power flow from section A to B [55]

For section A, active power P and reactive power Q can be shown as:

$$P_A = \frac{V_A^2}{Z} cos\theta - \frac{V_A V_B}{Z} \cos(\theta + \delta) \tag{4.1}$$

$$Q_A = \frac{V_A^2}{Z} sin\theta - \frac{V_A V_B}{Z} sin(\theta + \delta) \tag{4.2}$$

where,

$\theta = power\ factor\ angle\ at\ section\ A$

$Z = Total\ impedance\ of\ transmission\ line = R + jX;\quad R = resistance\ \&\ X = reactance$

Usually, the plant is connected to a grid through a transmission line or distribution line which is mainly inductive. Hence, the above equations become,

$$\delta \cong \frac{XP_A}{V_A V_B} \tag{4.3}$$

$$V_A - V_B \cong \frac{XQ_A}{V_A} \tag{4.4}$$

According to (4.3) and (4.4), the change in P_A and Q_A can affect voltage phase angle and magnitude, respectively. While there is a voltage drop between the two buses, to deliver the constant active power, current must be increased. Too much increase in the current can exceed the line loss. It may also overload lines and can cause cascade failures.

The effects can be examined using the modified IEEE 9 bus system shown in Fig. 4.2. In the standard IEEE 9-bus system with three generators [62], one of the generators (at bus 1) is represented as a grid (swing generator). This bus system was modified according to the needs and the 4th generator was added to bus 4.

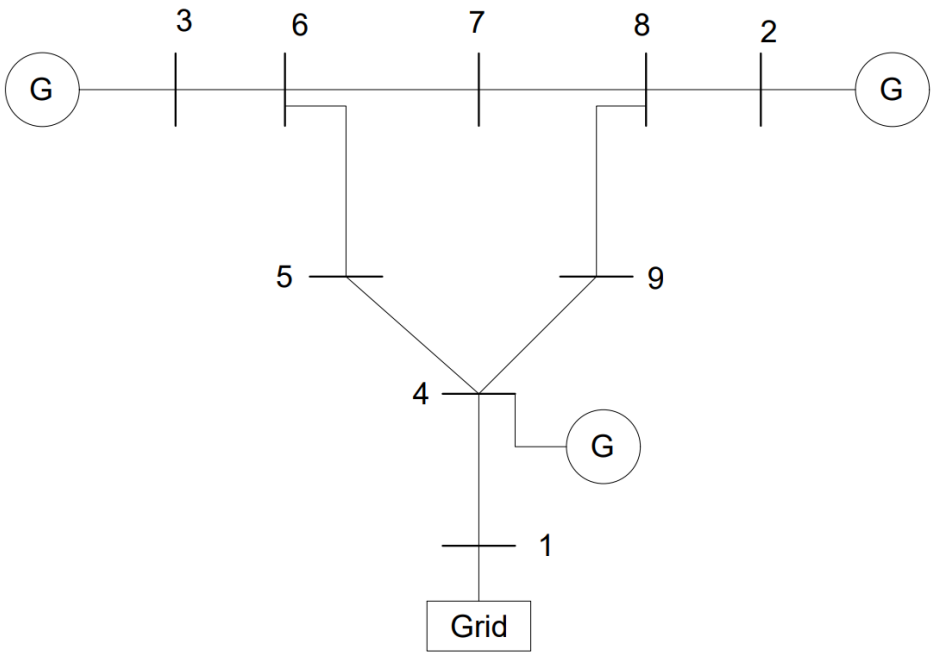

Figure 4.2 Modified IEEE 9 Bus system

In our case, as shown in Fig. 4.2, bus 1 is connected to the swing generator (grid). Buses 2, 3 and 4 are connected to the PQ generators (have P and Q references) and the rest of the buses are connected to PQ loads. The necessary information for the given bus system is given below [62]:

Base apparent power $S = 100\text{MVA}$

Base voltage $V = 230kV$

Remark 13: The line data are usually mentioned in pu (per unit). Any pu quantities can be converted in the standard units using base apparent power and base voltage.

Table 4.1 Line data

From Bus	To Bus	Line data (in per unit; pu)		
		Resistance r	Reactance x	Impedance z
1	4	0	0.0576	0.0576
4	5	0.017	0.092	0.093557
5	6	0.039	0.17	0.174416
3	6	0	0.0586	0.0586
6	7	0.0119	0.1008	0.1015
7	8	0.0085	0.072	0.0725
8	2	0	0.0625	0.0625
8	9	0.032	0.161	0.164149
9	4	0.01	0.085	0.085586

Table 4.2 Generated constant power during normal condition

	Active Power P (MW)	Reactive Power Q (MVAR)
Bus 2	162	8
Bus 3	85	3
Bus 4	20	2

Table 4.3 Connected constant load

	Active Power P (MW)	Reactive Power Q (MVAR)
Bus 5	90	30
Bus 7	100	35
Bus 9	125	50

Table 4.4 shows the voltage magnitude and power angle on each bus after a load flow analysis using the Newton Raphson method.

Table 4.4 Case 0: Load Flow data (under normal condition)

Bus	**Voltage V (pu)**	**Angle δ (rad)**
1	1	0
2	0.995991	0.177765
3	1.012541	0.090599
4	0.989662	-0.03078
5	0.980533	-0.05921
6	1.012	0.041974
7	0.989335	0.019969
8	0.996162	0.075564
9	0.959567	-0.06519

To see the effect on power angle δ due to change in active power, we first change (increase) the active power by 1% for the generator connected to bus 2. Next in the second scenario, we apply the same changes to all the generators (connected to buses 2, 3 and 4) at the same time. For this analysis, we will use voltage sensitivity matrix (2.27).

Case 1.1 (1% increase on Bus 2):

$\Delta P_{BUS\,2} = 1.62MW$

$\Delta P_{BUS\,3} = 0MW$

$\Delta P_{BUS\,4} = 0MW$

Table 4.5 Case 1.1: 1% increase in active power P on Bus 2

Bus	**$\|\Delta\delta\|$ (in rad)**
1	0
2	0.004472
3	0.002447
4	0.000933
5	0.001465
6	0.002447
7	0.003037
8	0.003459
9	0.001807

Case 1.2 (1% increase on Bus 2, 3 and 4):

$\Delta P_{BUS\,2} = 1.62MW$

$\Delta P_{BUS\,3} = 0.85MW$

$\Delta P_{BUS\,4} = 0.2MW$

Table 4.6 Case 1.2: 1% increase in active power P on Buse 2, 3 and 4

Bus	**$\|\Delta\delta\|$ (in rad)**
1	0
2	0.005871
3	0.004909
4	0.001538
5	0.002546
6	0.004411
7	0.004671
8	0.004859
9	0.002688

In case 1.1, there is no considerable change in the phase angle. The change increases when all the generators are going through the change in active power at the same time (case 1.2). Hence, if all or the larger group of plants are generating the watermarking at the same time, then there can be significant change in the phase angle.

To see the change in voltage magnitudes due to change in reactive power we do the same. First, we increase the reactive power by 1% for the generator connected to bus 2, and then we apply the same changes to all the generators at the same time.

Case 2.1 (1% increase on Bus 2):

$\Delta Q_{BUS\,2} = 0.08MVAR$

$\Delta Q_{BUS\,3} = 0MVAR$

$\Delta Q_{BUS\,4} = 0MVAR$

Table 4.7 Case 2.1: 1% increase in reactive power Q on Bus 2

Bus	|ΔV| (in pu)
1	0
2	0.000291
3	0.000191
4	0.00007
5	0.000117
6	0.000191
7	0.000223
8	0.000241
9	0.000134

Case 2.2 (1% increase on Bus 2, 3 and 4):

$\Delta Q_{BUS\,2} = 0.08MVAR$

$\Delta Q_{BUS\,3} = 0.03MVAR$

$\Delta Q_{BUS\,4} = 0.02MVAR$

Table 4.8 Case 2.2: 1% increase in reactive power Q on Bus 2, 3 and 4

Bus	**|ΔV| (in pu)**
1	0
2	0.00038
3	0.000319
4	0.000113
5	0.000185
6	0.000302
7	0.000323
8	0.00033
9	0.000193

As seen in Table 4.7 and 4.8, the voltage on each bus has changed. Even though the changes are not significant, as explained earlier, the value could increase as the number of generators which are going through the change at the same time also increases. The value |ΔV| could also increase when the magnitude of change in Q is larger.

4.2 Proposed Method

To prevent the watermarking signals from affecting the grid, the fluctuations should get cancelled in the grid. But it should happen after the detection of the watermarking. To eliminate grid power fluctuations, we can choose another plant and generate the watermarking signal in a particular manner so that the effects of watermarking on the two plant outputs cancel each other on the overall grid. But they are still detectable at each of their own points of measurement as shown in Fig 4.3.

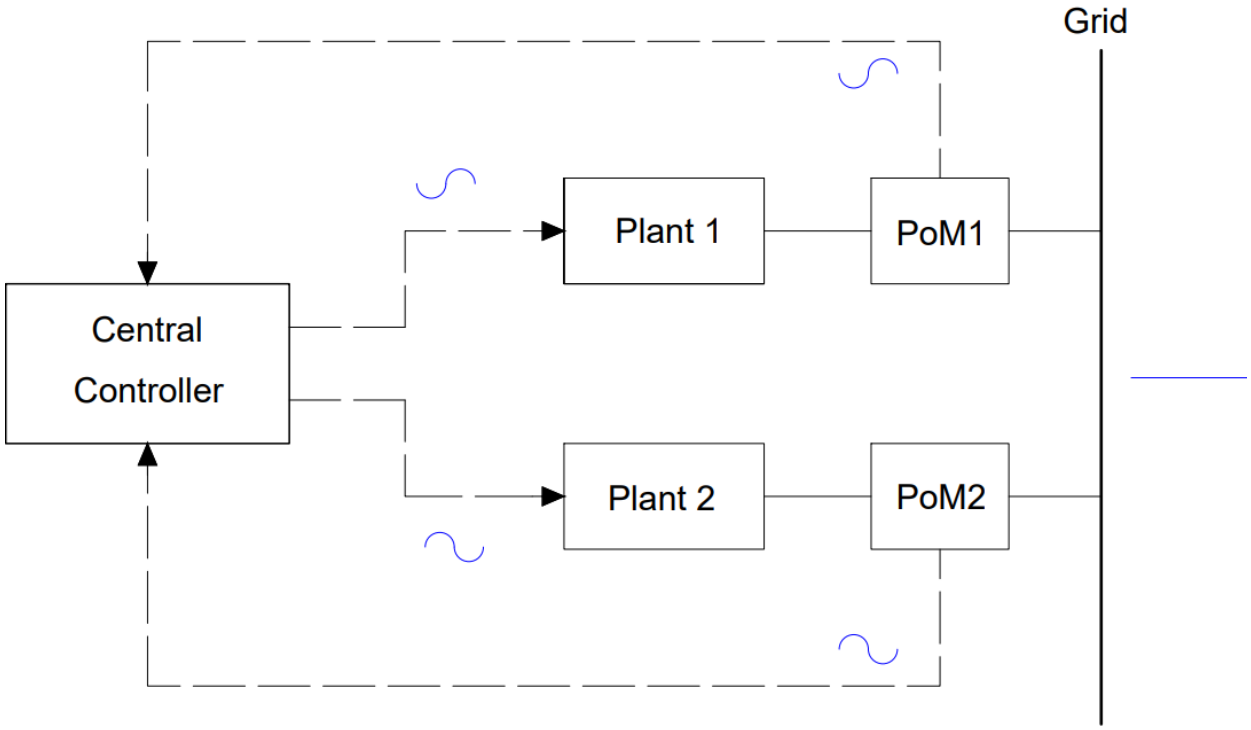

Figure 4.3 Two Plants cancelling each other's watermarking effects on the grid (in blue)

For cancelling each other's watermarking effects on the grid, these inverter-based plants should have enough power capacity to generate watermarking signals and should be located near to each other. For transmission lines, impedance is directly proportional to the distance. Hence, if the plants are far away from each other, due to higher impedance in between two plants, they will

not be able to cancel the changes effectively. This can be understood from the same modified IEEE 9 bus system (Fig. 4.2). In case 1.1, we increased active power by 1% (1.62MW) on bus 2. This time, we decrease the same amount of power in bus 3 and then 4.

Case 1.3 (1.62MW increase on Bus 2 and identical decrease on Bus 3):

$\Delta P_{BUS\,2} = 1.62MW$

$\Delta P_{BUS\,3} = -1.62MW$

$\Delta P_{BUS\,4} = 0MW$

Table 4.9 Case 1.3: 1.62MW increase on Bus 2 and identical decrease on Bus 3

Bus	**$\|\Delta\delta\|$ (in rad)**
1	0
2	0.002025
3	0.00203
4	0
5	0.00038
6	0.00108
7	0.000142
8	0.001012
9	0.000349

Total Impedance between bus 2 and 3 $Z_{Bus:2-3}$: 0.2951 (pu)

Case 1.4 (1.62MW increase on Bus 2 and identical decrease on Bus 4):

$\Delta P_{BUS\,2} = 1.62MW$

$\Delta P_{BUS\,3} = 0MW$

$\Delta P_{BUS\,4} = -1.62MW$

Table 4.10 Case 1.4: 1.62MW increase on Bus 2 and identical decrease on Bus 4

Bus	**$\|\Delta\delta\|$ (in rad)**
1	0
2	0.003539
3	0.001514
4	0
5	0.000531
6	0.001514
7	0.002103
8	0.002526
9	0.000874

Total Impedance between bus 2 and 4 $Z_{Bus:2-4}$: 0.3122 (pu)

Table 4.11 Comparisons of all cases (Case 1) for change in phase angle $|\Delta\delta|$ due to change in active power

Bus	Case 1.1 (1% Increase in Bus 2):	Case 1.2 (1% Increase in All Buses):	Case 1.3 (1.62MW increase in Bus 2 and identical decrease in Bus 3; $Z_{Bus:2-3}$: 0.2951 (pu)):	Case 1.4 (1.62MW increase in Bus 2 and identical decrease in Bus 4; $Z_{Bus:2-4}$: 0.3122 (pu)):
1	0	0	0	0
2	0.004472	0.005871	**0.002025**	**0.003539**
3	0.002447	0.004909	0.00203	0.001514
4	0.000933	0.001538	0	0
5	0.001465	0.002546	**0.00038**	**0.000531**
6	0.002447	0.004411	**0.00108**	**0.001514**
7	0.003037	0.004671	**0.000142**	**0.002103**
8	0.003459	0.004859	**0.001012**	**0.002526**
9	0.001807	0.002688	**0.000349**	**0.000874**

In case 1.3, the change in the phase angle of almost all buses is much smaller than in any other cases.

Similarly in Case 2.1, we decrease reactive power of 0.08MVAR on bus 3 and then bus 4:

Case 2.3 (0.08MVAR increase on Bus 2 and identical decrease on Bus 3):

$\Delta Q_{BUS\,2} = 0.08MVAR$

$\Delta Q_{BUS\,3} = -0.08MVAR$

$\Delta Q_{BUS\,4} = 0MVAR$

Table 4.12 Case 2.3: 0.08MVAR increase on Bus 2 and the similar decrease on Bus 3

Bus	|ΔV| (in pu)
1	0
2	0.0001
3	0.0001
4	0
5	0
6	0
7	0
8	0
9	0

Case 2.4 (0.08MVAR increase on Bus 2 and identical decrease on Bus 4):

$\Delta Q_{BUS\,2} = 0.08MVAR$

$\Delta Q_{BUS\,3} = 0MVAR$

$\Delta Q_{BUS\,4} = -0.08MVAR$

Table 4.13 Case 2.4: 0.08MVAR increase on Bus 2 and the similar decrease on Bus 4

Bus	|ΔV| (in pu)
1	0
2	0.000219
3	0.000118
4	0
5	0
6	0.000118
7	0.00015
8	0.000169
9	0

Table 4.14 Comparisons of all cases (Case 2) for change in voltage $|\Delta V|$ due to change in reactive power

Bus	**Case 2.1** **(1% Increase in Bus 2):**	**Case 2.2** **(1% Increase in All Buses):**	**Case 2.3** **(0.08MVAR increase in Bus 2 and identical decrease in Bus 3; $Z_{Bus:2-3}$: 0.2951 (pu)):**	**Case 1.4** **(0.08MVAR increase in Bus 2 and identical decrease in Bus 4; $Z_{Bus:2-4}$: 0.3122 (pu)):**
1	0	0	0	0
2	0.00029	0.00038	0.0001	0.000219
3	0.00019	0.00032	0.0001	0.000118
4	0.00007	0.00011	0	0
5	0.00012	0.00019	0	0
6	0.00019	0.0003	0	0.000118
7	0.00022	0.00032	0	0.00015
8	0.00024	0.00033	0	0.000169
9	0.00013	0.00019	0	0

Looking at Tables 4.11 and 4.14, we observer that case 1.3 and 2.3 have smaller changes because of the following two reasons:

1. Two generators are going through the same amount of change but in an opposite manner,
2. Both the generators are situated near to each other.

Hence, to decrease the power fluctuations on the grid due to watermarking, the central controller must send watermarking signals simultaneously to any two plants which has lower distance in between them (considering they have enough power capacities that they can generate for the short instant of the time for watermarking signal).

Consider Fig. 4.3. We would like the effects of watermarking on the "output" powers of the plants to cancel each other. Here we discuss how the "input" watermarking signals should be chosen. Inverter-based plants with PQ control are usually 3rd order system (as explained in previous chapter).

For plant 1, the watermarking signal (with $\alpha_1 = 0, \alpha_2 = \pi$) is

$$A_1 sin(\omega_1 t + \emptyset_1) + A_2 sin(\omega_2 t + \emptyset_2) \tag{4.5}$$

The output would be,

$$A_1|G_1(j\omega_1)|sin(\omega_1 t) + A_2|G_1(j\omega_2)|sin(\omega_2 t + \pi) \tag{4.6}$$

If for plant 2, the watermarking signal (with $\alpha_3 = 0, \alpha_4 = \pi$) is

$$-A_3 sin(\omega_1 t + \emptyset_3) - A_4 sin(\omega_2 t + \emptyset_4) \tag{4.7}$$

Then output will be,

$$-A_3|G_2(j\omega_1)|sin(\omega_1 t) - A_4|G_2(j\omega_2)|sin(\omega_2 t + \pi) \tag{4.8}$$

Phase angles $\emptyset_1, \emptyset_2, \emptyset_3$ & $\emptyset_4$ can be derived through the calculations explained in section 2.2. For effective cancellation of the effects of watermarking, the frequencies of both watermarking signals ω_1 & ω_2 should be the same.

Also, from (2.8), the restriction on A_1 and A_2 in G_1 and on A_3 and A_4 in G_2 are:

$$\frac{A_1|G_1(j\omega_1)|}{A_2|G_1(j\omega_2)|} = \frac{\omega_2}{\omega_1} = \frac{A_3|G_2(j\omega_1)|}{A_4|G_2(j\omega_2)|} \tag{4.9}$$

If we choose A_3 and A_4 such that,

$$A_1|G_1(j\omega_1)| = A_3|G_2(j\omega_1)| \tag{4.10}$$

then,

$$A_2|G_1(j\omega_2)| = A_4|G_2(j\omega_2)| \tag{4.11}$$

Hence, the outputs (4.6) and (4.8) will cancel each other.

The total delay of the plant ($\angle G(j\omega)$) is already considered during the derivation of the watermarking signal (section 2.2). But there might be a delay in the communication channels. For that, the delay compensation is necessary. The delay compensation t' can be represented as:

$$t' = t_{delay,1} - t_{delay,2} \tag{4.12}$$

where,

$t_{delay,i}$= total communication delay to i^{th} plant; $i = 1$ & 2.

In this case, (4.7) can be rewritten as,

$$-A_3 sin(\omega_1(t - t') + \emptyset_3) - A_4 sin(\omega_2(t - t') + \emptyset_4) \tag{4.13}$$

In the next section, a method for using this proposed solution is presented.

4.2.1 Algorithm for using a Proposed Solution

Figure 4.4 presents an algorithm for choosing a pair of suitable plants for the suggested solution. The following notations are used in Fig. 4.4.

$P(cap, i) = Total\ active\ power\ generation\ capacity\ of\ plant\ i\ (at\ present\ time)$

$P(det, i) = Minimum\ detectable\ amplitude\ of\ watermarking\ signal\ for\ plant\ i$

$Awm = total\ amplitude\ of\ the\ watermarking\ signal$

where,

$i = n, m$

Remark 14: This algorithm provides information on implementing the proposed watermarking strategy in the reference signal P, the same strategy is applicable for adding the watermarking in reference signal Q.

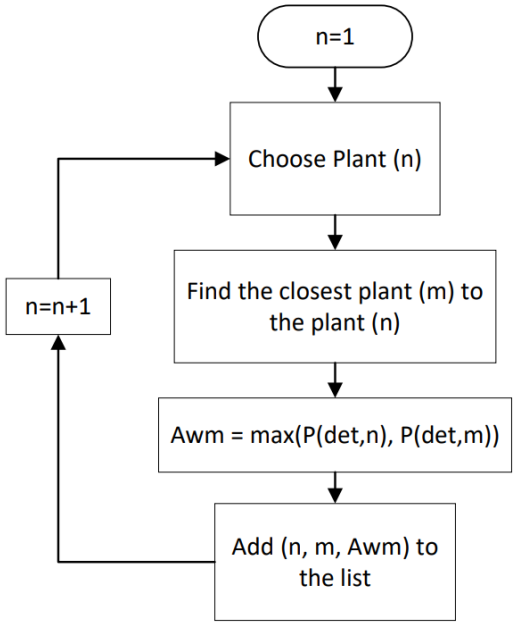

Figure 4.4 Flowchart for using a proposed method

The selection of pair of plants can be done offline before using the proposed method. The algorithm starts by choosing Plant n (where $n = 1$ at first) from total number of plants in the grid. Then, for the cancellation of effect of the watermarking signal in the grid, algorithm will pick the closest available plant (Plant m).

The next step would be to determine the amplitude of watermarking signal by checking $P(det)$ for both plants. The total amplitude of the watermarking signal will be equal to the maximum value of $P(det)$ between plants n and m.

After determining the pair of plants and total amplitude for them, the algorithm will save it to the list. Next, algorithm will choose another pair of plants and determine total amplitude for them.

This list can be used online to apply watermarking using the proposed method. After each frame, the watermarking can be switched to another pair.

Remark 15: Applying watermarking signals to two plants at the same time could help authenticate all the plants in the grid faster than applying watermark to one plant at a time. This could prevent attackers from getting sufficient time to record the data that is without the watermark.

Remark 16: For generating list offline, the CC can have the information about both $P(cap)$ *and* $P(det)$ *of each plant connected to the grid. That will make it easier for the CC to generate watermarking signals using the proposed method without facing any problems.*

In the next section, the simulation of two power plants connected to the grid is conducted using the proposed method.

4.2.2 Simulation of Two Plants using Proposed Method

Using Simulink, the two different grid connected plants are simulated (Fig. 4.5).

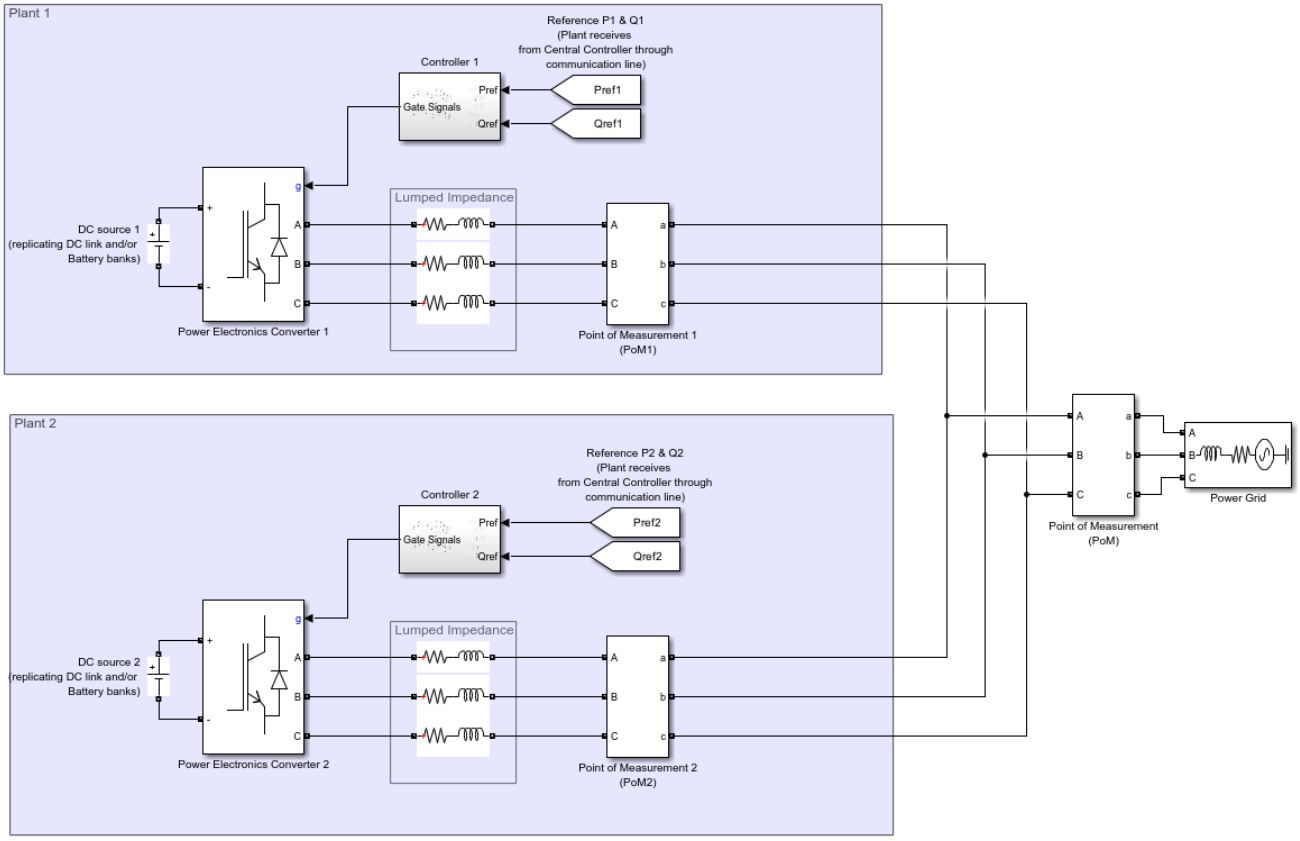

Figure 4.5 Simulation of two plants connected to the grid

To see the effectiveness of the proposed method, the simulation results are divided into two parts. In both parts, multi-sine watermarking is used, but in the first part, results are derived without using the proposed method and next the results using the proposed method are presented. Also, for both parts, watermarking is applied at the same time in both plants.

Grid's phase to phase, rms voltage $v_{ph-ph,rms}$: $400V$

Frequency f: $60Hz$

The parameters of plant 1 are the same as the plant that was used in Chapter 3. For plant 2,

$$R: 0.02\Omega \text{ and } L: 0.32mH$$

$$V_{DC} = 1000V$$

For the similar transient specifications explained in Chapter 3, for plant 2 the PI control gains will be,

P loop: $k_{pd1} = 0.003$, $k_{id1} = 0.04$; $k_{pd2} = 1$, $k_{id2} = 100$

Q loop; $k_{pq1} = -0.003$, $k_{iq1} = -0.04$; $k_{pq2} = 1$, $k_{iq2} = 100$

The reference set-points for both plants are:

$P_{ref,1} = 90kW$

$P_{ref,2} = 200kW$

$Q_{ref,1} = 15kVAR$

$Q_{ref,2} = 50kVAR$

Both the plants are 3rd order system. Furthermore, the watermarking frequencies are the same for both plants i.e.,

$\omega_{P1} = 0.6283\ rad/s$ $(f_1 = 0.1Hz)$,

$\omega_{P2} = 1.885\ rad/s$ $(f_2 = 0.3Hz)$ were used for P control loop and

$\omega_{Q1} = 0.942\ rad/s$ $(f_1 = 0.15Hz)$

$\omega_{Q2} = 2.826\ rad/s$ $(f_2 = 0.45Hz)$ were used for Q control loop.

Hence, for plant 2, the magnitude and phase angle,

$$\angle G_P(j\omega_{P1}) = 0.02\,rad \qquad \angle G_Q(j\omega_{Q1}) = 0.0487rad$$
$$\angle G_P(j\omega_{P2}) = 0.0645\,rad \qquad \angle G_Q(j\omega_{Q2}) = 0.14367rad$$
$$|G_P(j\omega_{P1})| = 1 \qquad |G_Q(j\omega_{Q1})| = 0.999$$
$$|G_P(j\omega_{P2})| = 0.945 \qquad |G_Q(j\omega_{Q2})| = 0.99$$

4.2.2.1 Simulation results ***without using the proposed method***

The amplitude of watermarking signals for both plants is 1% of their reference values. Using (2.8) and (2.9),

For plant 1:

watermarking signal for reference P =

$$675sin(0.6283t - 0.02512) + 226.7sin(1.885\,t + 3.06464)$$

watermarking signal for reference Q =

$$112.61sin(0.942\,t - 0.036116) + 37.88sin(2.826t + 3.02589\,)$$

For plant 2:

watermarking signal for reference P =

$$1500sin(0.6283t - 0.02) + 529.1sin(1.885t + 3.0755)$$

watermarking signal for reference Q =

$$375.38sin(0.942\,t - 0.0487) + 126.26sin(2.826t + 2.99633\,)$$

The other parameters such as T_{frame} remain the same which was used in chapter 3.

For both the plants, watermarking was applied in active power P between 6s to 16s.

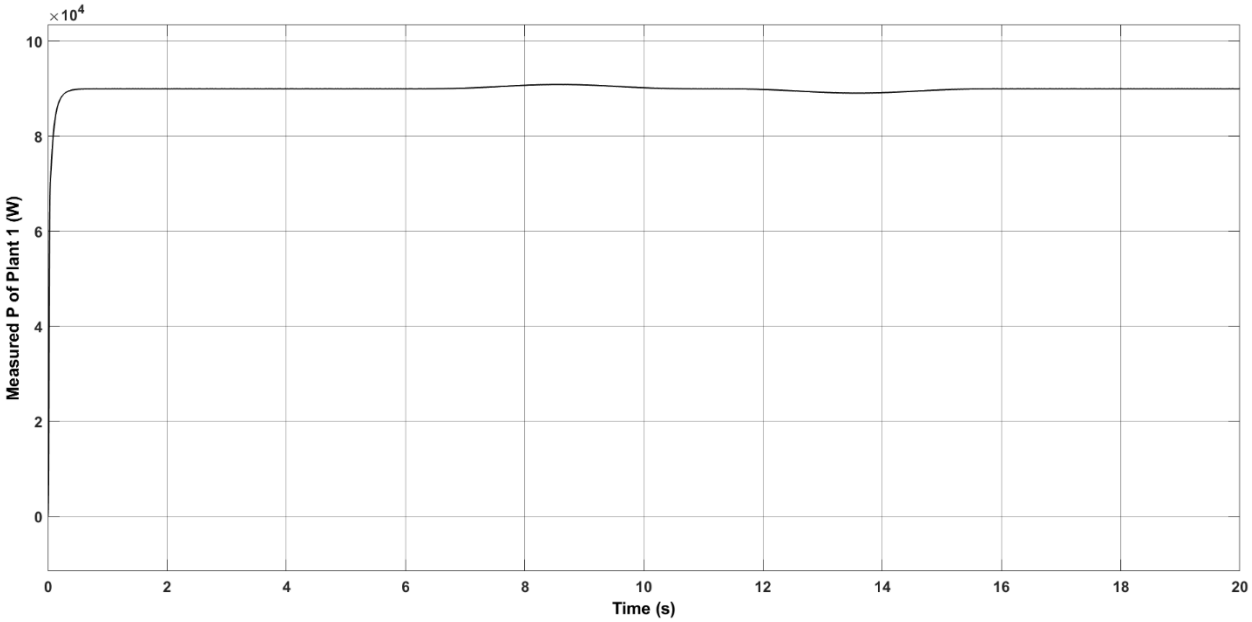

Figure 4.6 Measured active power P for plant 1

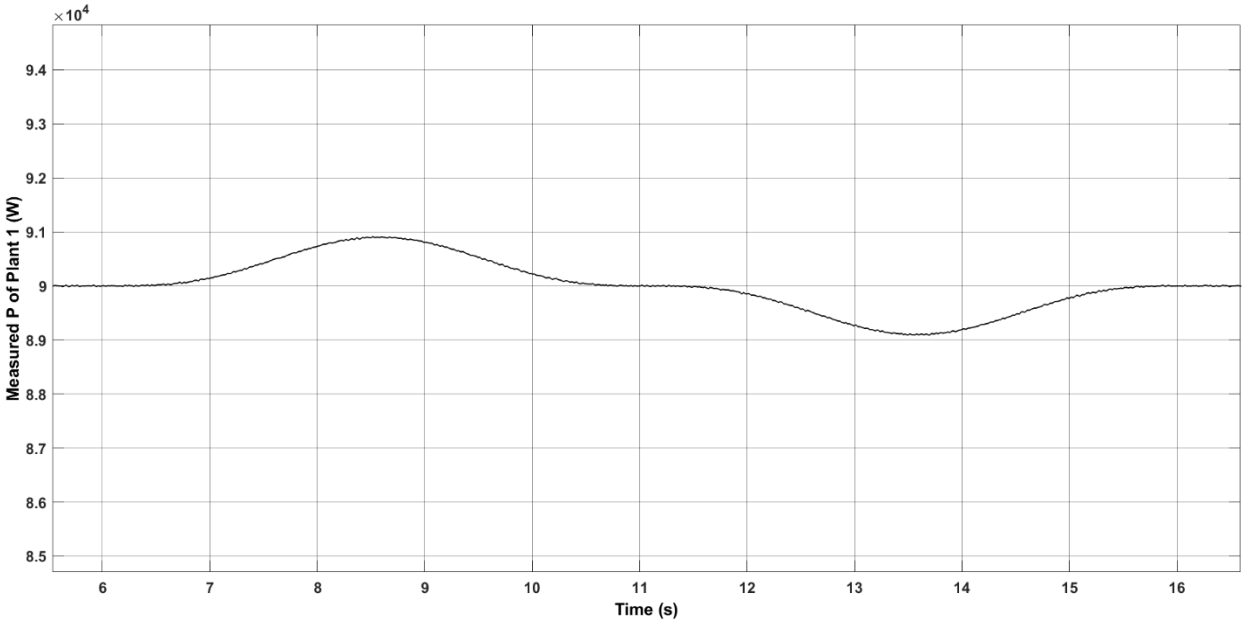

Figure 4.7 Measured active power P for plant 1(zoomed in)

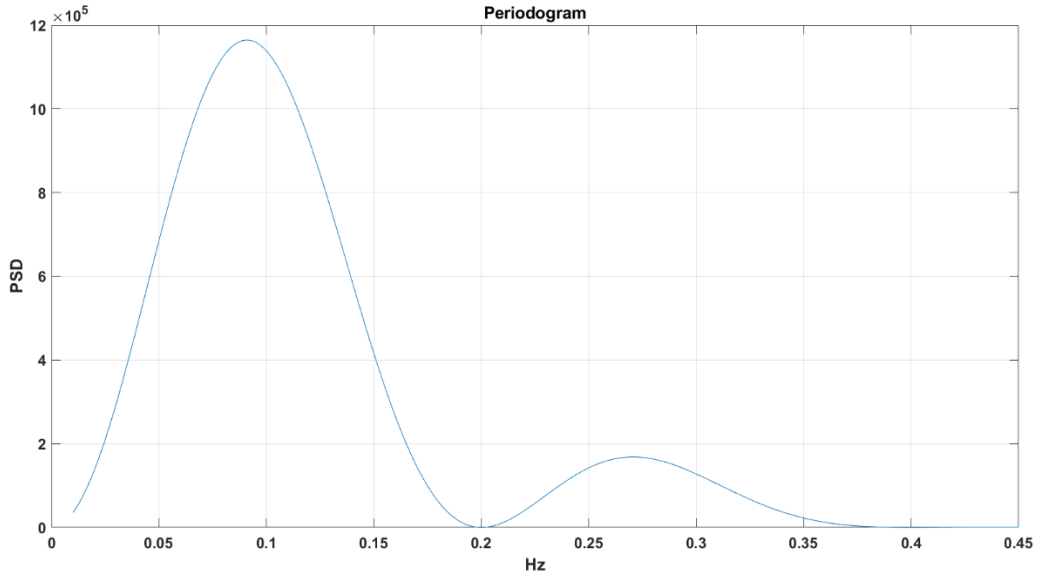

Figure 4.8 PSD estimation using Periodogram for the signal P of plant 1

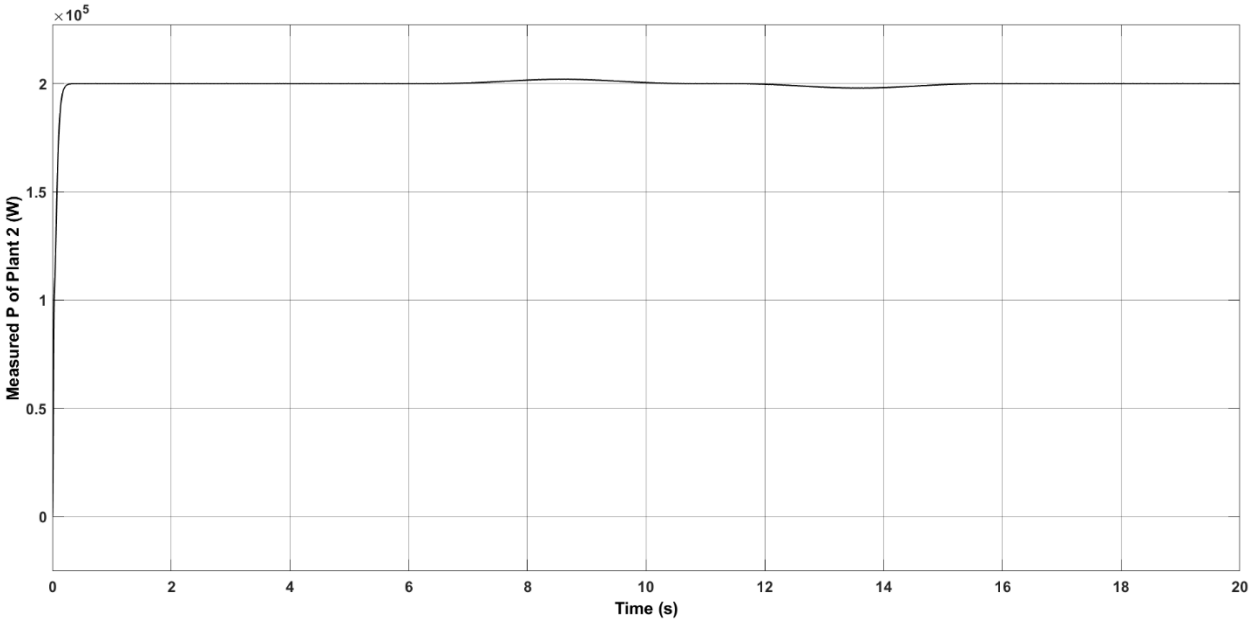

Figure 4.9 Measured active power P for plant 2

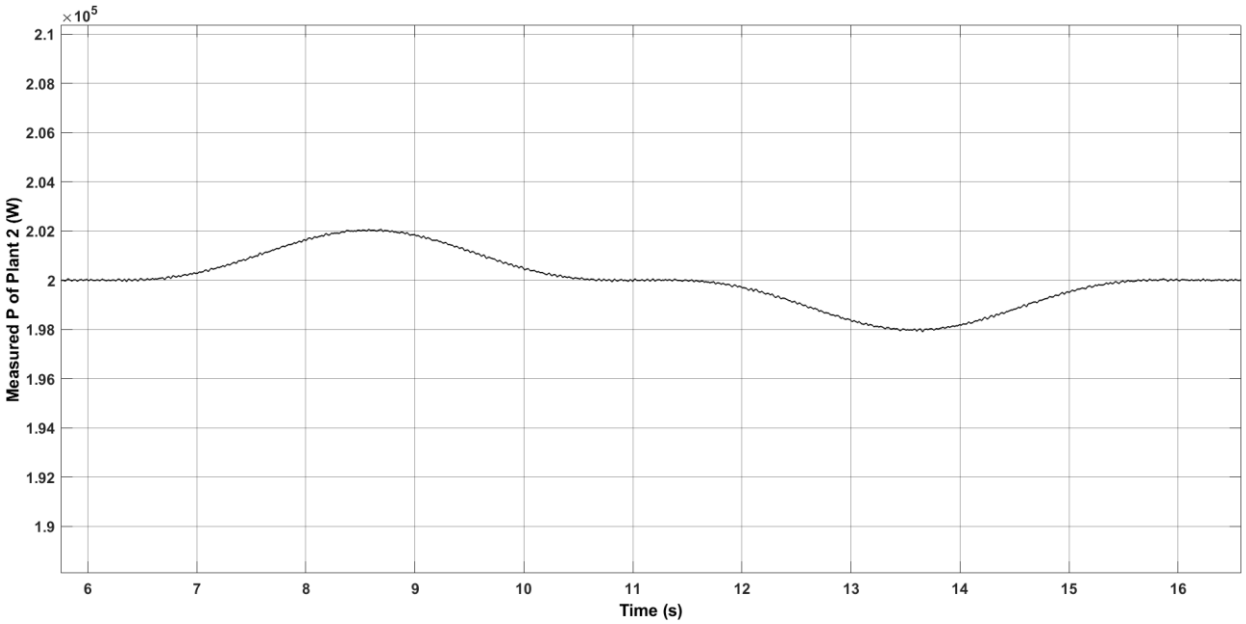

Figure 4.10 Measured active power P for plant 2(zoomed in)

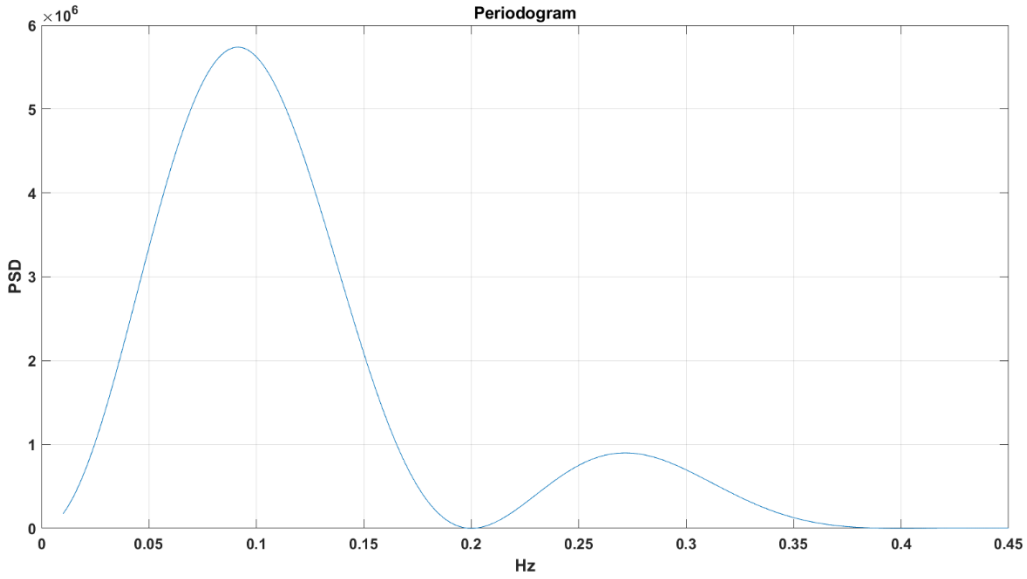

Figure 4.11 PSD estimation using Periodogram for the signal P of plant 2

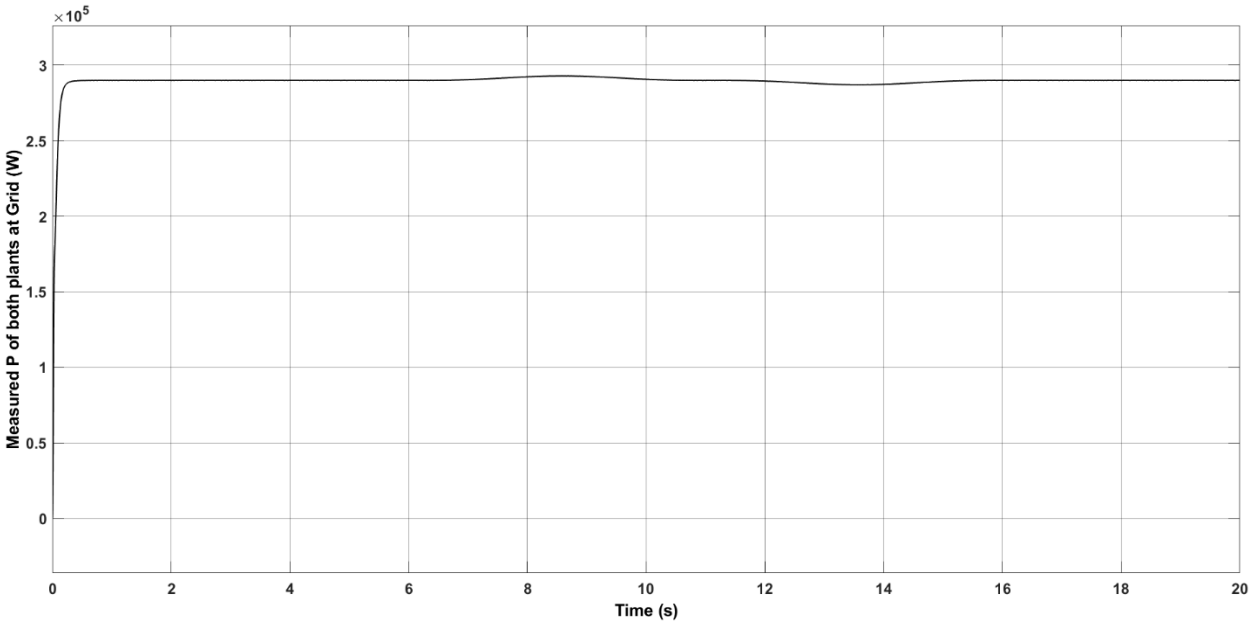

Figure 4.12 Measured P of both the plants at grid (without using proposed method)

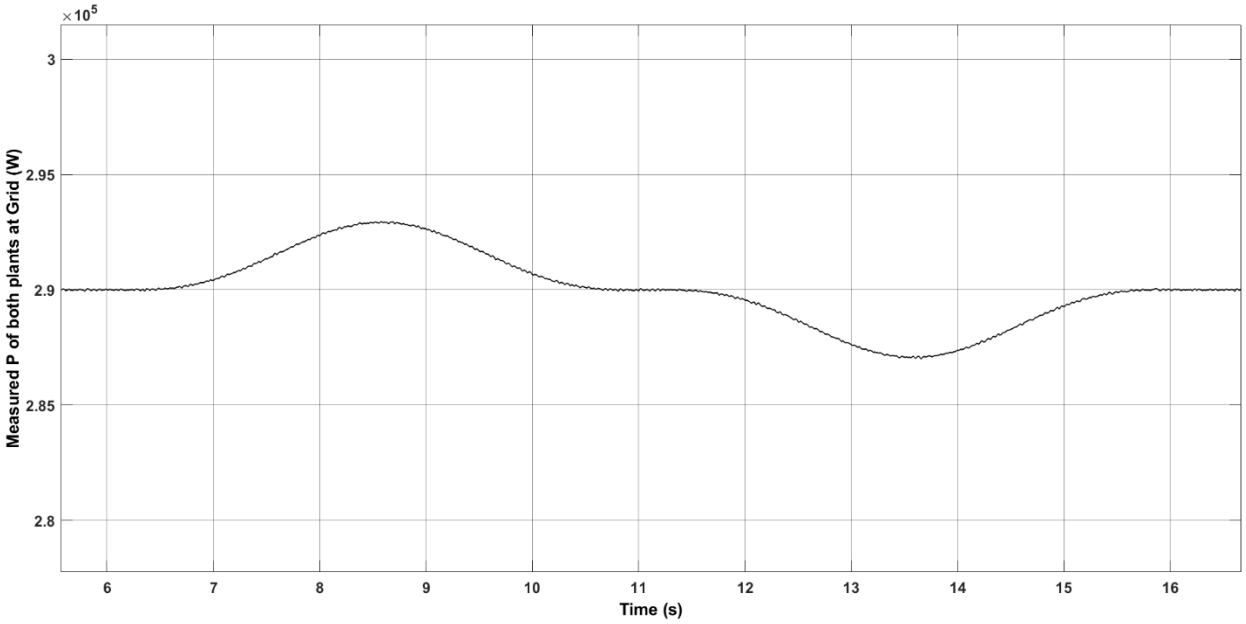

Figure 4.13 Measured P of both the plants at grid (without using proposed method; zoomed in)

According to PSD estimation using periodogram, for both plants (Fig. 4.8 and 4.11), the watermark in signal P can be successfully detected (0.1Hz & 0.3Hz), but the effects of watermarking signals got added and the added fluctuation can be seen in the grid as shown in Fig. 4.13.

In both plants, the watermarking in signal Q was applied between 10s and 16.67s (Fig. 4.14).

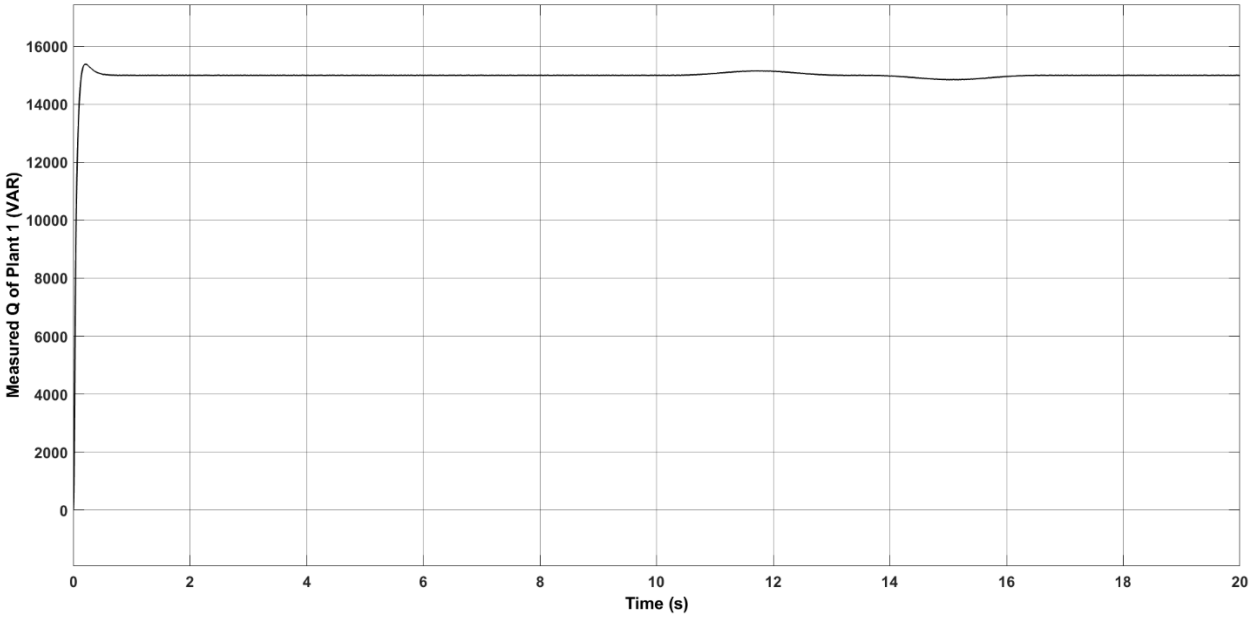

Figure 4.14 Measured reactive power Q for plant 1

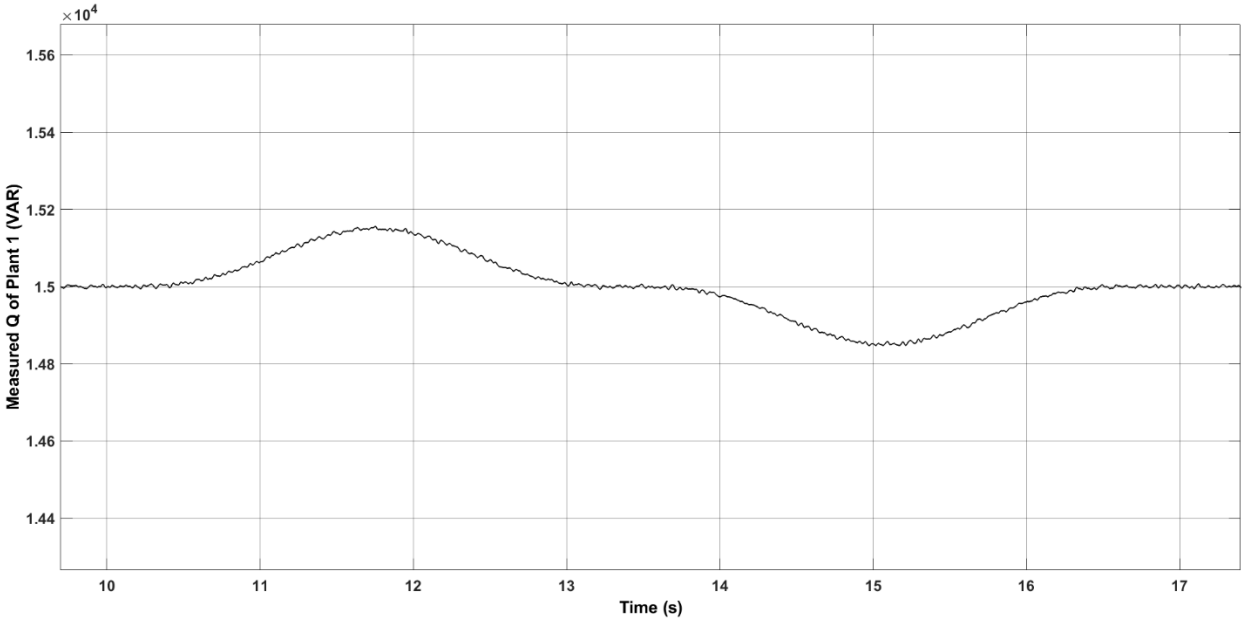

Figure 4.15 Measured reactive power Q for plant 1 (zoomed in)

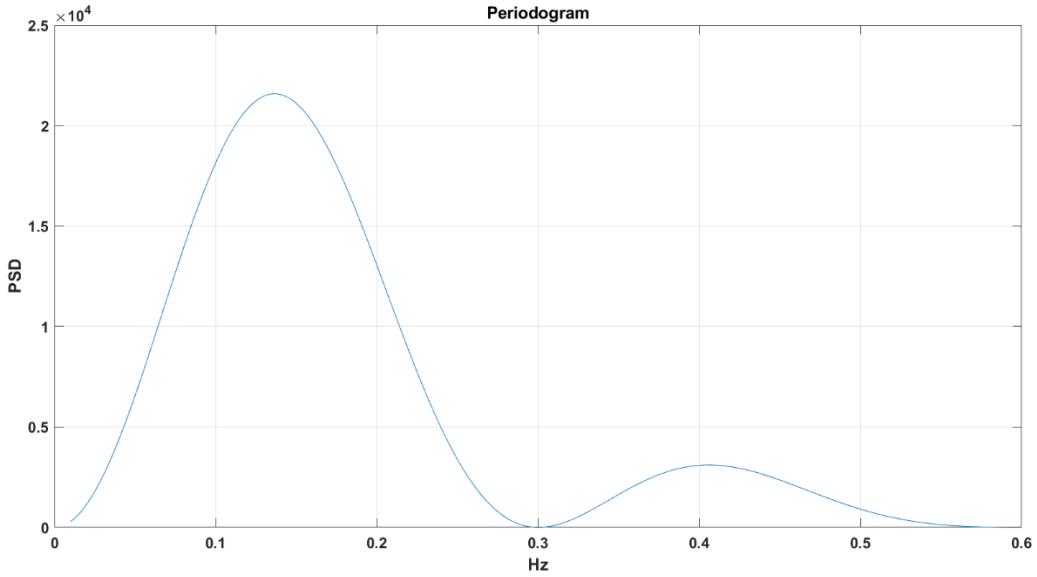

Figure 4.16 PSD estimation using Periodogram for the signal Q of plant 1

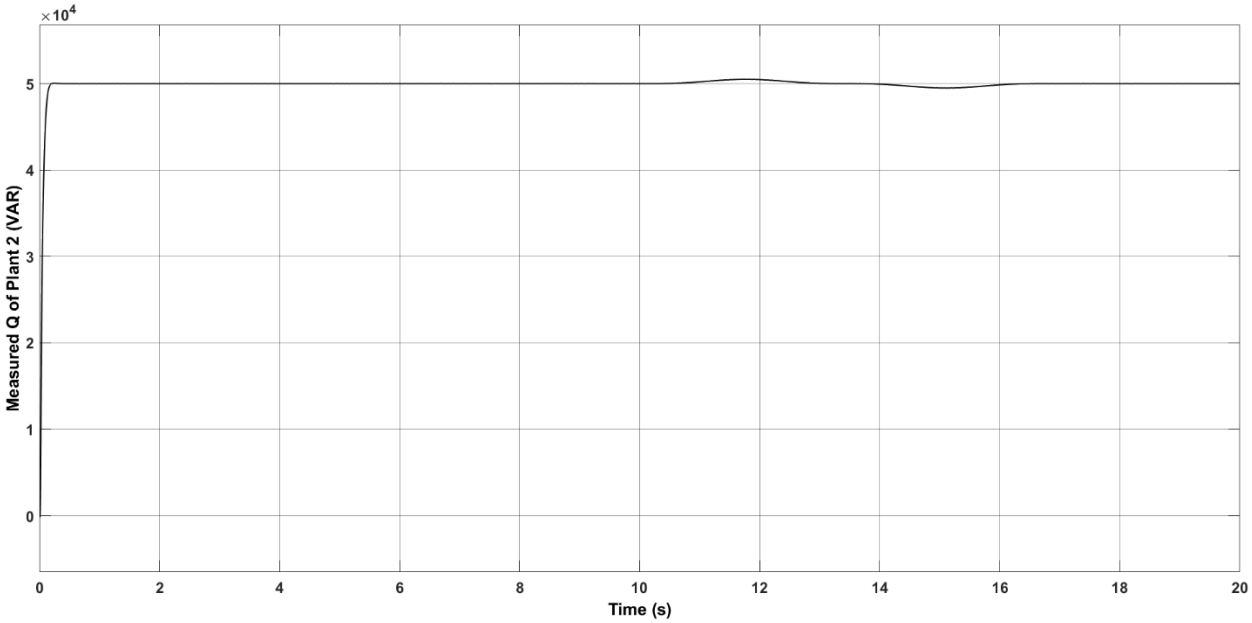

Figure 4.17 Measured reactive power Q for plant 2

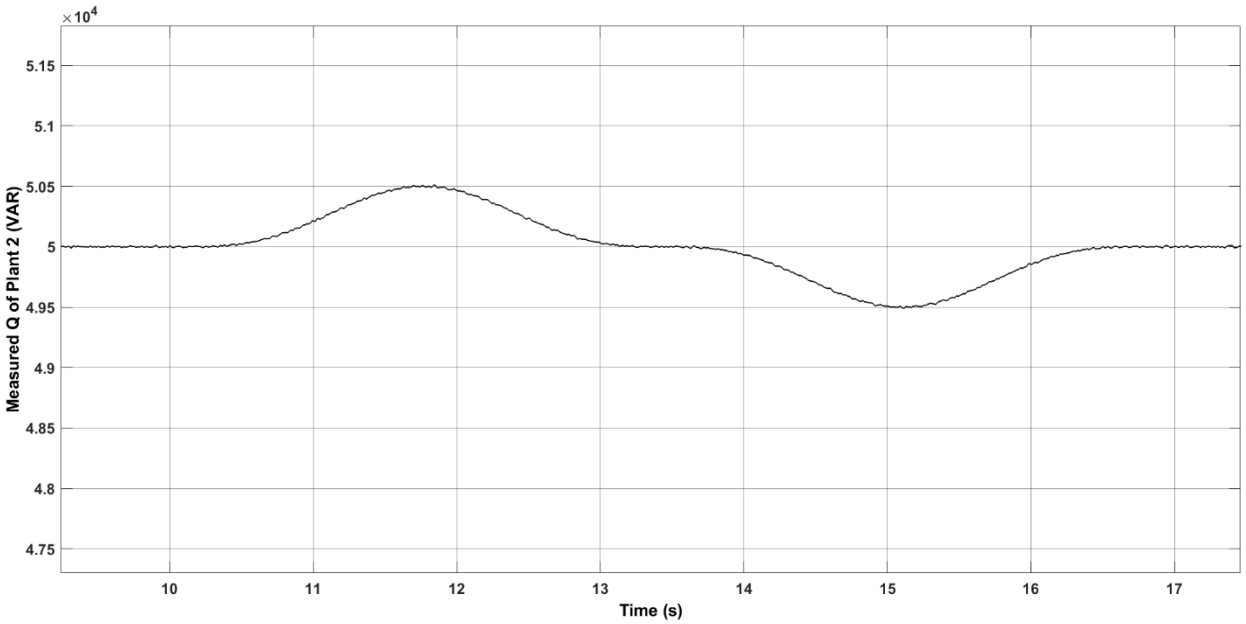

Figure 4.18 Measured reactive power Q for plant 2 (zoomed in)

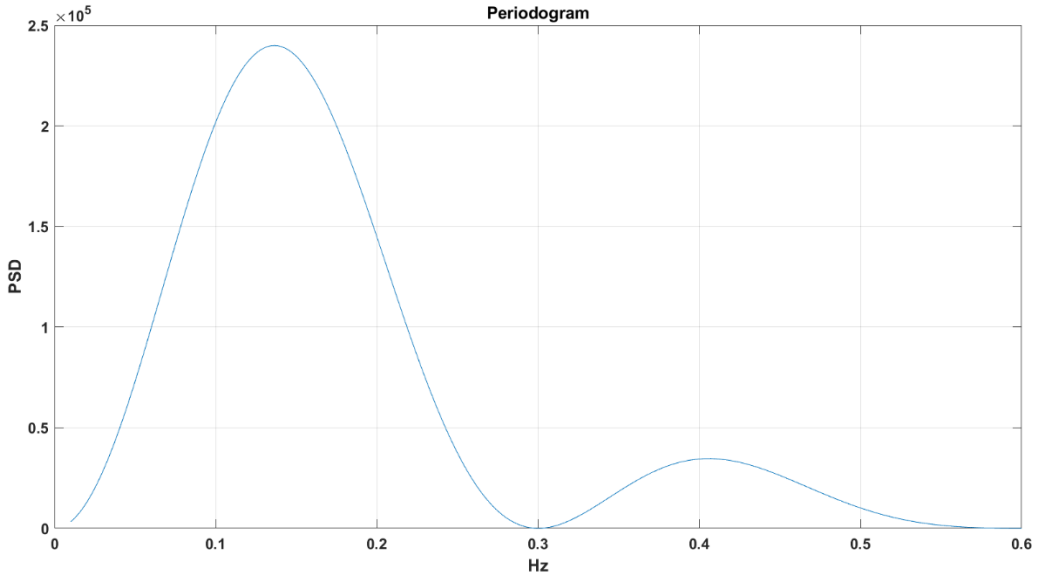

Figure 4.19 PSD estimation using Periodogram for the signal Q of plant 2

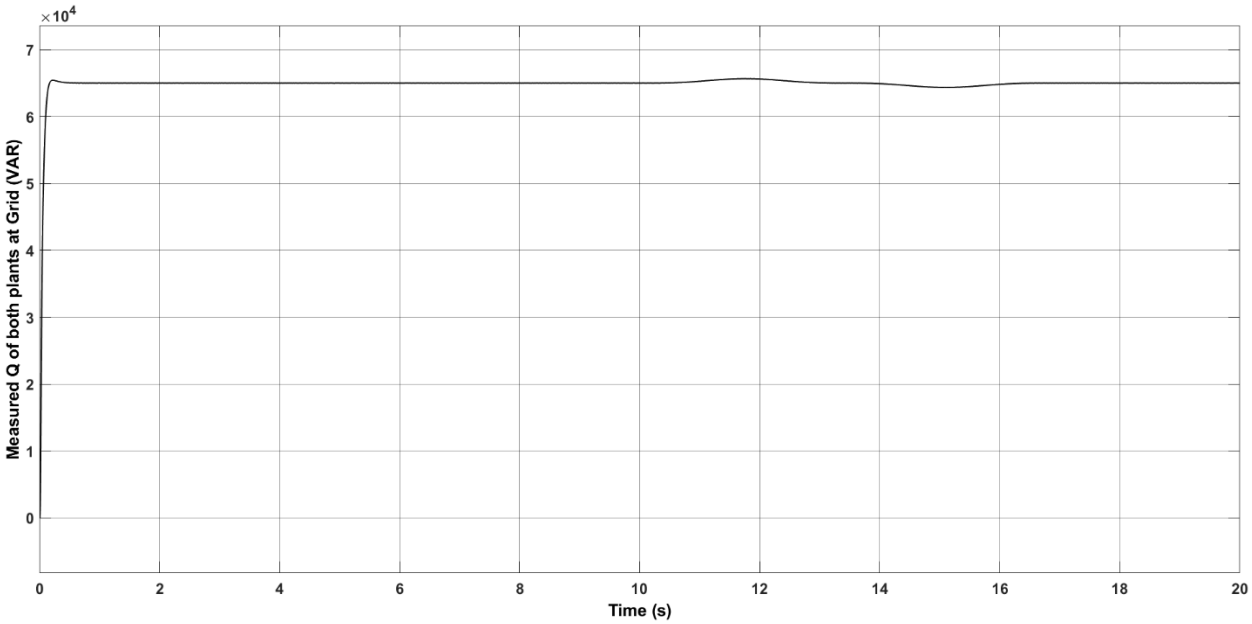

Figure 4.20 Measured Q of both the plants at grid (without using proposed method)

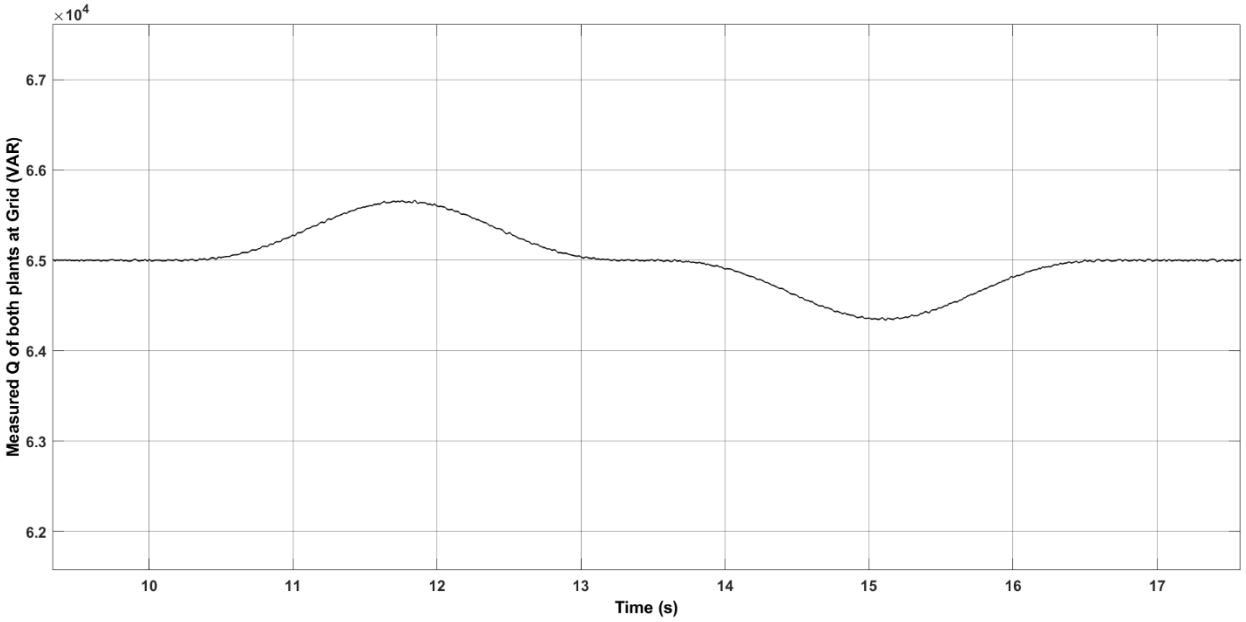

Figure 4.21 Measured Q of both the plants at grid (without using proposed method; zoomed in)

Similarly for both plants, watermarking in signal Q can be successfully estimated (0.15Hz and 0.45Hz) using periodogram but the fluctuations due to watermarking increases in the grid side as shown in Fig. 4.21. To decrease these unwanted fluctuations, the proposed method could be used.

4.2.2.2 Simulation results ***using proposed method****:*

As the reference signals P and Q of plant 2 are higher than plant 1, let us assume that $P(det)$ & $Q(det)$ of plant 2 (the lowest detectable watermarking amplitude of active and reactive power) will be higher too. So, in this case for both the plants, the total amplitude of the watermarking signals is taken 1% of Plant 2's reference values.

In our case, it is also considered that there is no time delay. Both plants are perfectly synchronized with the CC. Hence,

$$t' = 0s$$

Using (4.10) and (4.11),

For plant 1,

watermarking signal for reference P:

$$1500sin(0.6283t - 0.02512) + 503.78sin(1.885\ t + 3.06464)$$

watermarking signal for reference Q:

$$375.37sin(0.942\ t - 0.036116) + 126.27sin(2.826t + 3.02589\ )$$

For plant 2,

watermarking signal for reference P:

$$-1500sin(0.6283t - 0.02) - 529.1sin(1.885t + 3.0755)$$

watermarking signal for reference Q:

$$-375.38sin(0.942\ t - 0.0487) - 126.26sin(2.826t + 2.99633\ )$$

For both the plants, watermark was applied in active power P between 6s to 16s.

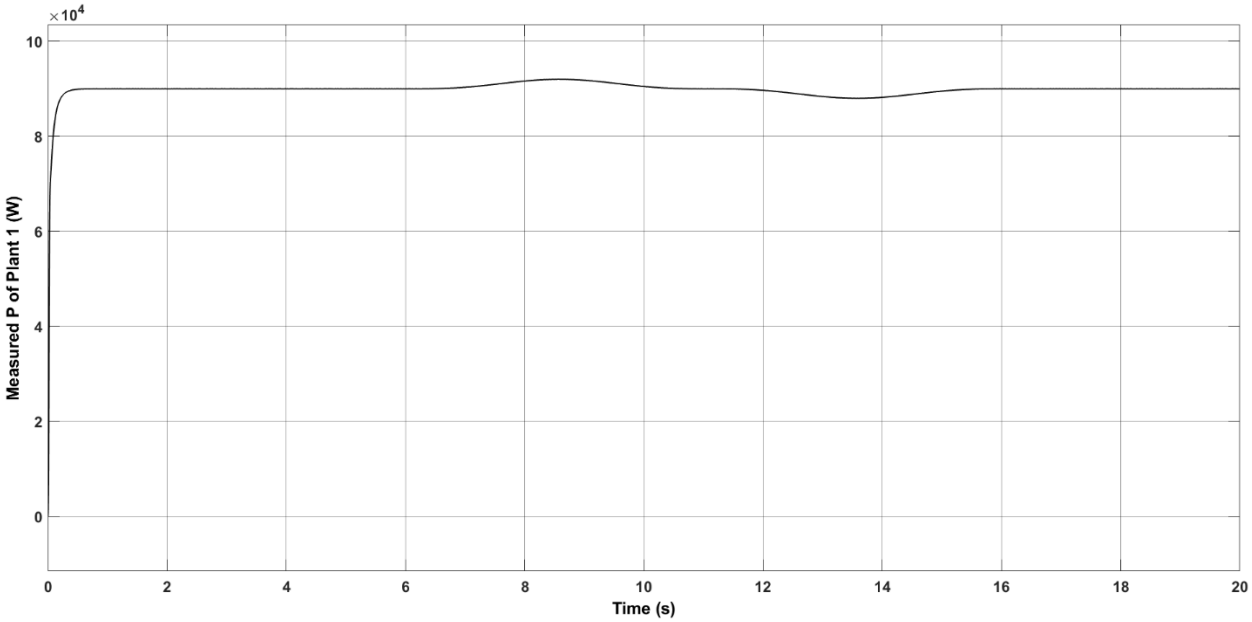

Figure 4.22 Measured active power P for plant 1

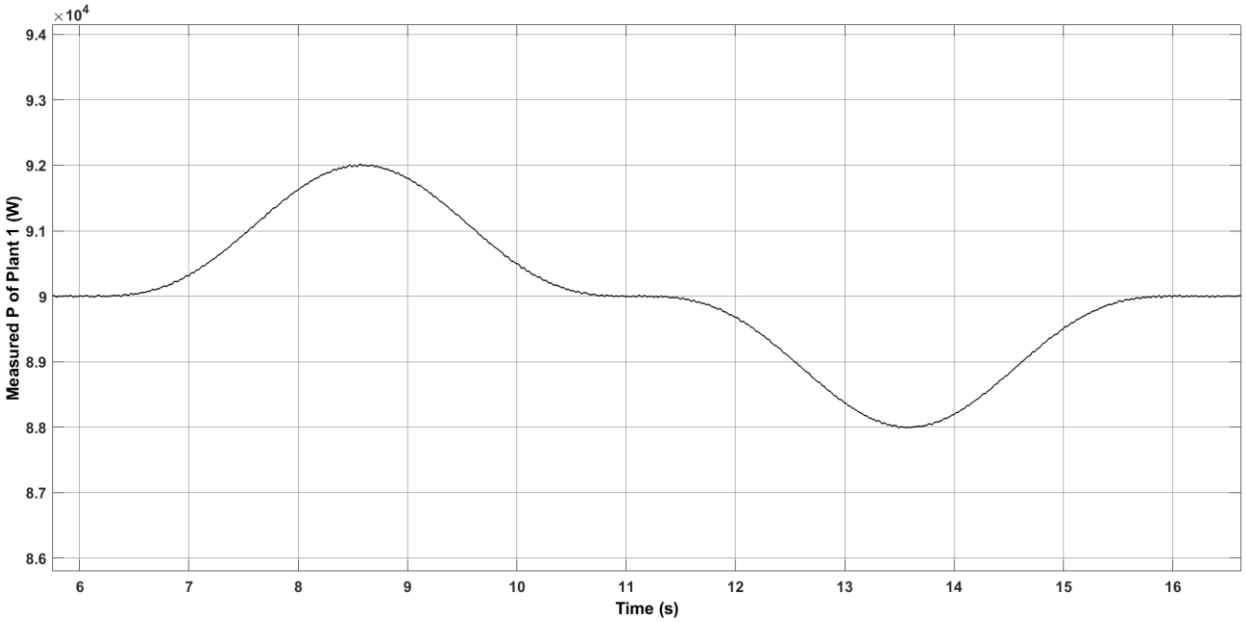

Figure 4.23 Measured active power P for plant 1 (zoomed in)

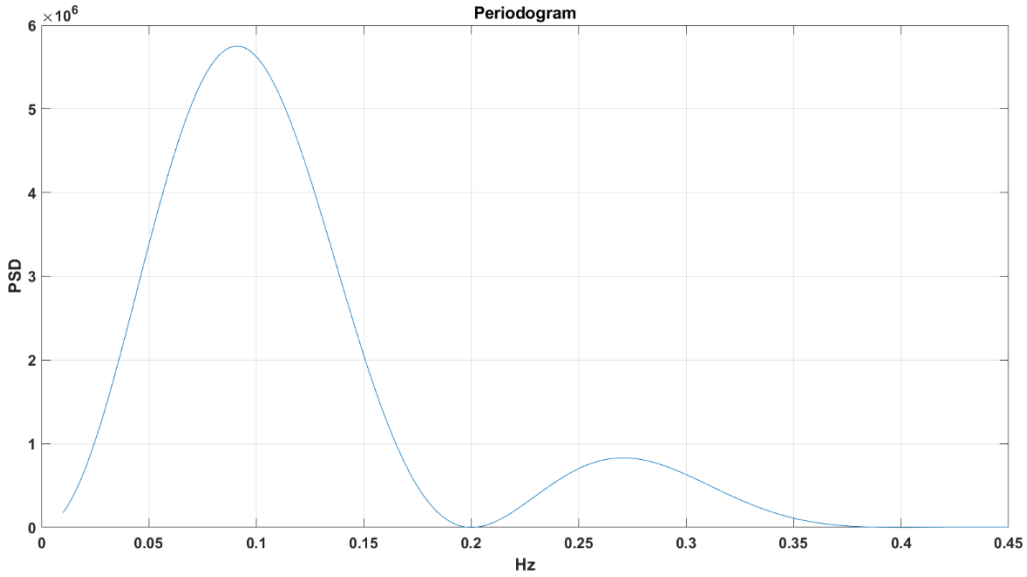

Figure 4.24 PSD estimation using Periodogram for the signal P of plant 1

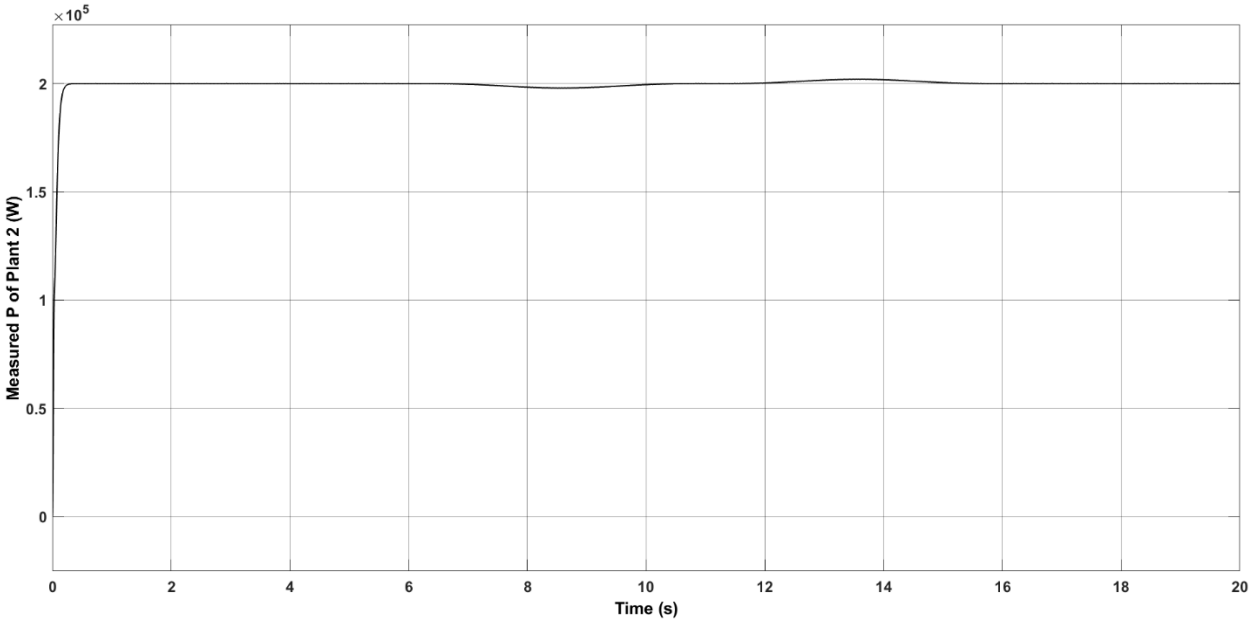

Figure 4.25 Measured active power P for plant 2

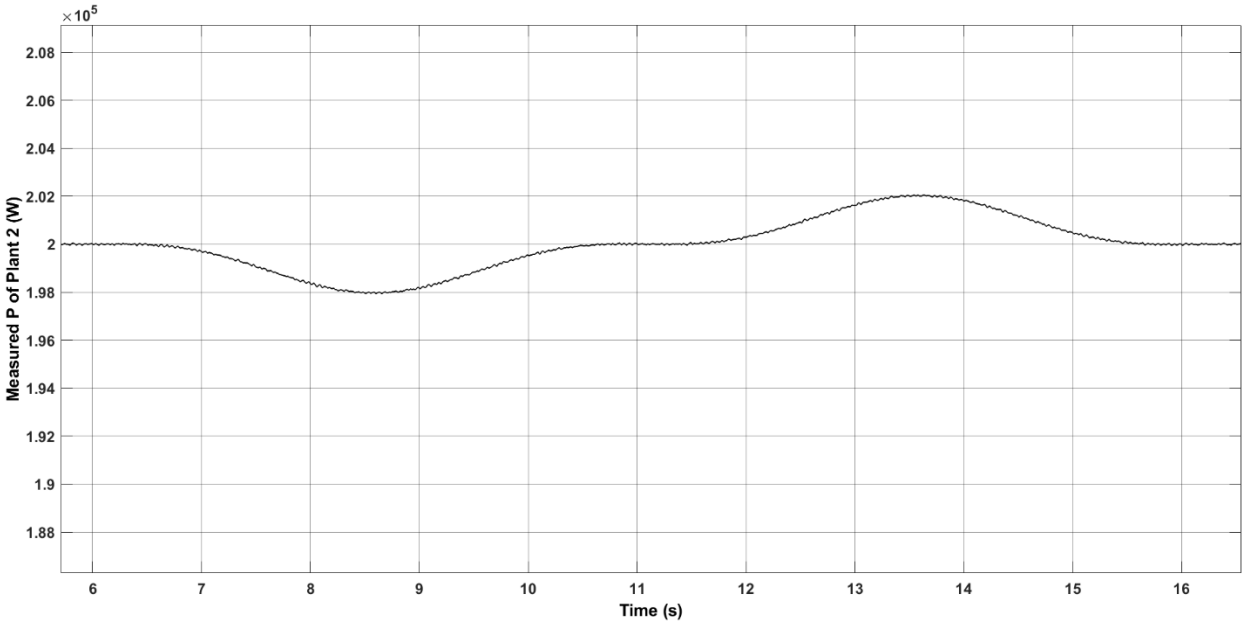

Figure 4.26 Measured active power P for plant 2 (zoomed in)

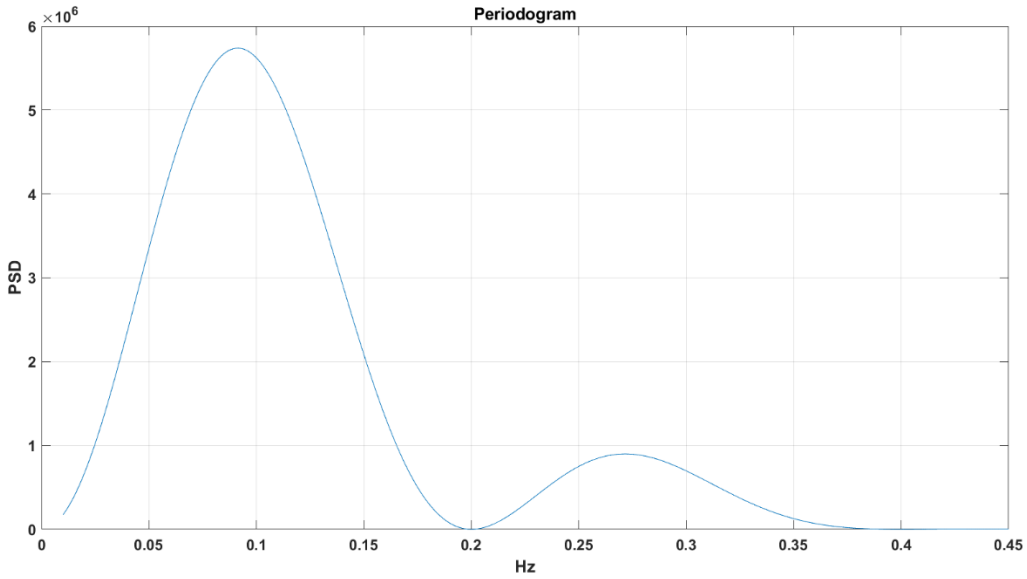

Figure 4.27 PSD estimation using Periodogram for the signal P of plant 2

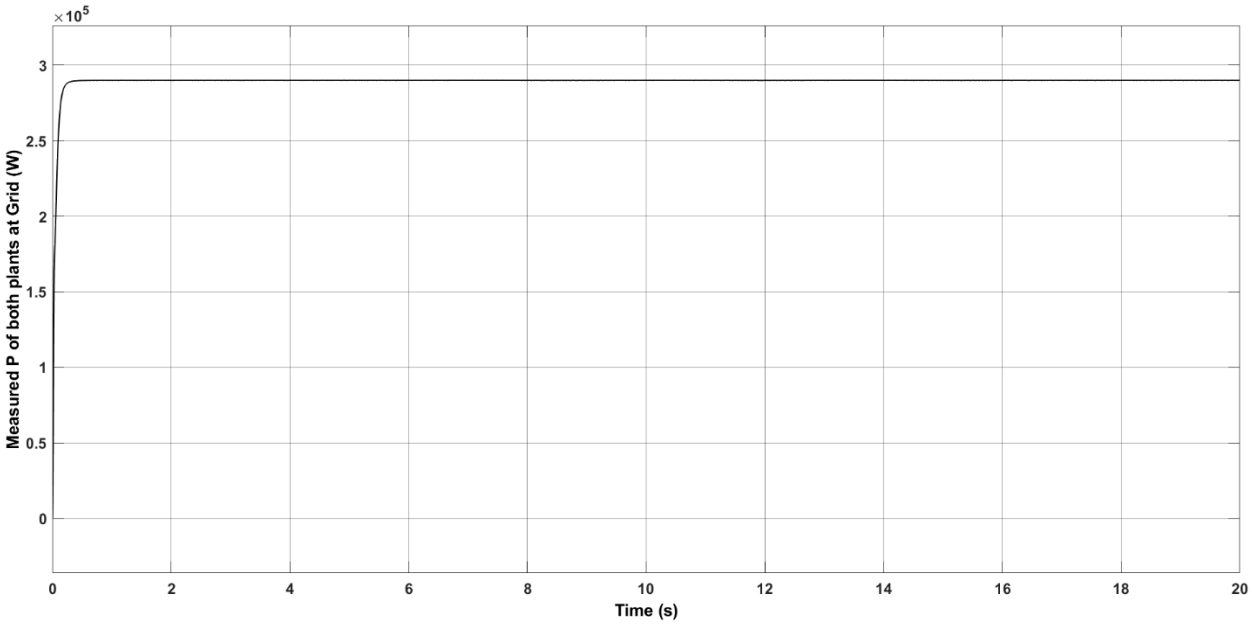

Figure 4.28 Measured P of both the plants at grid (using proposed method)

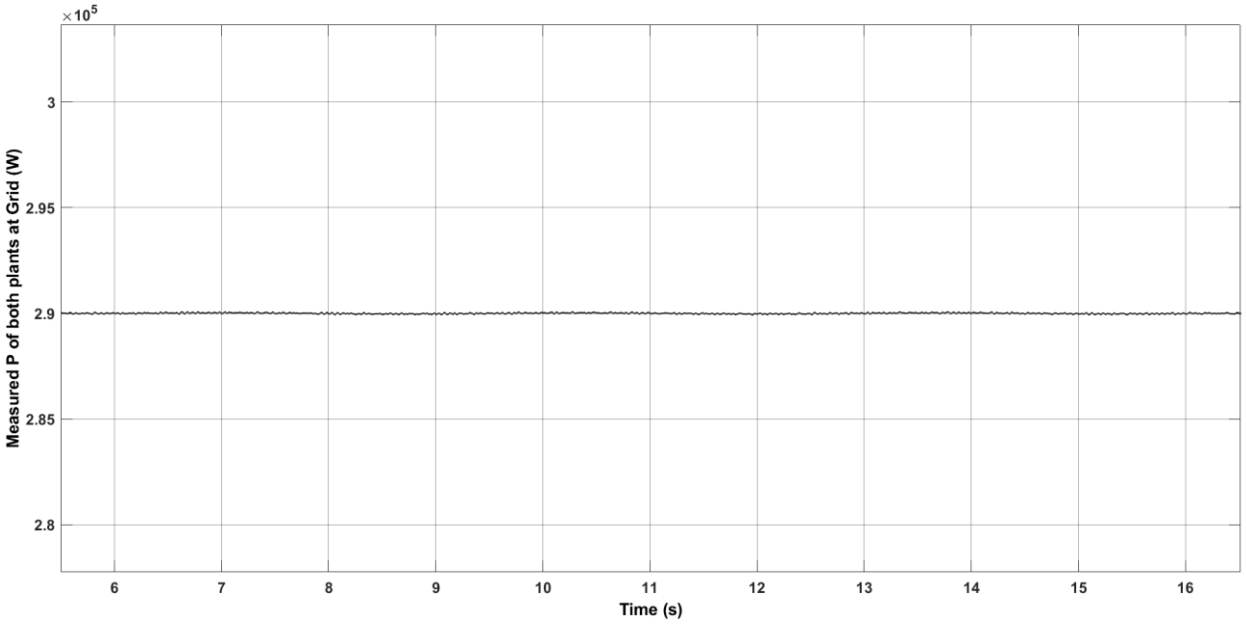

Figure 4.29 Measured P of both the plants at grid (using proposed method; zoomed in)

Hence, using the proposed method, for both plants, watermarking (in signal P) can be successfully detected (0.1Hz & 0.3Hz) at each of their own PoMs (as shown in fig. 4.24 and 4.27) and the fluctuations at the grid due to watermarking is almost zero as shown in fig. 4.29 (comparing to with Fig. 4.21).

Similarly for signal Q, the watermark was applied after 10s:

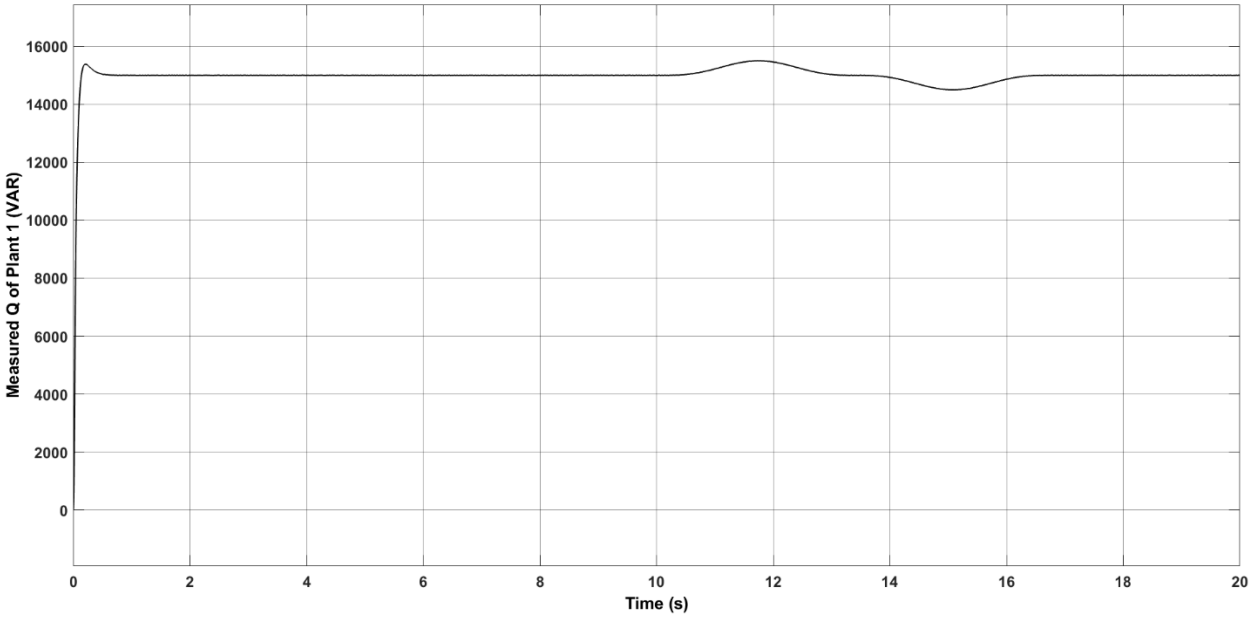

Figure 4.30 Measured reactive power Q for plant 1

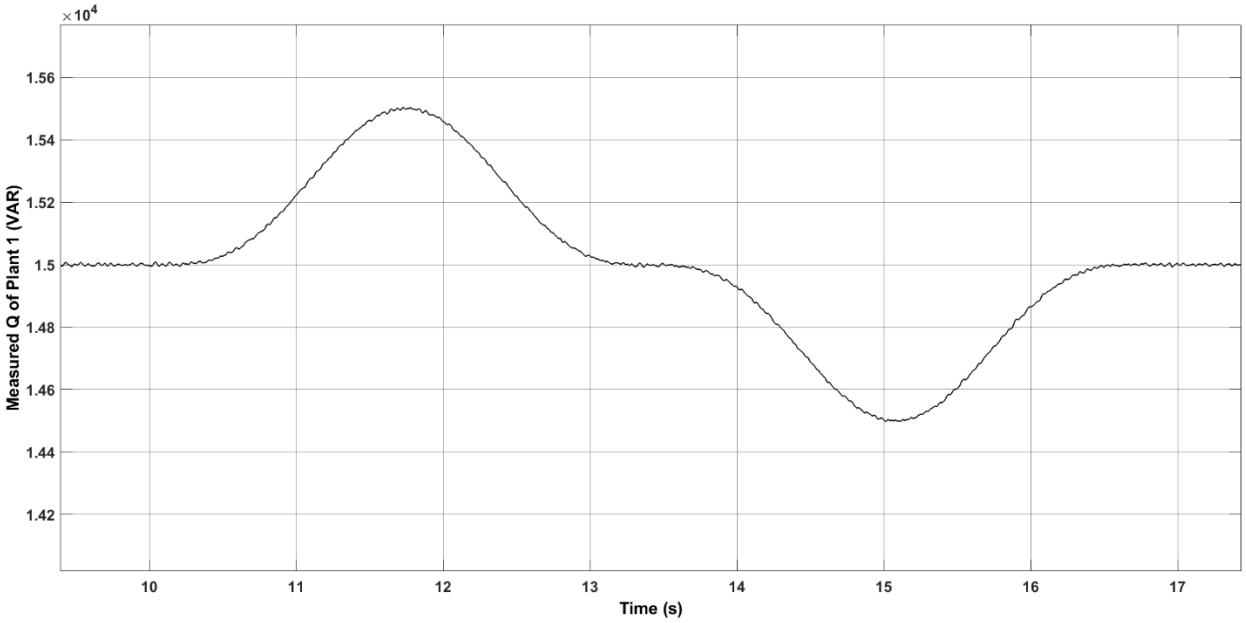

Figure 4.31 Measured reactive power Q for plant 1 (zoomed in)

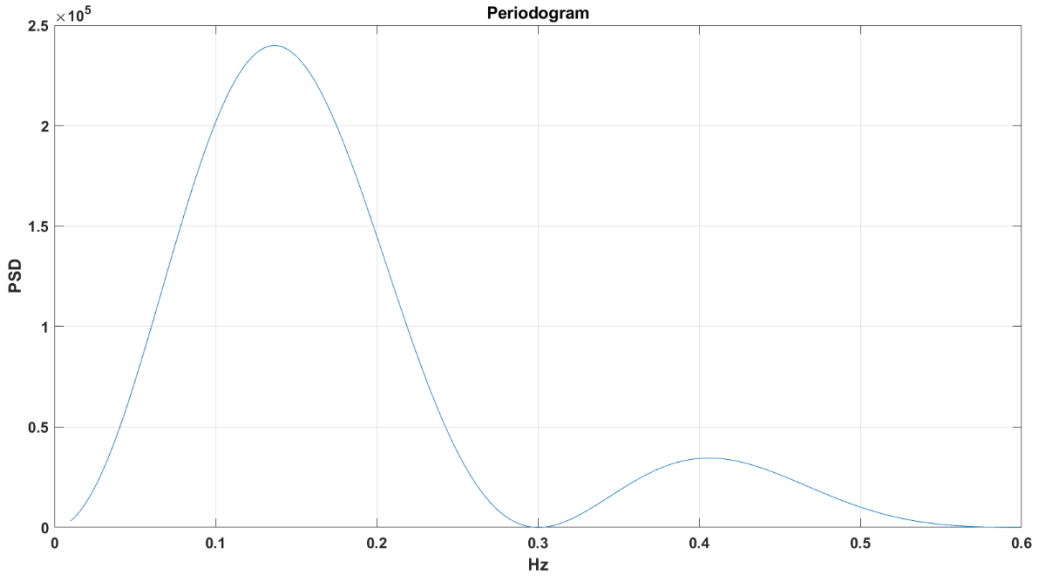

Figure 4.32 PSD estimation using Periodogram for the signal Q of plant 1

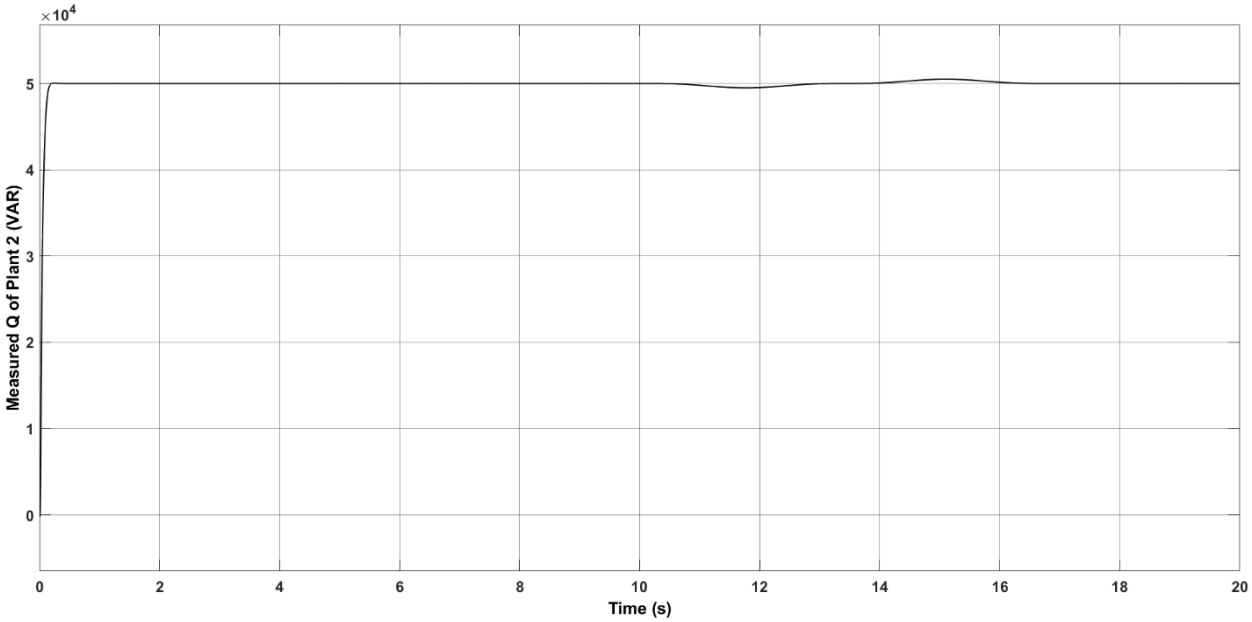

Figure 4.33 Measured reactive power Q for plant 2

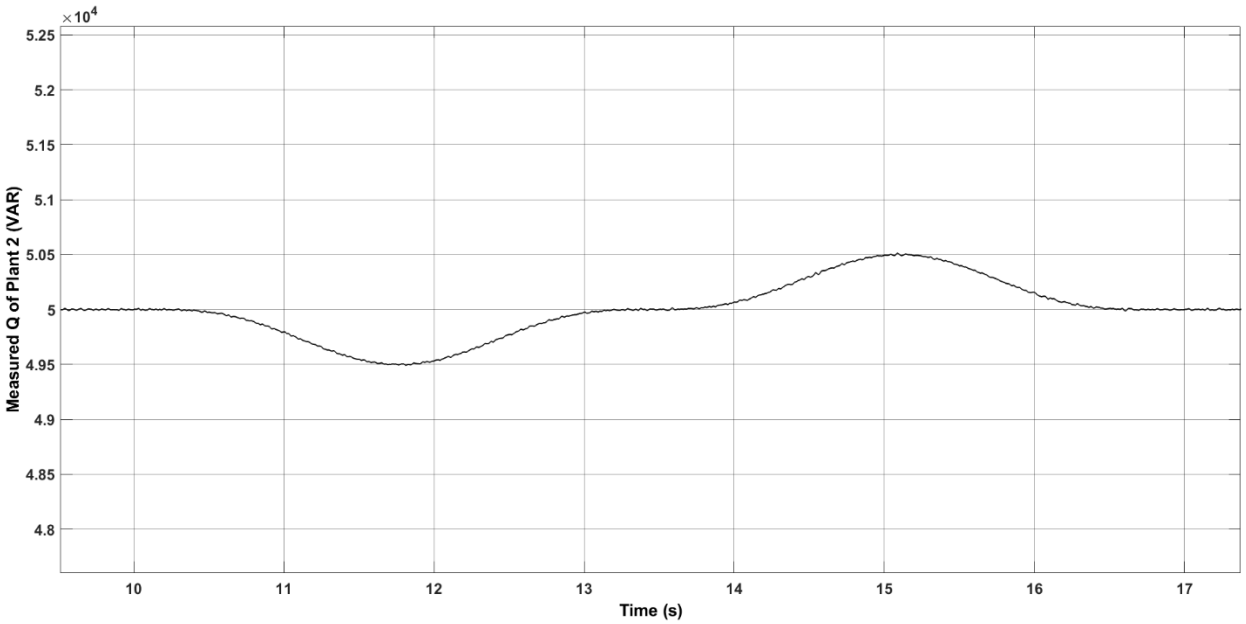

Figure 4.34 Measured reactive power Q for plant 2 (zoomed in)

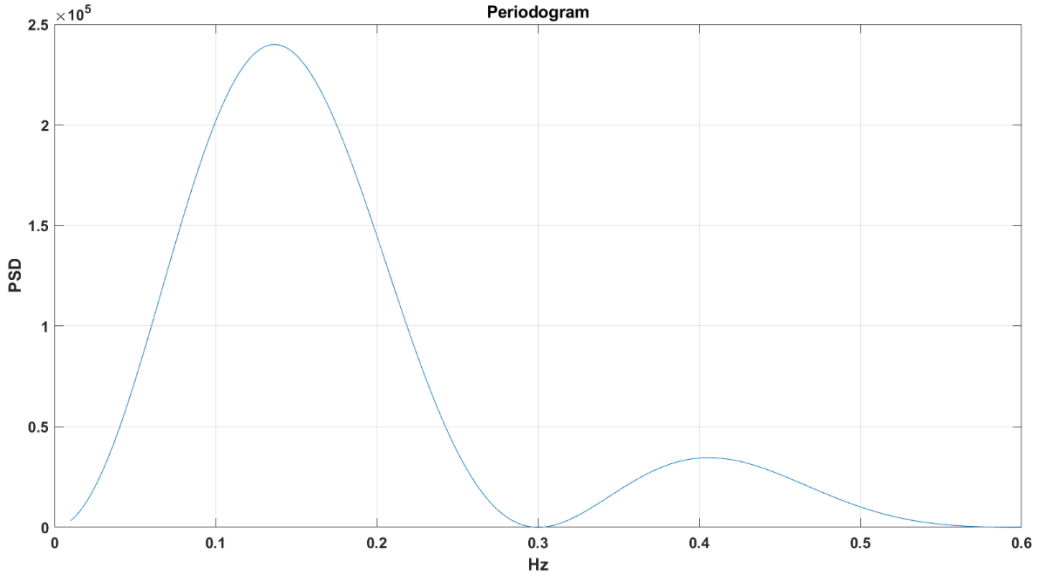

Figure 4.35 PSD estimation using Periodogram for the signal Q of plant 2

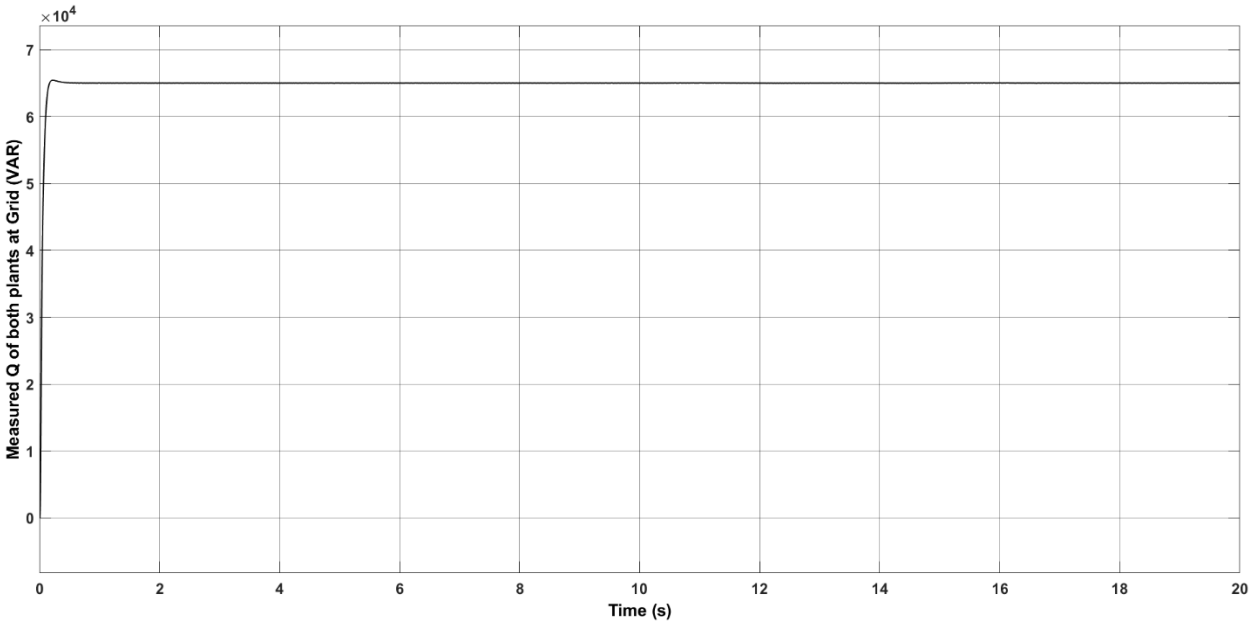

Figure 4.36 Measured Q of both the plants at grid using proposed method

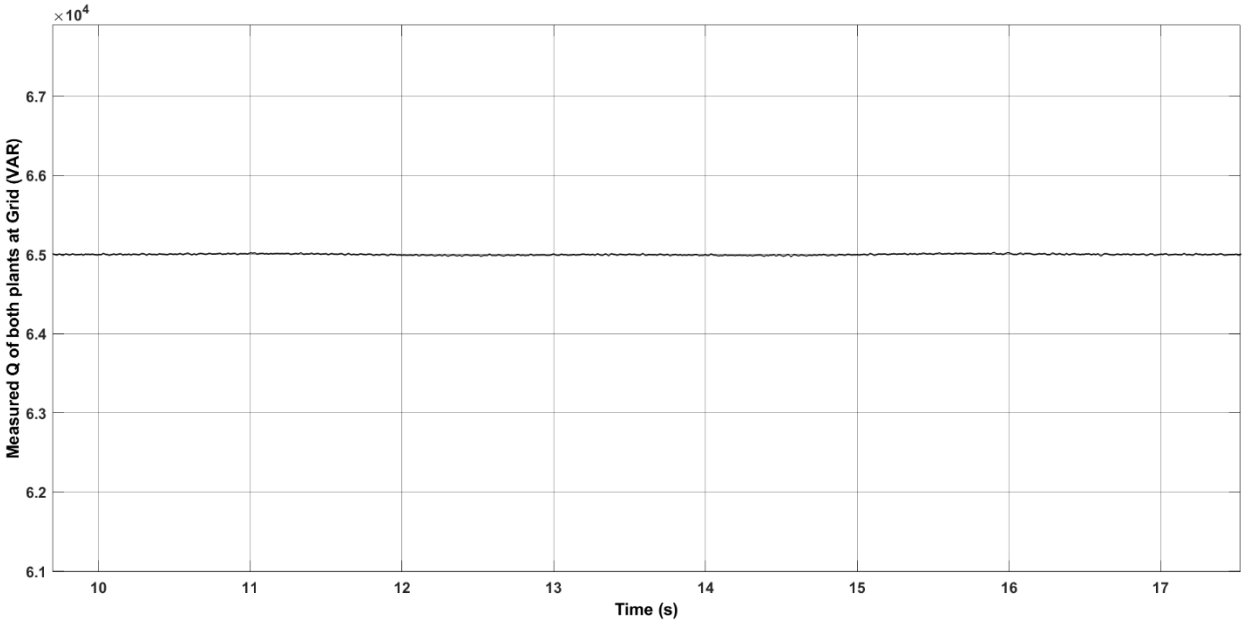

Figure 4.37 Measured Q of both the plants at grid using proposed method (zoomed in)

In signal Q as well, periodogram estimates the watermarking frequencies (0.15Hz & 0.45 Hz) successfully. Using the proposed method, the fluctuations at the grid due to watermarking were eliminated (Fig. 4.37).

4.3 Conclusion

In this chapter, one of the issues for using watermarking signal for detecting replay attacks in the smart grids is studied. Later, a solution to these problems is proposed. Using the suggested method, we can decrease the fluctuations due to watermarking on the grid and, the process of authenticating each plant can get faster. This prevents attackers from collecting data that is without the watermarking signals. Although for this method, faster communication between plants and CC is needed for accurate cancelling of the effects of watermarking on the grid.

Chapter 5

Conclusion and Future Research

5.1 Conclusion

In this thesis, the problem of detecting replay attacks in smart grids was explored. An approach based on switching multi-sine waves was adapted for smart grids and a design procedure suitable for smart grid was developed. Furthermore, the existing single-input-single-output approach for multi-sine watermarking was extended for smart grids to a two-input-two-output scheme that significantly reduced grid power fluctuations due to watermarking.

The proposed method was studied for inverter-based power plants operating at a steady state. Probably, the method could work for other cases. Throughout every frame, multi-sine wave signal changes smoothly. Therefore, there will be no additional burden on the components such as actuating system, power electronics, transmission lines, due to abrupt changes in watermarking. For developing the watermarking signals, the frequency response information is needed which can be experimentally obtained. The proposed method is useful for detecting replay attacks happening within the power plant and in communication channels situated between the plant and central controller. Moreover, the results show that there is no fluctuation or harmonics added in the grid due to the watermark.

In order to send the watermarking signal to the plant and measure its effects on the output, communication between the central controller and the plant has to happen at a higher rate.

5.2 Future Research

Some suggestions for future research are discussed below.

- In this thesis we used MATLAB/Simulink simulations to assess watermarking. This can be improved in at least two ways. In the study, the process and measurement noise were not considered. The noise will have an impact on the choice of sine wave amplitudes and needs to be considered. The effects of watermarking on the overall grids can further be studied in detail using grid emulators.
- In this thesis, we discussed watermarking in two power plants. For a larger grid, watermarking can be done in pairs of plants in a similar fashion. While the impact of watermarking on grid power is very small for the case of two power plants, the impact on a grid when watermarking is simultaneously applied to all plants needs to be investigated.
- We assumed that all plants were fault free. If an electrical failure occurs, the impact of watermarking on the fault detection mechanisms should be investigated. It is important to make sure that watermarking will not interfere with the operation of fault detection systems.
- In our work, we added watermarking in the reference signals P and Q. The other locations for adding watermarking should be examined. Local controllers usually have different modes of operations. We used one of the general control modes i.e., PQ control. For different modes, one will have to find different locations for adding watermarking. But, as a general solution to all the modes, watermarking can be implemented as harmonics in the current. The order of the harmonics can be changed to stop attackers figuring out the detection strategy. Although this will require to have a separate time stamped signal from the central control to the plants for giving the harmonic watermarking reference. One also needs to make sure that the harmonics do not get eliminated by the filter and the magnitude of harmonics stays within acceptable limit.
- As discussed, we added watermarking in the reference signals which travel through the plant. Watermark can also be implemented in the sensor data before sending through the communication channels. On the other hand, before using the received data, the watermarking can be detected and eliminated from the measurement signal. This way,

watermarking will not travel though the plant, nor the effects of watermarking appear on the grid.

References

[1] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” Proc. *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, pp. 4490–4494. doi: 10.1109/IECON.2011.6120048.

[2] H. Zhang, B. Liu, and H. Wu, “Smart Grid Cyber-Physical Attack and Defense: A Review,” *IEEE Access*, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 29641–29659, 2021. doi: 10.1109/ACCESS.2021.3058628.

[3] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, “A survey on security control and attack detection for industrial cyber-physical systems,” *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018, doi: 10.1016/j.neucom.2017.10.009.

[4] Y. Ashibani and Q. H. Mahmoud, “Cyber physical systems security: Analysis, challenges and solutions,” *Comput Secur*, vol. 68, pp. 81–97, Jul. 2017, doi: 10.1016/j.cose.2017.04.005.

[5] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, “Ukraine cyber-induced power outage: Analysis and practical mitigation strategies,” Proc. *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, 2017, pp. 1–8. doi: 10.1109/CPRE.2017.8090056.

[6] S. Padhan and A. K. Turuk, “Design of False Data Injection Attacks in Cyber-Physical Systems,” *Inf Sci (N Y)*, vol. 608, pp. 825–843, Aug. 2022, doi: 10.1016/j.ins.2022.06.082.

[7] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” Proc. *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2009, pp. 911–918. doi: 10.1109/ALLERTON.2009.5394956.

[8] R. Chabukswar, Y. Mo, and B. Sinopoli, “Detecting integrity attacks on SCADA systems,” in *IFAC Proceedings Volumes (IFAC-PapersOnline)*, IFAC Secretariat, 2011, pp. 11239–11244. doi: 10.3182/20110828-6-IT-1002.03712.

[9] Y. Mo, R. Chabukswar, and B. Sinopoli, “Detecting integrity attacks on SCADA systems,” *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014, doi: 10.1109/TCST.2013.2280899.

[10] Y. Mo, S. Weerakkody, and B. Sinopoli, “Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs,” *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2015, doi: 10.1109/MCS.2014.2364724.

[11] T. Irita and T. Namerikawa, “Detection of replay attack on smart grid with code signal and bargaining game,” Proc. *2017 American Control Conference (ACC)*, 2017, pp. 2112–2117. doi: 10.23919/ACC.2017.7963264.

[12] F. Miao, M. Pajic, and G. J. Pappas, “Stochastic game approach for replay attack detection,” in *52nd IEEE Conference on Decision and Control*, 2013, pp. 1854–1859. doi: 10.1109/CDC.2013.6760152.

[13] T.-T. Tran, O.-S. Shin, and J.-H. Lee, “Detection of replay attacks in smart grid systems,” Proc. *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*, 2013, pp. 298–302. doi: 10.1109/ComManTel.2013.6482409.

[14] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng, “Optimal periodic watermarking schedule for replay attack detection in cyber–physical systems,” *Automatica*, vol. 112, Feb. 2020, doi: 10.1016/j.automatica.2019.108698.

[15] C. Fang, Y. Qi, P. Cheng and W. X. Zheng, "Cost-effective watermark based detector for replay attacks on cyber-physical systems," 2017 11th Asian Control Conference (ASCC), Gold Coast, QLD, Australia, 2017, pp. 940-945, doi: 10.1109/ASCC.2017.8287297.

[16] A. Khazraei, H. Kebriaei, and F. R. Salmasi, “Replay attack detection in a multi agent system using stability analysis and loss effective watermarking,” Proc. *2017 American Control Conference (ACC)*, 2017, pp. 4778–4783. doi: 10.23919/ACC.2017.7963694.

[17] M. Hosseini, T. Tanaka, and V. Gupta, “Designing optimal watermark signal for a stealthy attacker,” Proc. *2016 European Control Conference (ECC)*, 2016, pp. 2258–2262. doi: 10.1109/ECC.2016.7810627.

[18] A. Naha, A. Teixeira, A. Ahlén, and S. Dey, “Sequential Detection of Replay Attacks,” *IEEE Trans Automat Contr*, vol. 68, no. 3, pp. 1941–1948, 2023, doi: 10.1109/TAC.2022.3174004.

[19] S. Weerakkody, Y. Mo, and B. Sinopoli, “Detecting integrity attacks on control systems using robust physical watermarking,” in *53rd IEEE Conference on Decision and Control*, 2014, pp. 3757–3764. doi: 10.1109/CDC.2014.7039974.

[20] J. Rubio-Hernan, L. De Cicco, and J. Garcia-Alfaro, “On the use of watermark-based schemes to detect cyber-physical attacks,” *EURASIP J Inf Secur*, vol. 2017, no. 1, 2017, doi: 10.1186/s13635-017-0060-9.

[21] B. Satchidanandan and P. R. Kumar, “Dynamic watermarking: Active defense of networked cyber-physical systems,” *Proceedings of the IEEE*, vol. 105, no. 2, pp. 219–240, Feb. 2017, doi: 10.1109/JPROC.2016.2575064.

[22] B. Satchidanandan and P. R. Kumar, “Secure control of networked cyber-physical systems,” Proc. *2016 IEEE 55th Conference on Decision and Control (CDC)*, 2016, pp. 283–289. doi: 10.1109/CDC.2016.7798283.

[23] P. Hespanhol, M. Porter, R. Vasudevan, and A. Aswani, “Dynamic watermarking for general LTI systems,” in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017, pp. 1834–1839. doi: 10.1109/CDC.2017.8263914.

[24] W.-H. Ko, B. Satchidanandan, and P. R. Kumar, “Theory and implementation of dynamic watermarking for cybersecurity of advanced transportation systems,” Proc. *2016 IEEE Conference on Communications and Network Security (CNS)*, 2016, pp. 416–420. doi: 10.1109/CNS.2016.7860529.

[25] A. Khazraei, H. Kebriaei, and F. R. Salmasi, “A new watermarking approach for replay attack detection in LQG systems,” Proc. *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017, pp. 5143–5148. doi: 10.1109/CDC.2017.8264421.

[26] J. Ramos-Ruiz *et al.*, "Validation of a Robust Cyber Shield for a Grid Connected PV Inverter System via Digital Watermarking Principle," Proc. *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021, pp. 1–6. doi: 10.1109/PEDG51384.2021.9494227.

[27] H. Ibrahim, J. Kim, P. Enjeti, P. R. Kumar, and L. Xie, "Detection of Cyber Attacks in Grid-tied PV Systems Using Dynamic Watermarking," in *IEEE Green Technologies Conference*, IEEE Computer Society, 2022, pp. 57–61. doi: 10.1109/GreenTech52845.2022.9772036.

[28] J. Ramos-Ruiz *et al.*, "An Active Detection Scheme for Cyber Attacks on Grid-tied PV Systems," in *2020 IEEE CyberPELS (CyberPELS)*, 2020, pp. 1–6. doi: 10.1109/CyberPELS49534.2020.9311539.

[29] C. Zhang, D. Du, Q. Sun, X. Li, A. Rakić, and M. Fei, "Security weakness of dynamic watermarking-based detection for generalised replay attacks," *Int J Syst Sci*, vol. 53, no. 5, pp. 948–966, 2022, doi: 10.1080/00207721.2021.1979687.

[30] D. Du, C. Zhang, X. Li, M. Fei, and H. Zhou, "Attack Detection for Networked Control Systems Using Event-Triggered Dynamic Watermarking," *IEEE Trans Industr Inform*, vol. 19, no. 1, pp. 351–361, 2023, doi: 10.1109/TII.2022.3168868.

[31] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 5820–5826. doi: 10.1109/CDC.2015.7403134.

[32] B. Tang, L. D. Alvergue, and G. Gu, "Secure networked control systems against replay attacks without injecting authentication noise," Proc. *2015 American Control Conference (ACC)*, 2015, pp. 6028–6033. doi: 10.1109/ACC.2015.7172286.

[33] O. Ozel, S. Weerakkody, and B. Sinopoli, "Physical watermarking for securing cyber physical systems via packet drop injections," Proc. *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2017, pp. 271–276. doi: 10.1109/SmartGridComm.2017.8340720.

[34] A. Abdelwahab, W. Lucia, and A. Youssef, "Set-Theoretic Control for Active Detection of Replay Attacks with Applications to Smart Grid," Proc. *2020 IEEE Conference on Control*

Technology and Applications (CCTA), 2020, pp. 1004–1009. doi: 10.1109/CCTA41146.2020.9206373.

[35] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, Oct. 2015, pp. 1004–1015. doi: 10.1145/2810103.2813679.

[36] R. Romagnoli, S. Weerakkody, and B. Sinopoli, "A Model Inversion Based Watermark for Replay Attack Detection with Output Tracking," Proc. *2019 American Control Conference (ACC)*, 2019, pp. 384–390. doi: 10.23919/ACC.2019.8814483.

[37] A. Hoehn and P. Zhang, "Detection of replay attacks in cyber-physical systems," in *2016 American Control Conference (ACC)*, 2016, pp. 290–295. doi: 10.1109/ACC.2016.7524930.

[38] C. Trapiello and V. Puig, "A Zonotopic-Based Watermarking Design to Detect Replay Attacks," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 11, pp. 1924–1938, 2022, doi: 10.1109/JAS.2022.105944.

[39] C. Trapiello and V. Puig, "Replay attack detection using a zonotopic KF and LQ approach," Proc. *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2020, pp. 3117–3122. doi: 10.1109/SMC42975.2020.9282865.

[40] C. Trapiello and V. Puig, "Set-based replay attack detection in closed-loop systems using a plug & play watermarking approach," Proc. *2019 4th Conference on Control and Fault Tolerant Systems (SysTol)*, 2019, pp. 330–335. doi: 10.1109/SYSTOL.2019.8864790.

[41] C. Trapiello, D. Rotondo, H. Sanchez, and V. Puig, "Detection of replay attacks in CPSs using observer-based signature compensation," Proc. *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2019, pp. 1–6. doi: 10.1109/CoDIT.2019.8820639.

[42] H. Liu, J. Yan, Y. Mo, and K. H. Johansson, "An On-line Design of Physical Watermarks," in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 440–445. doi: 10.1109/CDC.2018.8619632.

[43] H. Liu, Y. Mo, J. Yan, L. Xie, and K. H. Johansson, “An Online Approach to Physical Watermark Design,” *IEEE Trans Automat Contr*, vol. 65, no. 9, pp. 3895–3902, Sep. 2020, doi: 10.1109/TAC.2020.2971994.

[44] Y. Yu, W. Yang, W. Ding, and J. Zhou, “Reinforcement Learning Solution for Cyber-Physical Systems Security Against Replay Attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2583–2595, 2023, doi: 10.1109/TIFS.2023.3268532.

[45] A. Ghamarilangroudi, “Detection of Replay Attack in Control Systems Using Multi-Sine Watermarking,” MASc thesis, Dept. of ECE, Concordia University, Montreal, Canada, March 2020.

[46] R. M. G. Ferrari and A. M. H. Teixeira, “Detection and isolation of routing attacks through sensor watermarking,” in *2017 American Control Conference (ACC)*, 2017, pp. 5436–5442. doi: 10.23919/ACC.2017.7963800.

[47] D. Ye, T. Y. Zhang, and G. Guo, “Stochastic coding detection scheme in cyber-physical systems against replay attack,” *Inf Sci (N Y)*, vol. 481, pp. 432–444, May 2019, doi: 10.1016/j.ins.2018.12.091.

[48] H. Liu, Y. Li, Q.-L. Han, and T. Raïssi, “Watermark-Based Proactive Defense Strategy Design for Cyber-Physical Systems With Unknown-but-Bounded Noises,” *IEEE Trans Automat Contr*, vol. 68, no. 6, pp. 3300–3315, 2023, doi: 10.1109/TAC.2022.3184396.

[49] H. Guo, Z. H. Pang, J. Sun, and J. Li, “An Output-Coding-Based Detection Scheme against Replay Attacks in Cyber-Physical Systems,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 10, pp. 3306–3310, Oct. 2021, doi: 10.1109/TCSII.2021.3063835.

[50] M. Ghaderi, K. Gheitasi, and W. Lucia, “A blended active detection strategy for false data injection attacks in cyber-physical systems,” *IEEE Trans Control Netw Syst*, vol. 8, no. 1, pp. 168–176, Mar. 2021, doi: 10.1109/TCNS.2020.3024315.

[51] A. M. H. Teixeira and R. M. G. Ferrari, “Detection of Sensor Data Injection Attacks with Multiplicative Watermarking,” in *2018 European Control Conference (ECC)*, 2018, pp. 338–343. doi: 10.23919/ECC.2018.8550114.

[52] R. M. G. Ferrari and A. M. H. Teixeira, “A Switching Multiplicative Watermarking Scheme for Detection of Stealthy Cyber-Attacks,” *IEEE Trans Automat Contr*, vol. 66, no. 6, pp. 2558–2573, Jun. 2021, doi: 10.1109/TAC.2020.3013850.

[53] L. Wu, D. Du, C. Zhang, M. Fei and I. Popovic, "An Active Detection Method for Generalized Replay Attacks Using Multiplicative Watermarking," 2022 41st Chinese Control Conference (CCC), Hefei, China, 2022, pp. 4460-4465, doi: 10.23919/CCC55666.2022.9901662.

[54] P. Welch, “The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms,” *IEEE Transactions on Audio and Electroacoustics*, vol. 15, no. 2, pp. 70–73, 1967, doi: 10.1109/TAU.1967.1161901.

[55] R. Teodorescu, M. Liserre, and P. (Electrical engineer) Rodríguez, *Grid converters for photovoltaic and wind power systems*. Wiley-IEEE Press, 2007. Accessed: Jul. 07, 2023. [Online]. Available: www.wiley.com/go/grid_converters

[56] S. Li, T. A. Haskew, and L. Xu, “Conventional and novel control designs for direct driven PMSG wind turbines,” *Electric Power Systems Research*, vol. 80, no. 3, pp. 328–338, Mar. 2010, doi: 10.1016/j.epsr.2009.09.016.

[57] H. Karimi, H. Nikkhajoei, and R. Iravani, “Control of an electronically-coupled distributed resource unit subsequent to an islanding event,” *IEEE Transactions on Power Delivery*, vol. 23, no. 1, pp. 493–501, Jan. 2008, doi: 10.1109/TPWRD.2007.911189.

[58] Se-Kyo Chung, "A phase tracking system for three phase utility interface inverters," in IEEE Transactions on Power Electronics, vol. 15, no. 3, pp. 431-438, May 2000, doi: 10.1109/63.844502.

[59] M. Ben Saïd-Romdhane, M. W. Naouar, I. S. Belkhodja, and E. Monmasson, “Simple and systematic LCL filter design for three-phase grid-connected power converters,” *Math Comput Simul*, vol. 130, pp. 181–193, Dec. 2016, doi: 10.1016/j.matcom.2015.09.011.

[60] A. C. Z. de Souza, F. M. Portelinha, B. De Nadai, D. Q. Oliveira, and D. Marujo, “Overview on microgrids: Technologies, control and communications,” in *Sustainable Development in*

Energy Systems, Springer International Publishing, 2017, pp. 1–18. doi: 10.1007/978-3-319-54808-1_1.

[61] C. Li, Y. Yang, Y. Cao, L. Wang, and F. Blaabjerg, "Frequency and Voltage Stability Analysis of Grid-Forming Virtual Synchronous Generator Attached to Weak Grid," *IEEE J Emerg Sel Top Power Electron*, vol. 10, no. 3, pp. 2662–2671, Jun. 2022, doi: 10.1109/JESTPE.2020.3041698.

[62] A. Ranjan, D. V. Bhaskar, O. Al Zaabi, P. Kumar, K. Al Hosani, and U. R. Muduli, "Voltage Fluctuations and Sensitivity Assessment of Load Flow Solutions for the IEEE 9-bus System," Proc. *2023 IEEE IAS Global Conference on Renewable Energy and Hydrogen Technologies, GlobConHT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/GlobConHT56829.2023.10087888.

Appendix

Appendix A

Simulink files:

Single plant with watermarking

Double plants with watermarking

Bode plots of the Single plant

Appendix B

```
% Power Spectral Density estimates using Periodogram

scopedata = out.ScopeDataWMQ2;
x = scopedata.signals.values(10000001:16667000); % data

%x = scopedata.signals.values(6000001:16000000);
flow=0.1*0.1; % choosing lower range
fup=1.5*0.4; % choosing upper range
nf=1000;
fstep=(fup-flow)/nf;
f=flow:fstep:fup;
[pxx,fxx]=periodogram(x,[],f,10^6);
plot(fxx,pxx)
xlabel('Hz')
ylabel('PSD')
title('Periodogram')
grid
```

% Periodogram with 95% confidence bound

```
fs = 1000; % sampling frequency
t = 0:1/fs:1-1/fs;
x = cos(2*pi*120*t) + 0.3*sin(2*pi*200*t) + randn(size(t)); % signal with noise

[pxx,f,pxxc] = periodogram(x,rectwin(length(x)),length(x),fs,...
    'ConfidenceLevel',0.95);

plot(f,10*log10(pxx))
hold on
plot(f,10*log10(pxxc(:,1)),'r-.')
hold on
plot(f,10*log10(pxxc(:,2)),'g-.')

xlim([80 220])
xlabel('Hz')
ylabel('dB/Hz')
title('Periodogram with 95%-Confidence Bounds')
```

Appendix C

```
clc
clear

% Modified IEEE 9 bus test system


Sbase = 100; % MVA base

% defining impedance of the lines
nfrom = [1 4 5 3 6 7 8 8 9]';

nto = [4 5 6 6 7 8 2 9 4]';

r = [0 0.017 0.039 0 0.0119 0.0085 0 0.032 0.01]';

x = [0.0576 0.092 0.17 0.0586 0.1008 0.072 0.0625 0.161 0.085]';

b = [0 0.158 0.358 0 0.209 0.149 0 0.306 0.176]';

z = [];

for i = 1 : length(r)
    z(i) = sqrt((r(i)*r(i))+(x(i)*x(i)));
end

z = z';
```

```
% Power flow data

is = 1; ipq = [2 3 4 5 6 7 8 9]'; ipv = [1]'; Vo = [1]';

toler = 0.0001; maxiter = 10;

Pd = [0 0 0 0 90 0 100 0 125]'; Qd = [0 0 0 0 30 0 35 0 50]';

Pg = [0 162 85 20 0 0 0 0 0]'; Qg = [0 8 3 2 0 0 0 0 0]';

dPg = [0 0 0 0 0 0 0 0 0]'; dQg = [0 0.08 0 -0.08 0 0 0 0 0]';


nbranch = length(nfrom);   % Used to know the number of branches(lines).
y = zeros(nbranch,1);  % Form the vector of line admittances, initialized with zero.
i = sqrt(-1);
for n = 1:nbranch
    y(n)=1/(r(n)+(i*x(n)));        % Calculates the admittances of each line.
end
Id = eye(nbranch);
A = Id(1:nbranch,nfrom)-Id(1:nbranch,nto);  % Form the Incidence Matrix.
Yb=diag(y);
Y=(A*Yb*A') + (1/2)*diag(abs(A)*(i*b));  % Admittance Matrix is formed and returned.




% Function called.
[Ni,time, J] = nrpf(Y,is,ipq,ipv,Pg,Qg,Pd,Qd,Vo,Sbase,toler,maxiter);

% calculating the change
delPQ = [];
for i = 1:n-1
    delPQ(i) = dPg(i+1);
end
for i = 1:n-1
    delPQ(i+n-1) = dQg(i+1);
end

Sen = inv(J);

delPQ = delPQ'/Sbase;

delVD = Sen*delPQ;

%% ----- Newton Rhapson Power Flow Algorithm ----- %%

function [Ni,time, J] = nrpf(Y,is,ipq,ipv,Pg,Qg,Pd,Qd,Vo,Sbase,toler,maxiter)
npq = length(ipq);              % Number of PQ nodes.
npv = length(ipv);              % Number of PV nodes.
N = npq+npv;                    % Total number of nodes(PQ+PV+slack).
del = zeros(N,1);               % Defining the delta vector.
```

```
V = zeros(N,1);                 % Defining the voltage vector.
V(:) = 1;                       % Intializing all the voltages with 1 pu value.
for i=1:N
    for j=1:npv
        if i== ipv(j)
            V(i)=Vo(j);         % Setting the voltage magnitudes at the PV bus.
        end
    end
end
Pinj = (Pg - Pd)/Sbase;         % P and Q injection calculated in pu.
Qinj = (Qg - Qd)/Sbase;
G = real(Y);                    % The conductance G is taken.
B = imag(Y);                    % The susceptance B is taken.
iter = 0;
t0 = cputime;                   % Time count started.

% Below is the iteration of the algorithm.
while true
    P = zeros(N,1);             % Initializing P.
    Q = zeros(N,1);             % Initializing Q.
    for i=1:N                   % Calculating P and Q at all the nodes.
        for j=1:N
            P(i) = P(i) + V(i)*V(j)*(G(i,j)*cos(del(i) - del(j)) + B(i,j)*sin(del(i)
- del(j)));
            Q(i) = Q(i) + V(i)*V(j)*(G(i,j)*sin(del(i) - del(j)) - B(i,j)*cos(del(i)
- del(j)));
        end
    end
    dPk = Pinj - P;       % Finding the difference in the Power(mismatch).
    dQk = Qinj - Q;
    dP = dPk(2:N,1);    % del P at all nodes, other than slack node viz 1 here(N-1).
    dQ = zeros(npq,1);        % del Q at PQ nodes(Npq elements).
    for i=1:N
        for j=1:npq
            if i==ipq(j)
                dQ(j,1) = dQk(i);      % Defining the del q for main equation.
            end
        end
    end
    fx = [dP; dQ]; % The fx viz. the vector of the dP and dQ used to solve for del d
and del V.
    tol = max(abs(fx));
    if tol<toler               % When the convergence occurs it stops.
        break
    end

    % Now calcluations of H,L,M,N need to be done.
    % First for H.
    H = zeros(N-1,N-1);         % H initialized.
    for i=1:N-1
        k=i+1;                  % k and m tends for 2 to N.
        for j=1:N-1
            m=j+1;
            if k==m
```

```
                for n=1:N
                    H(i,j) = H(i,j) - V(k)*V(n)*(G(k,n)*sin(del(k) - del(n)) -
B(k,n)*cos(del(k) - del(n)));
                end
                H(i,j) = H(i,j) - B(k,k)*(V(k)^2);
            else
                H(i,j) = V(k)*V(m)*(G(k,m)*sin(del(k) - del(m)) - B(k,m)*cos(del(k) -
del(m)));
            end
        end
    end
    % Calculations for N.
    Nj = zeros(N-1,npq);
    for i=1:N-1
        k=i+1;
        for j=1:npq
            m=ipq(j);
            if k==m
                for n=1:N
                    Nj(i,j) = Nj(i,j) + V(k)*V(n)*(G(k,n)*cos(del(k) - del(n)) +
B(k,n)*sin(del(k) - del(n)));
                end
                Nj(i,j) = Nj(i,j) + G(k,m)*(V(k)^2);
            else
                Nj(i,j) = (V(k)*V(m))*(G(k,m)*cos(del(k) - del(m)) +
B(k,m)*sin(del(k) - del(m)));
            end
        end
    end
    % Calculating for M.
    M = zeros(npq,N-1);
    for i=1:npq
        k=ipq(i);
        for j=1:N-1
            m=j+1;
            if k==m
                for n=1:N
                    M(i,j) = M(i,j) + V(k)*V(n)*(G(k,n)*cos(del(k) - del(n)) +
B(k,n)*sin(del(k) - del(n)));
                end
                M(i,j) = M(i,j) - G(k,m)*(V(k)^2);
            else
                M(i,j) = (-1)*V(k)*V(m)*(G(k,m)*cos(del(k) - del(m)) +
B(k,m)*sin(del(k) - del(m)));
            end
        end
    end
    % Calculating for L.
    L = zeros(npq,npq);
    for i=1:npq
        k=ipq(i);
        for j=1:npq
            m=ipq(j);
            if k==m
```

```
                for n=1:N
                    L(i,j) = L(i,j) + V(k)*V(n)*(G(k,n)*sin(del(k) - del(n)) -
B(k,n)*cos(del(k) - del(n)));
                end
                L(i,j) = L(i,j) - B(k,m)*(V(k)^2);
            else
                L(i,j) = (V(k)*V(m))*(G(k,m)*sin(del(k) - del(m)) - B(k,m)*cos(del(k)
- del(m)));
            end
        end
    end
    J = [H Nj; M L];        % Forming the Jacobian Matrix.

    % Now calcuating the x viz. change in delta and voltages.
    x = J\fx;
    ddel = x(1:N-1);        % Dividing the x vector in two form ddel and dV.
    dV = x(N:end);

    iter = iter+1;                  % Increase in the iteration.
    if maxiter == iter % If there is limitation in the iteration, the loop will get
break.
        break
    end
end
t1 = cputime - t0;                  % End of counting time, at the end of the
convergence.
Ni = iter;
time = t1;
end

%% ----- Code Ends ----- %%
```