

# STATE ESTIMATION THROUGH SECURE WIRELESS COMMUNICATION IN A SMART GRID

---

A Thesis submitted in partial fulfilment  
Of the Requirements for the Award of the degree of  
Master of Technology  
In  
Industrial Electronics

By

JOYA SANKAR DWIBEDY

ROLL No: 212EE5513



Department of Electrical Engineering  
National Institute of Technology, Rourkela  
Rourkela-769008, India  
<http://www.nitrkl.ac.in>

# STATE ESTIMATION THROUGH SECURE WIRELESS COMMUNICATION IN A SMART GRID

---

A Thesis submitted in partial fulfilment  
Of the Requirements for the Award of the degree  
of Master of Technology  
In

Industrial Electronics

By

JOYA SANKAR DWIBEDY

Under the Guidance of  
Prof. Bidyadhar Subudhi



Department of Electrical Engineering  
National Institute of Technology, Rourkela  
Rourkela-769008, India  
<http://www.nitrkl.ac.in>



# **National Institute of Technology Rourkela**

## **CERTIFICATE**

This is to certify that the thesis entitled, “**State Estimation Through Secure Wireless Communication in a Smart Grid**” submitted by **Mr. Joya Sanakr Dwibedy (Roll No. 212EE5513)** in partial fulfilments for the requirements for the award of Master of Technology Degree in Electrical Engineering with specialization in “**Industrial Electronics**” during 2012-2014 at National Institute of Technology, Rourkela is an authentic work carried out by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University / Institute for the award of any degree or diploma.

Date:

**Prof. Bidyadhar Subudhi**  
Department of Electrical Engineering  
National Institute of Technology  
Rourkela-769008



## **National Institute of Technology Rourkela**

### **Declaration**

I certify that

- a) The work contained in the thesis is original and has been done by myself under the general supervision of my supervisor.
- b) The work has not been submitted to any other Institute for any degree or diploma.
- c) I have followed the guidelines provided by the Institute in writing the thesis.
- d) Whenever I have used materials (experimental analysis, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.
- e) Whenever I have quoted written materials from other sources, I have put them under quotation marks and given due credit to the sources by citing them and giving required details in the references.

Date:

Joya Sankar Dwibedy

## **ACKNOWLEDGEMENT**

I have been very fortunate to have **PROF. BIDYADHAR SUBUDHI**, Department of Electrical Engineering, National Institute of Technology; Rourkela as my project supervisor. I am highly indebted to him and express my deep sense of gratitude for his guidance and support. I am grateful to my supervisor, who gave me the opportunity to realize this work. He encouraged, supported and motivated me with much kindness throughout the work. In particular, he showed me the interesting side of the power system and communication engineering and those of the highly interdisciplinary project work. I always had the freedom to follow my own ideas, which I am very grateful for him. I really admire him for patience and staying power to carefully read the whole manuscript. I am also grateful to our head of department, **PROF. A. K. PANDA**, who gave me the opportunity work in this field.

I express my sincere gratitude to all the faculty members of the Department of Electrical Engineering, NIT Rourkela for their unparalleled academic support.

Date:

**Joya Sanakr Dwibedy**  
Roll. No.: 212EE5441  
4<sup>th</sup>Semester, M.Tech (Regular)  
Dept. of Electrical Engineering

# CONTENTS

ABSTRACT .....	viii
LIST OF ABBREVIATIONS .....	x
LIST OF SYMBOLS .....	xi
LIST OF FIGURE.....	xii
<b>1 INTRODUCTION.....</b>	<b>2</b>
1.1 OVERVIEW .....	2
1.2 LITERATURE REVIEW ON STATE ESTIMATION IN SG.....	3
1.3 PROBLEM DEFINATION.....	4
1.4 MOTIVATION AND OBJECTIVE OF THE THESIS .....	5
1.4.1 MOTIVATION.....	5
1.4.2 OBJECTIVE OF THE THESIS .....	5
1.4 ORGANIZATION OF THE THESIS .....	6
<b>2 SIMPLIFIED SMART GRID MODEL .....</b>	<b>8</b>
2.1 THEORETICAL SETUP OF SMART GRID MODEL .....	8
2.3 SYSTEM MODEL OF SMART GRID .....	9
2.3.1 SYSTEM DYNAMICS:.....	10
2.3.2 COMMUNICATION LINKS .....	10
<b>3 SECURE STATE ESTIMATION IN SMART GRID MODEL .....</b>	<b>13</b>
3.1 SECURE COMMUNICATION FOR DYNAMIC SYSTEM.....	13
3.1.1 TOPOLOGICAL ENTROPY.....	14
3.1.2 SPANNING SET.....	15
3.1.3 CAPACITY REQUIREMENT FOR STATE ESTIMATION.....	15
3.2 SYSTEM STATE ESTIMATION .....	16
3.2.1 SECURE STATE ESTIMATION.....	18
3.3 DEFULT SETUP .....	19
3.3.1 SIMULATION RESULT AND CONCLUSION.....	19

<b>4 SECURE TRANSMISSION OF ESTIMATED SYSTEM STATE IN SMART GRID MODEL</b> .....	<b>23</b>
4.1 INTRODUCTION.....	23
4.1.1 ATTACK IN WIRELESS NETWORK .....	23
4.1.2 SECURITY ISSUE .....	24
4.2 SPREAD SPECTRUM (SS) .....	24
4.2.1 PN SEQUENCE CODE GENERATOR .....	25
4.2.2 PROCESSING GAIN IN SPREAD SPECTRUM.....	26
4.2.3 TYPES OF SPREAD SPECTRUM .....	27
4.2.4 DIRECT SEQUENCE SPREAD SPECTRUM WITH BPSK.....	28
4.3 SIMULATION RESULT OF SMART GRID MODEL USING SINGLE OBSERVER .....	29
4.3.1 SIMULATED WAVE FORM AT TRANSMITTER END .....	30
4.3.2 SIMULATED WAVE FORM AT WIRELESS CHANNEL.....	31
4.3.3 SIMULATED FREQUENCY RESPONSE AT TRANSMITTER END .....	32
4.3.4 SIMULATED WAVE FORM AT RECEIVER INPUT .....	33
4.3.5 RECEIVER OUTPUT OBTAINED FROM SIMULATION .....	34
4.4 SIMULATION RESULT OF SMART GRID MODEL USING MULTIPLE OBSERVER .....	35
4.4.1 SIMULATED WAVE FORM AT TRANSMITTER END .....	36
4.4.2 PN SEQUENCE GENERATION AT TRANSMITTER END.....	37
4.4.3 FREQUENCY RESPONSE AT TRANSMITTER END.....	38
4.4.4 WAVE FORM OF WIRELESS CHANNEL & RECEIVER O/P OBTAINED FROM SIMULATION .....	39
<b>5 CONCLUSION AND SCOPE FOR FUTURE WORK.....</b>	<b>41</b>
5.1 CONCLUSION .....	41
5.2 SCOPE FOR FUTURE WORK.....	41

## ABSTRACT

Secure system state estimation and anti-jamming transmission is a critical issue in smart grid to assure reliability and stability. The smart grid is modelled as a linear dynamic system. This paper consider an observer station, an eavesdropper listening in presence of Gaussian noise communication channel and a control centre. In smart grid model, the problem of how to evaluate information rate (bit/sec) and system state of the linear dynamic system as well as securely transmit to destination through wireless link is studied. The capacity requirement is evaluated by numerical simulation in typical configuration of smart grid. The open nature of the wireless network has raised issues of confidentiality and security of transmitted information. Various attacks such as eavesdropping, information tampering, and malicious control command injection would impose serious threat on secure and stable smart grids operation in wireless channel. Spread spectrum techniques is an important ingredient that prevent such threats of attack in wireless communication as well as achieve the privacy of dynamic system state information during transmission. The project focus on securely recovery of system state at control centre in case of single and multiple observer system using DSSS (direct sequence spread spectrum) in simplified smart grid dynamic model through MATLAB simulation.

Key word: channel capacity; smart grid; spread spectrum; eavesdropper; direct sequence spread spectrum (DSSS)

## **LIST OF ABBREVIATIONS**

SG	Smart Grid
PN	Pseudo Noise
SS	Spread Spectrum
PSD	Power Spectral Density
WSNs	Wireless Sensor Networks
BPSK	Binary Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
FSSS	Frequency Hopping Spread Spectrum

## LIST OF SYMBOLS

### Symbol

$\Delta$	Security meter
$H(.)$	Topological entropy
$E_b$	Energy bit per second
$\tau_g$	Time constant of supply
$\tau_d$	Time constant of demand
$E$	Accumulated Energy Error
$\lambda$	Market price at any given time
$T_b$	Time per bit of message sequence
$\lambda_i$	Eigen Values of matrix $i = 1,2,3,4$
$\tau_\lambda$	Time constant price change due to market
$\lambda_g$	Marginal cost of producing $P_g$ per unit power
$C_d$	Increasing rate of benefit w.r.t consumed Power
$C_g$	Increasing rate of cost rate w.r.t generated Power

## LIST OF FIGURE

Figure 1. Problem identification in smart grid.....	4
Figure 2. Smart grid model.....	8
Figure 3. Timing structure of smart grid model.....	10
Figure 4. Coding and decoding procedure of smart grid model.....	11
Figure 5. Simplified smart grid dynamic model.....	13
Figure 6. Topological Entropy Vs. large value of $C_g$ and $C_d$ .....	19
Figure 7. Topological Entropy Vs. $T_g$ and $T_d$ .....	20
Figure 8. Topological entropy Vs. $\tau_\lambda$ and $k$ .....	21
Figure 9. Secrecy capacity Vs. gain at different power level.....	21
Figure 10. Eavesdropper attack in wireless medium.....	23
Figure 11. Spread spectrum communication in simplified smart grid model.....	24
Figure 12. Linear feedback shift register.....	25
Figure 13. Linear feedback shift register for $m=5$ .....	26
Figure 14. Spreading and de-spreading signal in DSSS.....	27
Figure 15. Model of a direct-sequence spread bpsk system.....	28
Figure 16. Wave form of original bit sequence in NRZ form at transmitter end.....	30
Figure 17. Waveform of Pseudo random sequence.....	30
Figure 18. Waveform of Spreaded signal at transmitter end.....	30
Figure 19. Waveform of carrier signal, bpsk modulated signal and transmitted signal (signal + noise (snr=-10db)) at wireless channel.....	31
Figure 20. Waveform of frequency response of original signal, spreaded signal and BPSK modulator output signal at transmitter end.....	32

Figure 21. Waveform of de-spread signal with noise at receiver end .....	33
Figure 22. Waveform of demodulated and de-spreaded data without noise at receiver end.....	34
Figure 23. Multiple observer in simplified smart grid model.....	35
Figure 24. Wave form of Input signal, NRZ form of input signal and BPSK modulator output signal of observer1 and observer2 at transmitter end.....	36
Figure 25. Wave form of PN sequence and spreaded signal of observer1 and observer2.....	37
Figure 26. Waveform of frequency response of original signal and spreaded signal of observer1 and observer2 at transmitter end. ....	38
Figure 27. Waveform of composite signal, composite signal with noise, o /p of demodulated BPSK signal and received bit sequence observer1 and observer2 at receiver end.....	39

# **CHAPTER-1**

## **INTRODUCTION**

# 1 INTRODUCTION

---

## 1.1 OVERVIEW

In current scenario, the technology of smart grid has attracted much attention in the communities of power systems, communications, networking and control systems [2]. In a smart grid, modern information technologies are applied for power systems to report the instantaneous power load information on the distributed observer to a control centre and feedback the time varying price information to the power consumers such that power consumption can be controlled efficiently [1]. This can be possible only when if information is not interrupted by noise and capacity of channel will be sufficient enough. Here information's are continuous in nature as source is dynamic system. Hence communication play a crucial role as information of system state and control messages need to dispatched over communication network in smart grid. This two ways digital communication technology add value added service where as it is liable to security threat like eavesdropping, information tampering, and malicious control command injection etc. So it is very much essential to design a protocol or model that can deal with all possible threats. In this thesis for simplicity consider a simplified model of smart grid that contain single observer station and a control centre. Here observations are collected from many distributed observers, like the load information is retrieved from the reports of smart meters and the power generation information is retrieved from the power generation companies respectively. Here information is continuous in nature as data is collected from dynamic sources. It is a challenging task to compute information rate in dynamic system as communication with security usually focuses on stationary and ergodic information sources as per traditional information theory concept [10].

Wireless communication offers the benefits of low cost, rapid deployment, shared communication medium and mobility. At the same time the open nature of the wireless network has raised issues of confidentiality and security of transmitted information. Here we applied spread spectrum technique to smart grid model that generate scrambling code to protect from various attacks such as eavesdropping, information tampering, and malicious control command injection. This project focuses on physical layer security of single and multiple observer systems in the presence

of passive eavesdroppers, i.e. the transmitter is unaware of the eavesdropper's presence. The strategy adopted for secure communication is artificial pseudo noise (PN sequence) generation both transmitter and receiver side. This paper mainly concentrates on direct sequence spread spectrum (DS/SS) for single and multiple observer in simplified smart grid model. The model considered here is simpler than practical case. Results from MATLAB simulations are presented and discussed in detail.

## **1.2 LITERATURE REVIEW ON STATE ESTIMATION IN SG**

Day by day new technologies are added in smart grid to meet current and future requirement of customer as well as increase reliability, quality of service and efficiency. This addition or up gradation of new technology introduce new security vulnerabilities into the system. Various researched worked done against security issue in smart grid for stable operation. The smart grid is a large and complex system, so review on security threat can divided into three different research category: Process Control Security, Smart Meter Security and Power System State Estimation. Out of these we focus on power system state estimation security as it control the physical properties by maintaining stable state of the existing electrical power system. The security of system state is challenging as system instability and financial gain is the motivation of attackers. In [18] Xie, Mo, and Sinopoli worked on false data injection attacks. The contribution of this work carried out to build an algorithm to find observer able and un- observable attack and does not manipulate the pricing model of smart grid. Dan and Sandberg worked on false injection attack in system state estimation model in [19]. They designed an algorithm to compute security index for state estimator protect against manipulation at input source flow.

### **OBSERVATION FROM LITERATURE REVIEW**

Researcher designed some algorithms to detect observable, un-observable attack and false injection attack in system state. Also designed a security index for protect state estimator against manipulation at input source.

### 1.3 PROBLEM DEFINATION

In smart grid system state has ability to control and monitor the physical properties of the electrical power system. Thus smart grid maintain the stable state in electrical power grid. Here system state is time varying load and price signal. Communication play a crucial role since information about load (generated power or consumed power) and price needs to be conveyed through communication network. In this thesis we identified two problems that are given below

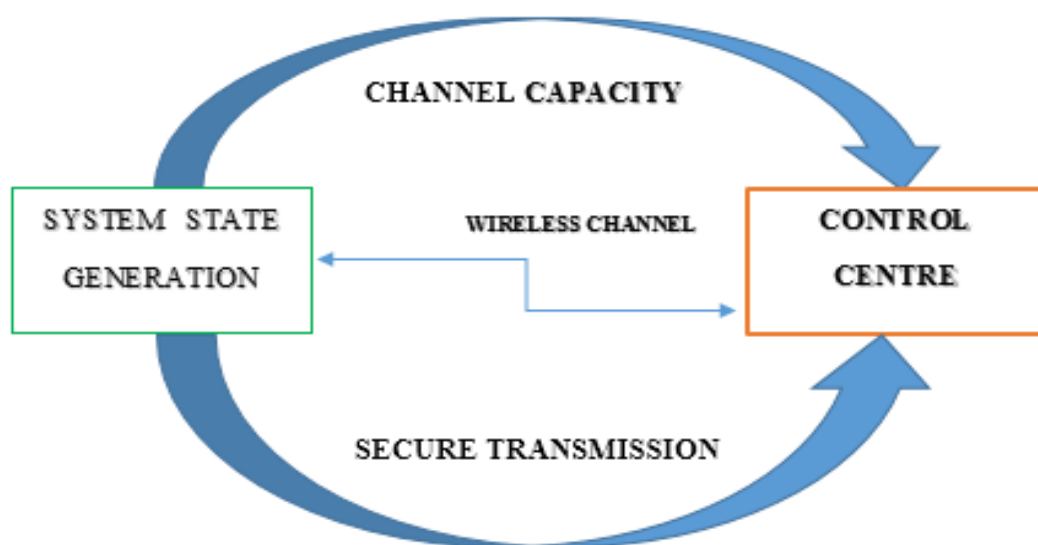


FIGURE 1. PROBLEM IDENTIFICATION IN SMART GRID

**Capacity:** The communication channel capacity should be able to convey the system state information to the destinations like control centre with negligible error in a real-time manner.

**Security:** Secure transmission and privacy of system state is a major issue in smart grid. The security of system state is challenging as system instability and financial gain is the motivation of attackers.

## **1.4 MOTIVATION AND OBJECTIVE OF THE THESIS**

### **1.4.1 MOTIVATION**

In current scenario, the technology of smart grid has attracted much attentions from engineer and researcher in both electric power and communication sector. The concept of smart grid appeared in literature in different flavors like future grid or intelligent grid. The aim of the smart grid concept is to provide electricity as well as some value added service to the end-users or customers with securely and reliably in stable manner using two way digital communication technology. This two ways digital communication technology enable both customer as well as power supplier to enhance the service quality, reliability by reducing energy consumption and the cost per unit price. The additional value added application in smart grid communication directly or indirectly liable to security threat like eavesdropping, information tampering, and malicious control command injection etc. So it is very much essential to design a protocol or model that can deal with all possible threats.

### **1.4.2 OBJECTIVE OF THE THESIS**

- ❖ To study system dynamics of simplified smart grid model and establish a limit to the information rate (bits/sec) for secure communication of dynamic source with information theoretic approach.
- ❖ Implement the system state model of Alvarado in SG model and the requirement of communication in wireless channel that influenced by different parameter in for secure state estimation. Also calculate the secrecy capacity in presence of eavesdropper.
- ❖ To maintain privacy as well securely transmit the estimated system state in wireless medium by using spread spectrum technique to retrieve original system state at receiver output for the case of single and multiple observer station in smart grid model in presence of passive eavesdropper using MATLAB software.

## 1.4 ORGANIZATION OF THE THESIS

This thesis is organised into five different chapter including introduction

**Chapter 1:** In this chapter includes the introduction, problem identification, motivation & objective of the project. It also covers literature review on secure system state estimation and transmission in smart grid.

**Chapter 2:** This chapter describes the concept of simplified smart grid dynamic model. It includes dynamics of system model and procedure of coding & decoding.

**Chapter 3:** This chapter discussed about the security metrics and system state estimation with linear dynamic. These chapters contain numerical simulation result of impact of different factors on channel capacity requirement as well as secrecy capacity for reliable and secure state estimation of the developed model has been discussed.

**Chapter 4:** In this chapter focused on threatening in wireless channel and spread spectrum technique and generation of PN sequence or scrambling code using linear feedback shift register (LFSR). It also cover the verification of original system state at receiver output with conclusion of secure transmission process in wireless medium using DSSS through single as well as multiple observer case of simplified smart grid model in MATLAB software.

**Chapter 5:** Finally this chapter concludes the thesis work and scope for future work.

# **CHAPTER 2**

## **SIMPLIFIED SMARTGRID MODEL**

## 2 SIMPLIFIED SMART GRID MODEL

### 2.1 THEORETICAL SETUP OF SMART GRID MODEL

Here we take a simpler dynamics model in smart grid environment .This model build foundation for more precise problems with answer that could provide important insights into the nature of secrete communication. The insights may be used to shape development of practical systems for smooth communication in complex setting of smart grid.

The simplified smart grid dynamic model consists of

- Observer station
- Control centre
- Wireless channel
- Eavesdropper

In the below model:

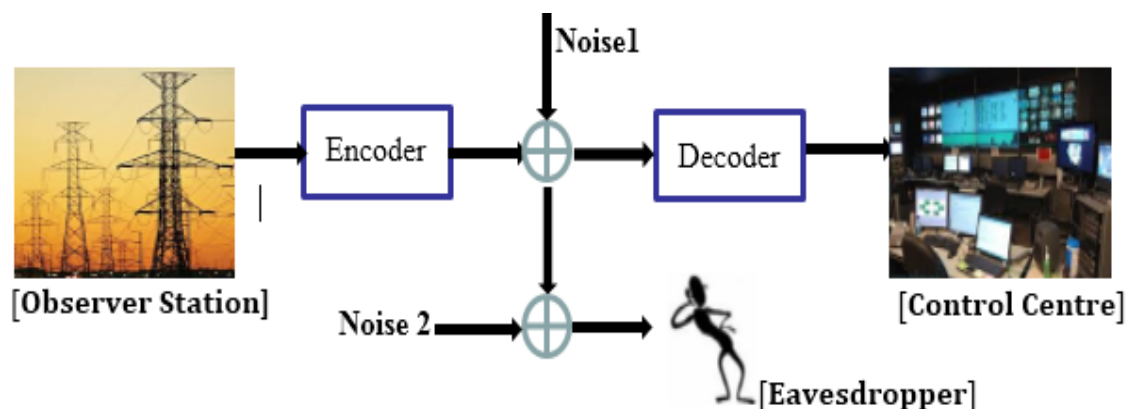


FIGURE 2. SMART GRID MODEL

System State : Represent Observation Station

Noise 1 & 2 : Represent Gaussian Noise

Channel : Wireless link

**Observer Station:** In simplicity the SG model consider a single observer station out of distributed observers .The observer station consists of encoder and sensor. Here sensor measure and send the load information (power, current, voltage...etc.) to the encoder in different time slot with continuous manner. This information with specific time is treated as system state. The binary sequence state is encoded into bit string or code using suitable technique. The derived code of system state is then communicated to control center through wireless media.

**Wireless Channel:** Here we consider wireless medium as information could conveyed through multi hop mesh network. The open nature of the wireless network has raised issues of confidentiality and security of transmitted information. The transmitted channel symbols are contaminated by noise (hostile jamming signal or interference). Information security and protection is an important issue. Wireless links prone to eavesdropping attacks. To prevent from adversary's effect we use direct sequence spread spectrum technique for unassailable and reliable communication for system state estimation.

**Control Center:** Here control center receive the contaminated code from distributed observer and recover the original system state. Then it execute the corresponding system state for monitoring and supervise the system.

**Eavesdropper:** In SG model eavesdropper act as malicious node or intruder. The malicious node keep potential to decode the confidential information of ongoing broadcast communication as the network is wireless sensor networks (WSNs). Here an eavesdropper used for cross checking whether information leaked or not and also used as an intentional jammer for testing purpose. If information is leaked during transmission then eavesdropper use information and break the stability of the system.

## 2.3 SYSTEM MODEL OF SMART GRID

The system model of the smart grid consists of two part

- System Dynamics
- Communication Link

### 2.3.1 SYSTEM DYNAMICS

For simplicity, we consider a discrete time system with an N-dimensional system state. Here time is divided into numbers of time slots for the smart grid. The dynamics of smart grid model is given [14] below

$$X(t+1) = F[x(t), w(t)]$$

Where

$X(t)$  = System state at the time  $t$

$W(t)$  = Random variable

$F$  = Mapping the previous state to next state

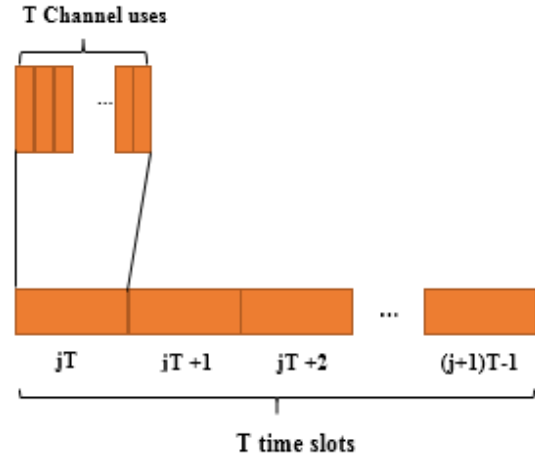


FIGURE 3. TIMING STRUCTURE OF SMART GRID MODEL

### 2.3.2 COMMUNICATION LINKS

In communication link [14] observation sensor can send a coded message about the state vector every  $T$  time slots, denoted by  $m(jT)$  at time slot  $jT$ . When the control centre receives a message at time slot  $jT$ , it will decode the message for further processing.

The coding function at sensor at time slot  $jT$  are given below

$$m_n(jT) = \mathcal{E}_n(x_n(1), \dots, x_n(jT))$$

$n$  = number of sensors

The decoding function at controller at time slot  $jT$  are given below

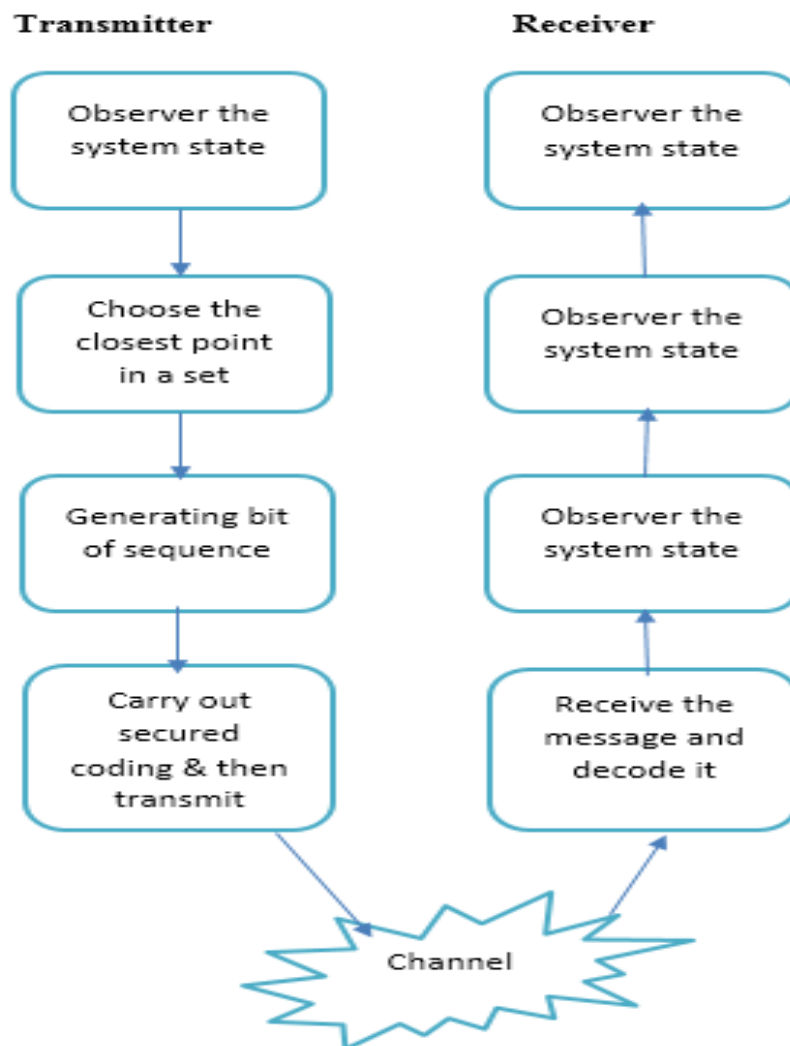
$$x((j-1)T+1), \dots, x(jT) = D(m(1), \dots, m((j-1)T))$$

The received signal at the eavesdropper is represented as

$\{z(jT)\}_{j=1,2,3,\dots}$  is the addition of signal received from source and noise.

The received signal at observation center is denoted by  $\{y(jT)\}_{j=1,2,3,\dots}$

For secure communication we prepare the coding and decoding procedure for securely receive the system state at receiver end. The coding and decoding procedure for simplified smart grid model is given below



**FIGURE 4. CODING AND DECODING PROCEDURE OF SMART GRID MODEL**

Here we use pseudo random code or scrambling code for better security purpose that generation method is discussed in chapter-4.

**Chapter Summary:** This chapter define concept of smart grid model and its different component. Also discussed about the system dynamics, communication link and coding and decoding procedure of this model in smart grid environment.

# **CHAPTER 3**

## **SECURE STATE ESTIMATION IN SMART GRID MODEL**

# 3 SECURE STATE ESTIMATION IN SMART GRID MODEL

## 3.1 SECURED COMMUNICATION FOR DYNAMIC SYSTEMS

In information theoretic approach we establish a limit on the rate (bit/sec) and security metric for secure communication of state information in dynamic system. The below figure 5 of smart grid model [14] describe

$s^k$  = Source Output

$X^N$  = Encoder Output

$Y = X + N_1$

$Z = X + N_1 + N_2$

$Z^k$  = Eavesdropper output

$N_1 \sim N(0, \sigma_0^2)$  = Noise with zero mean at wireless channel

$N_2 \sim N(0, \sigma_e^2)$  = Noise with zero mean at eavesdropper end

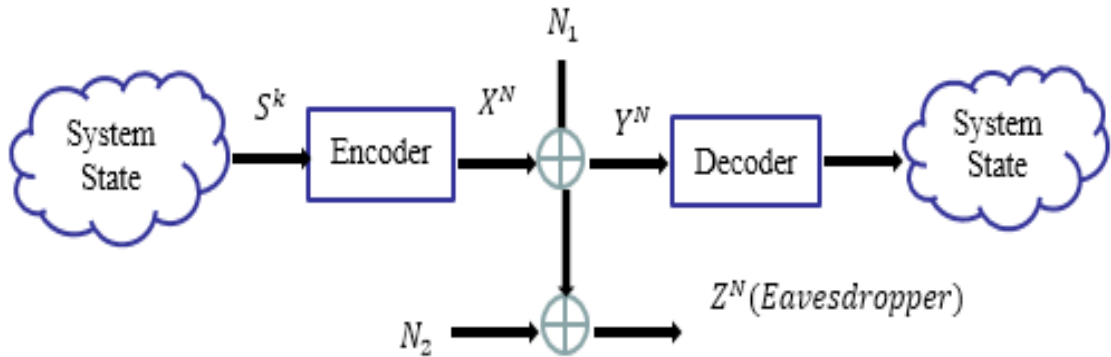


FIGURE 5. SIMPLIFIED SMART GRID DYNAMIC MODEL

If source of information is ergodic one and denoted by  $S$ , then security metric is defined as normalized equivocation is given by [15]

$$\Delta = \frac{H(S^k|Z^N)}{H(S^k)}$$

= residual uncertainty about the message at the eavesdropper

$$= \begin{cases} 0 & \text{no secrecy} \\ 1 & \text{perfect secrecy} \end{cases}$$

For ergodic finite-length alphabet source  $\Delta = \frac{H(S^k|Z^N)}{H(S^k)}$

Normalised equivocation  $\Delta$  need to modify as:

1. Smart grid is dynamic system, information might not be ergodic.
2. Source of alphabet is continuous nature in dynamic smart grid model.

Tools required to modify the normalised equivocation  $\Delta$  for smart grid dynamic system is given below

- Topological Entropy.
- Spanning Set

### 3.1.1 TOPOLOGICAL ENTROPY

It measures the uncertainty of the dynamic System. Representation of topological entropy in discrete system [1] is defined as

$$H(F, \mathcal{X}) = \lim_{\varepsilon \rightarrow 0} \lim_{k \rightarrow \infty} \frac{1}{k} \log q(k, \varepsilon)$$

$H(F, \mathcal{X})$  = is the uncertainty of the dynamic system

$F$  = Mapping function of the dynamics of smart grid

$\mathcal{X}$  = Alphabet of the state vector

$k$  = Arbitrary time slot

$$\log q(k, \varepsilon) =$$

No's of bit to describe an approximation ( $\varepsilon$ ) of system dynamic behavior during time  $k$  slots.

Also entropy represents in power system state in linear differential equation in continuous time domain is given by

$$H(A) = \sum_{i=1}^4 \log_2(\max\{1, |\lambda_i|\})$$

$A$  = Known Matrix

$\lambda_i$  = Eigen Values of matrix  $i = 1,2,3,4$

### 3.1.2 SPANNING SET

$X_k$  = Set of all possible  $\{x_1 \dots \dots x_k\}$  generated by the dynamic system

$$x(t+1) = F[x(t), w(t)]$$

**Definition: (k, ε)-Spanning Set [3]:**

For  $k > 0, \epsilon > 0$ , a finite set  $Q \subset X_k$  is  $(k, \epsilon)$  spanning set if for any  $x \in X_k$ , we can always find an  $\hat{x} \in Q$ , s. t.  $\|x(t) - \hat{x}(t)\|_\infty < \epsilon, t = 1, \dots, k$ .

For ergodic finite-length alphabet source  $\Delta = \frac{H(S^k|Z^N)}{H(S^k)}$

Using topological entropy:  $H(S^k) \rightarrow H(F, \mathcal{X})$

Using  $(k, \epsilon)$ -spanning set:  $H(S^k|Z^N) \rightarrow H(F, (\mathcal{X}|Z))$

For a smart grid dynamic system:  $\Delta = \frac{H(F, (\mathcal{X}|Z))}{H(F, \mathcal{X})}$

If communication between sensors and controller satisfy  $\Delta = 1$  then communication is secure.

### 3.1.3 CAPACITY REQUIREMENT FOR STATE ESTIMATION

Secrecy capacity [20] of the smart grid model is given below

$$\begin{aligned} C_s &= C_1 - C_2 \\ &= \log\left(1 - \frac{P}{\sigma_0^2}\right) - \log\left(1 - \frac{P}{\sigma_0^2 + \sigma_e^2}\right) \end{aligned}$$

Where

$P$  = Transmitter power

$C_1$  and  $C_2$  = Capacity of main channel and eavesdropper channel

$N_2 \sim N(0, \sigma_e^2)$  = Noise with zero mean at eavesdropper end

The following point concluded from security matrix of smart grid dynamic model

- If  $H(F, X) \leq C_1 - C_2$ , reliable and secure communication is guaranteed.
- If  $H(F, X) < C_1 - C_2$ , only reliable communication is guaranteed.
- If  $H(F, X) > C_1 - C_2$ , neither reliable communication nor security is guaranteed.

## 3.2 SYSTEM STATE ESTIMATION

We referred Alvarado model [4], [6] for the power market system to estimate system state. In this model system state contain four variable:

$P_g$ : The amount of generated power.

$P_d$ : The amount of consumed power.

$E$ : Integral difference between generated power and consumed power

$\lambda$ : The price of unit power

In the continuous time domain, the system state satisfies the following dynamics

$$\dot{P}_g = \frac{\lambda - b_g - c_g P_g - kE}{\tau_g}$$

$$\dot{P}_d = \frac{b_d + c_d P_d - \lambda}{\tau_d}$$

$$\dot{E} = P_g - P_d$$

$$\dot{\lambda} = -\frac{E}{\tau_\lambda}$$

Where

$C_g$  = Increasing rate of Cost rate w.r.t Generated Power

$C_d$  = Increasing rate of Benefit w.r.t Consumed Power

$E$  = Accumulated Energy Error

$b_g - c_g P_g$  = Marginal cost of producing  $P_g$  per unit power.

$b_d + c_d P_d$  = Marginal benefit of consuming  $P_d$  per unit power.

$C_g > 0$  = Producer wish to sell more power when price increases.

$C_d < 0$  = Consumption decreases as price of power increases.

$\tau_g, \tau_d$  and  $\tau_\lambda$  are time constants of supply, demand and price change due to market.

The interpretation of the equations are given below

1. The rate of expansion of supplier proportional to difference between observed price and actual production cost. Means generator act in a way that tends to increase production when market prices ( $\lambda$ ) exceed its production marginal costs ( $\lambda_{gi}$ ) for supplier i.
2. Consumers act in such a way that tends to increase the consumption when marginal benefits exceed price. The speed of expansion is consumer dependent and characterized by a time constant  $\tau_d$ .
3. Since it is not possible to balance supply and consumption at any time, any discrepancy accumulates as an energy error. Store energy is the integral of power imbalances.
4. The result of excess energy is the reduction in the system price with time constant  $\tau_\lambda$ . This reduction in the system price increase the consumption and decreases the production that leading to decrease in the excess energy.

The above equation can be written as in matrix in balance form

$$\begin{pmatrix} -\frac{c_g}{\tau_g} & 0 & \frac{k}{\tau_g} & \frac{1}{\tau_g} \\ 0 & \frac{c_d}{\tau_d} & 0 & -\frac{1}{\tau_d} \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -\frac{1}{\tau_\lambda} & 0 \end{pmatrix} \begin{pmatrix} P_g \\ P_d \\ E \\ \lambda \end{pmatrix} + \begin{pmatrix} -\frac{b_g}{\tau_g} \\ \frac{b_d}{\tau_d} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$\Delta t =$  A very small interval time

$$X(t+1) = A x(t) + b$$

$$A = \Delta t \begin{pmatrix} -\frac{c_g}{\tau_g} & 0 & \frac{k}{\tau_g} & \frac{1}{\tau_g} \\ 0 & \frac{c_d}{\tau_d} & 0 & -\frac{1}{\tau_d} \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -\frac{1}{\tau_\lambda} & 0 \end{pmatrix}$$

$$\mathbf{b} = \Delta t \begin{pmatrix} -\frac{b_g}{\tau_g} & \frac{b_d}{\tau_d} & 0 & 0 \end{pmatrix}^T$$

And the system state is given by

$$\mathbf{x} = (P_g \ P_d \ E \ \lambda)^T$$

### 3.2.1 SECURE STATE ESTIMATION

The following cases acknowledge the channel capacity requirement [20] for the simplified smart grid model when matrix A is reachable and stable

**Case 1 :- (  $\mathbf{b} = \mathbf{b}_g = \mathbf{b}_d = \mathbf{0}$  )**

When matrix A is stable means absolute value of all Eigen value  $< 1$

$H(A) = 0 =$  requiring zero channel capacity.

If matrix A is not stable then

$H(A) \neq 0 =$  requires non zero channel capacity.

**Case 2:- (  $\mathbf{b} = \mathbf{b}_g = \mathbf{b}_d \neq \mathbf{0}$  )**

$H(A) = \infty$

This means we can't calculate system state in communication channel with a finite capacity. The system state estimation cannot be achieved, it does not mean that the system state can no longer be estimated in practice. It only means that the estimation error is high. Hence if we reduce estimation error i.e. very small, then it applicable to practical systems.

### 3.3 DEFULT SETUP

The default setup value [14] is

$$\Delta t = 1, \tau_g = 0.2, C_g = 0.1$$

$$C_d = -0.2, \tau_d = 0.2$$

$$\tau_\lambda = 100, k = 0.1$$

$$b_g = b_d = 0.$$

The topological entropy is computed using equation is given below

$$H(A) = \sum_{i=1}^4 \log_2(\max\{1, |\lambda_i|\})$$

A = Known Matrix

$\lambda_i$  = Eigen Values of matrix  $i = 1, 2, 3, 4$

#### 3.3.1 SIMULATION RESULT AND CONCLUSION

The impact of different parameter on channel capacity requirement for reliable and secure state estimation through MATLAB software is given below

##### A. IMPACTS OF $C_g$ and $C_d$

###### I. Large value of $C_g$ and $C_d$

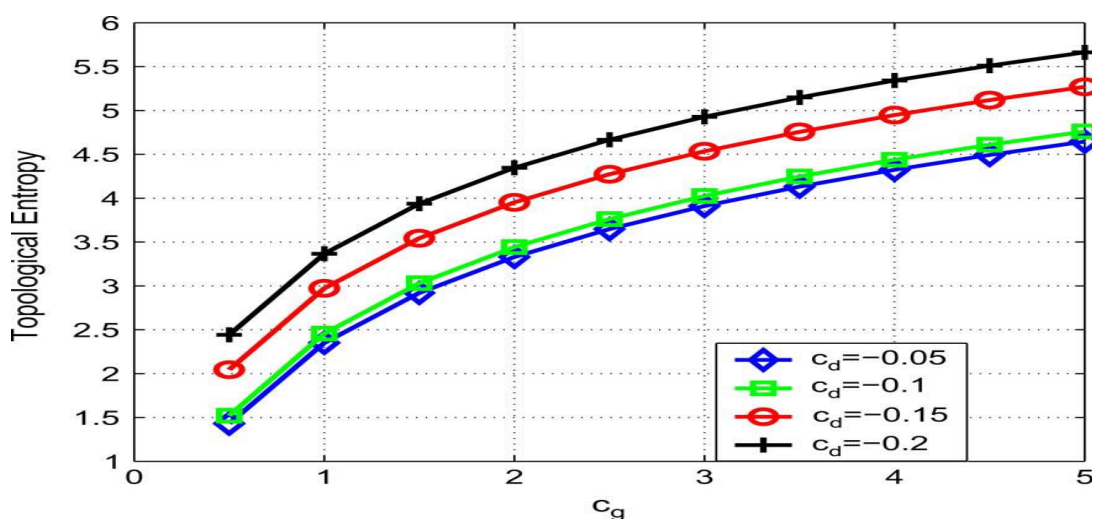


FIGURE 6. TOPOLOGICAL ENTROPY VS. LARGE VALUE OF  $C_g$  AND  $C_d$  [14]

## II. Small value of $C_g$ and $C_d$

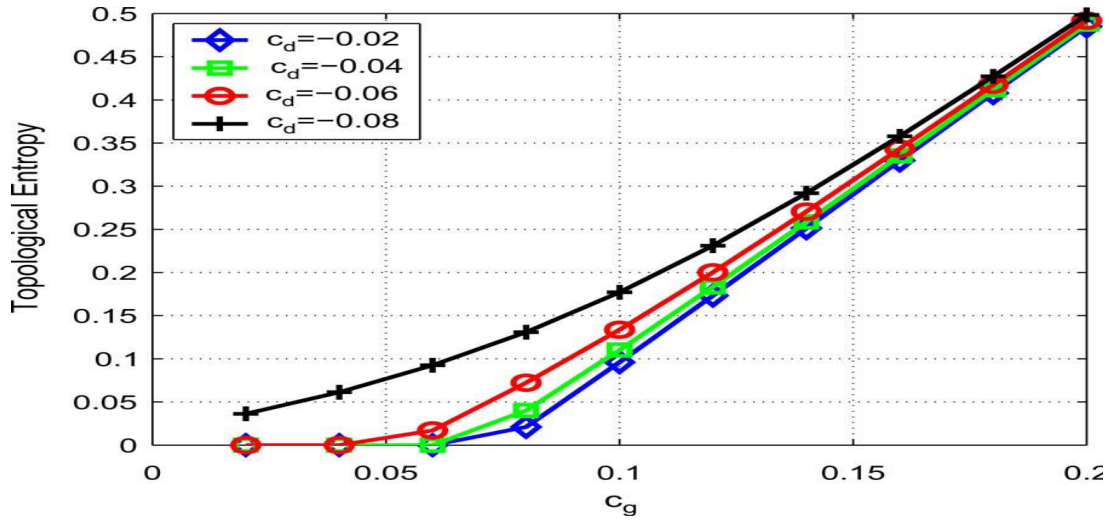


FIGURE 7. TOPOLOGICAL ENTROPY VS. SMALL VALUE OF  $C_g$  AND  $C_d$  [14]

**Result:** The communication requirement increases with large values of  $C_g$  &  $C_d$  as well as decreases with small value of  $C_g$  &  $C_d$ .

**Remark:** This simulation depicts that the information rate is improved when the rates of cost and benefit are increased.

### B. IMPACT OF $\tau_g$ and $\tau_d$ :

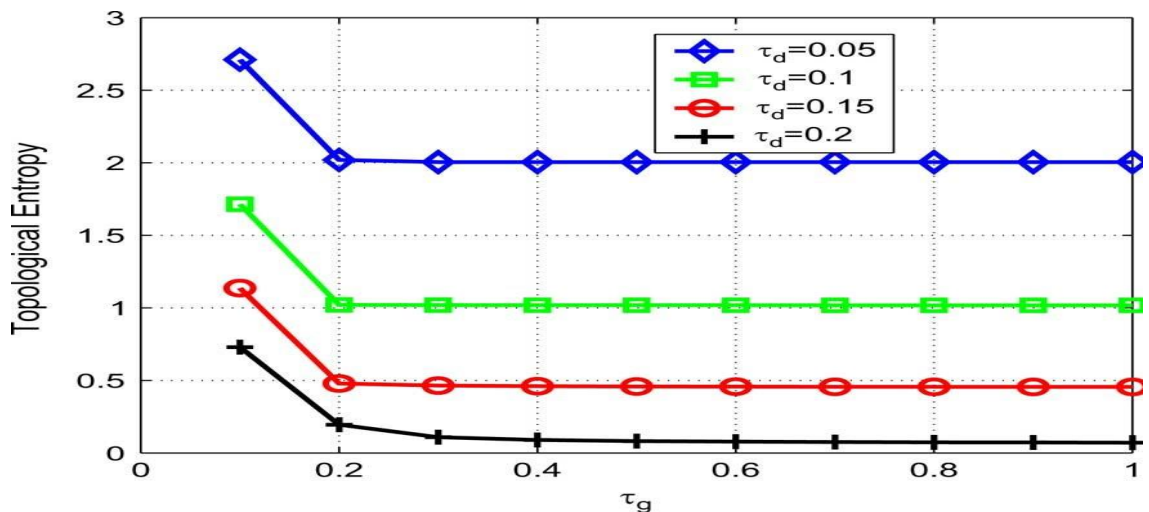
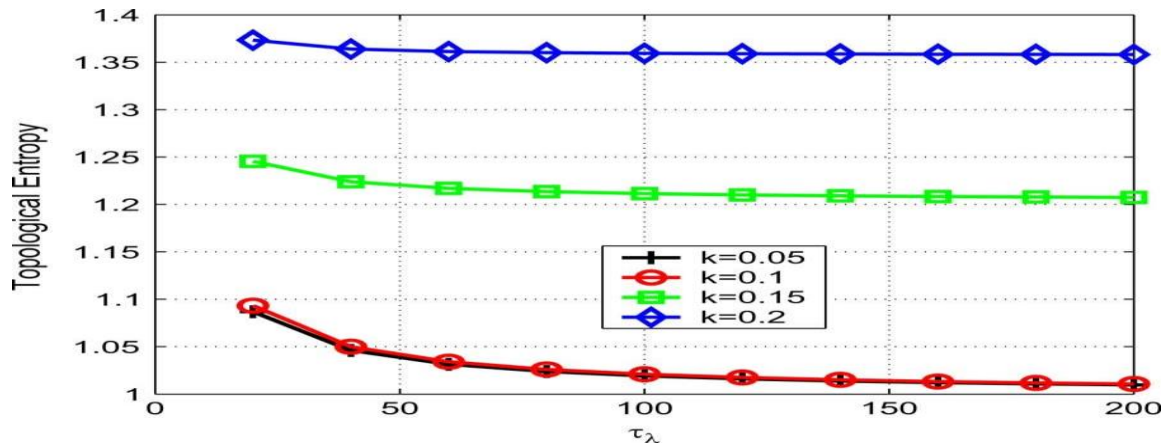


FIGURE 7. TOPOLOGICAL ENTROPY VS.  $\tau_g$  AND  $\tau_d$  [20]

**Result:** Topological entropy decreases with  $\tau_g$  and  $\tau_d$ . This means increase the response time make the system less dynamics. Thus become easier to estimate the system state.

**C. IMPACT OF  $\tau_\lambda$  and  $k$ :**

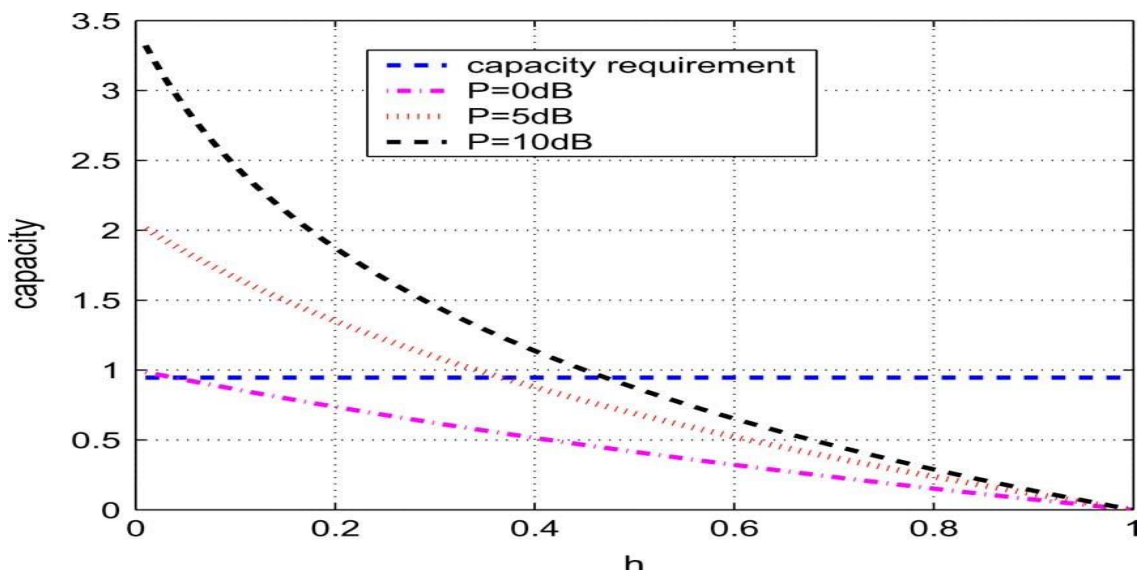


**FIGURE 8. TOPOLOGICAL ENTROPY VS.  $\tau_\lambda$  AND  $k$  [20]**

**Result:** The communication rate increases with  $k$  that add more dynamic factor to the system. But decreases with  $\tau_\lambda$ .

**D. SECRECY CAPACITY IN WIRELESS CHANNEL:**

Parameter: Power = 0dB, 5dB, 10dB,  $C_s = C_1 - C_2 = \log(1 + p) - \log\left(1 + \frac{hp}{1+h}\right)$



**FIGURE 9. SECRECY CAPACITY VS. GAIN AT DIFFERENT POWER LEVEL [14]**

**Result:** Secrecy of channel capacity is decreased rapidly when channel gain to the eavesdropper ( $h$ ) is increased.

**Chapter Summary:** The transmission of system state information require some channel capacity. Also with increase the strength of eavesdropper the secrecy capacity of channel is sharply decreases means information is completely lost during transmission.

# **CHAPTER 4**

## **SECURE TRANSMISSION OF ESTIMATED SYSTEM STATE IN SMART GRID MODEL**

# 4 SECURE TRANSMISSION OF ESTIMATED SYSTEM STATE IN SMART GRID MODEL

---

## 4.1 INTRODUCTION

Information security and protection is an important issue. The open nature of the wireless network has raised issues of confidentiality and security of transmitted information. Pricing information and control actions are transmitted via the information network. Various attacks such as eavesdropping, information tampering, and malicious control command injection would impose serious threat on secure and stable smart grids operation.

### OBJECTIVE OF CHAPTER:

Preserve privacy and securely transmit system state information to the destination in smart grid model.

### 4.1.1 ATTACK IN WIRELESS NETWORK

In wireless sensor networks (WSNs) serious security threat is eavesdropping attack. So eavesdropping means any wireless node residing in the transmission range of the transmitter can potentially decode the signal when both transmitter and receiver are unaware of the reconnaissance. In smart grid wireless links prone to eavesdropping attacks.

**Passive Eavesdropping:** Here intruder or malicious nodes listening on going communication in the broadcasting wireless medium and capture confidential information or modified the pattern of traffic .

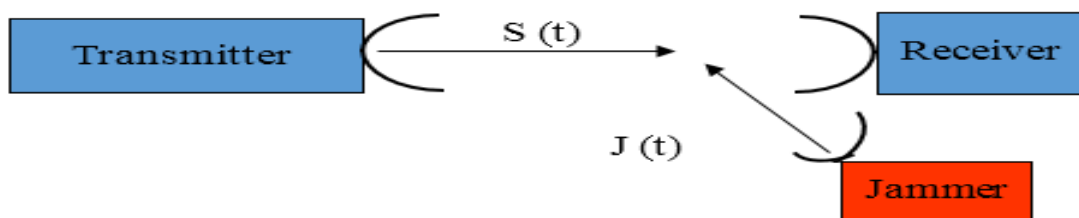


FIGURE 10. EAVESDROPPER ATTACK IN WIRELESS MEDIUM

**Active Eavesdropping:** Here malicious nodes actively grab the information or congesting the network via sending queries to transmitters by disguising themselves as friendly nodes.

## 4.1.2 SECURITY ISSUE

**Confidentiality** - The information only understood to whom it was proposed.

**Integrity** - The information cannot be changed during transition and storage between sender and intended receiver.

**Non-repudiation** – The service that provides proof of integrity and origin of data means sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

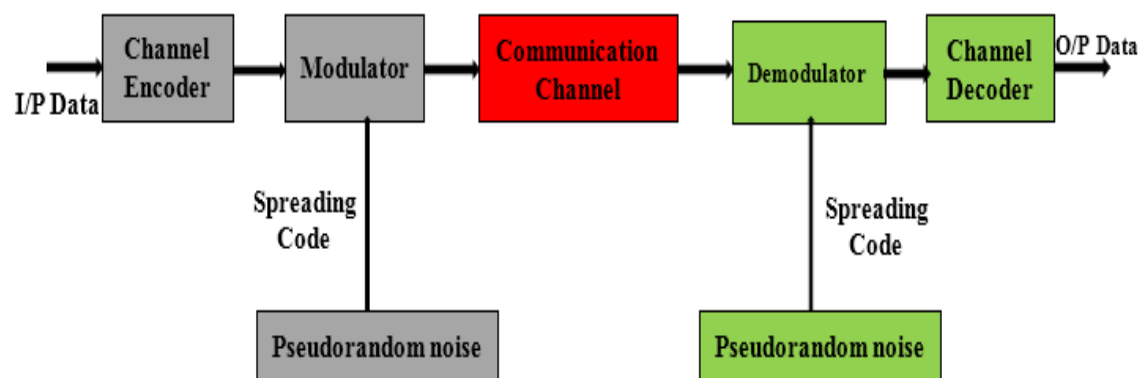
**Authentication** - The sender and receiver can confirm each other's identity and the origin/destination of the information.

To prevent from security issues and vulnerabilities (majorly jamming and eavesdropping) in wireless network we adopt spread spectrum technology.

## 4.2 SPREAD SPECTRUM (SS)

It is a signal transmission [9] technique where

- At transmitter use data independent random sequence (PN Sequence) to spread a narrow band information signal over a wideband of frequency.



**FIGURE 11. SPREAD SPECTRUM COMMUNICATION IN SIMPLIFIED SMART GRID MODEL**

- At receiver end, despreading is done by correlating the received SS signal with a synchronized receiver copy of spreading code (PN Sequence).

- Spectrum is spreading by means of spreading code or Pseudo noise code.

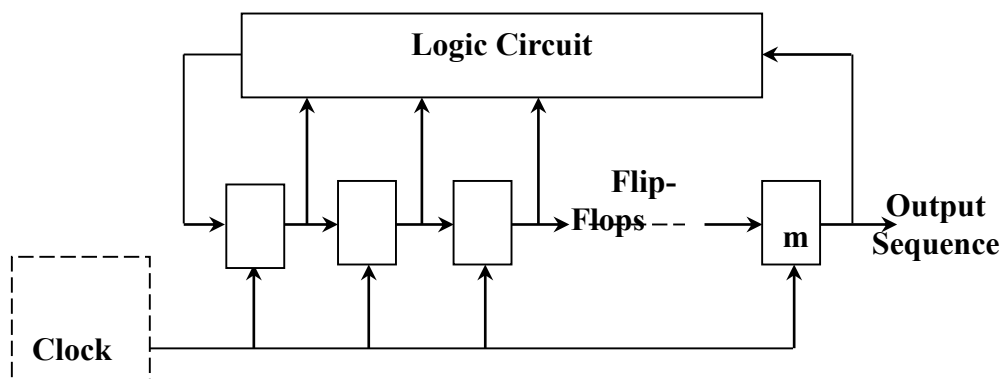
**Advantages:** The below reasons are the main factor to adopt spread spectrum technique in smart grid model is given below

- Remove hostile jamming as well as unintentional interference.
- Lowers probability of intercept because it's spread over larger bandwidth, making detection harder because signal is likely below the noise level.
- Protect the signal against eavesdropping so increases the privacy of the signal.
- Provides good resistance from multipath signal and multiple accesses (Communication resource sharing with privacy).
- Operating distance range is longer due its non-interfering nature.
- Hard to intercept or demodulate because code use to spread the signal.

The key factor in spread spectrum technique is generation of pseudo noise code or scrambling code for secure communication in wireless network.

#### 4.2.1 PN SEQUENCE CODE GENERATOR

PN sequence is a periodic binary sequence with a noise like waveform generated by means of a linear feedback shift register (LFSR). It consists of a shift register made up of  $m$  flip-flops and logic circuit to form multi loop feedback circuit.



**FIGURE 12. LINEAR FEEDBACK SHIFT REGISTER**

The maximum length sequence is  $(2^m-1)$  chips, where  $m$  is the number of stages in the shift register. This code is also called as scrambling code or chipping code that divides the data according to spreading ratio. The bit rate of code is also called as chip rate. This chip rate is always higher than information rate.

For  $m = 5$  register =  $2^5-1 = 31$

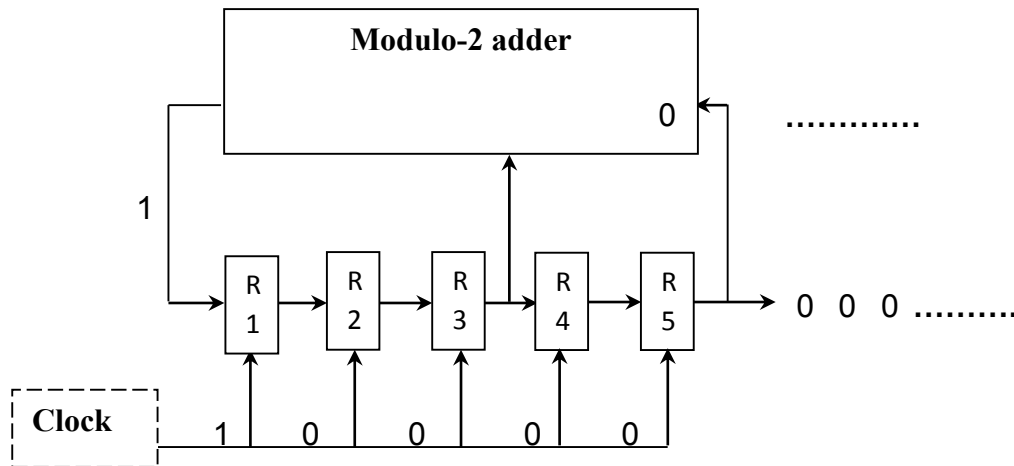


FIGURE 13. LINEAR FEEDBACK SHIFT REGISTER FOR  $M=5$

PN Sequence = 0000100101100111110001101110101.

PN codes utilised in a spread-spectrum system for:

- **Protect against noise:** The processing gain increases the code length as well as bandwidth and signal likely transmit below the noise level that protect against interfering signal.
- **Provision for privacy:** The code protect the signal against eavesdropping so increases the privacy of the signal.

#### 4.2.2 PROCESSING GAIN IN SPREAD SPECTRUM

It is the ratio of bandwidth of spreaded signal to original signal. Spread spectrum increases BW of message signal by a factor  $N$ . It describe unique property of spread spectrum waveform.

$$\text{Processing gain (N)} = \frac{\text{Bandwidth of spreaded signal}}{\text{Bandwidth of orginal signal}} = 10 \log_{10} \frac{\text{bandwidth of spreaded signal}}{\text{bandwidth of orginal signal}}$$

## 4.2.2 TYPES OF SPREAD SPECTRUM

Spread spectrum technology are of two types

- **DIRECT SEQUENCE SPREAD SPECTRUM(DSSS)**

The carrier of the direct-sequence signal stays at a fixed frequency. Narrowband information is spread out into a much larger (at least 5 times) bandwidth by using a pseudo-random chip sequence.

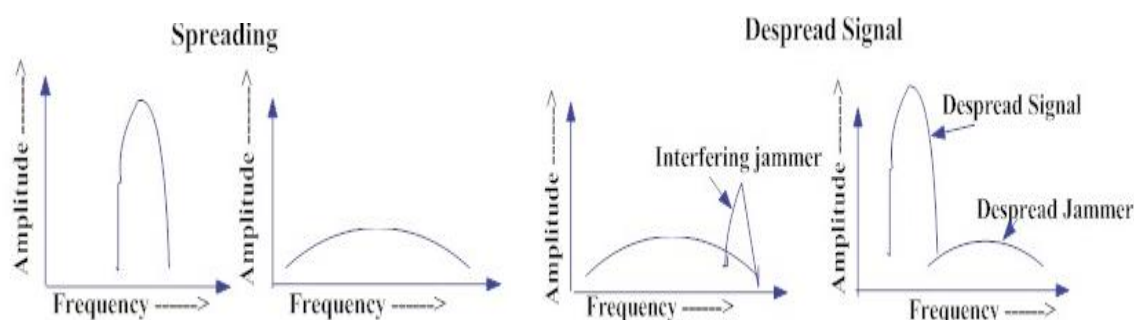


FIGURE 14. SPREADING AND DE-SPREADING SIGNAL IN DSSS

- **FREQUENCY HOPPING SPREAD SPECTRUM(FSSS)**

The FSSS systems obtain the same output provided by direct-sequence systems by using different carrier frequency at different time. The frequency-hop system's carrier will hop around within the band so that hopefully it will avoid the jammer at some frequencies. The frequency-hopping technique does not spread the signal, as a result, there is no processing gain.

In this thesis we use direct sequence spread spectrum technique as performance is better and reliable because of the below reason

### **Synchronisation problem:**

The frequency hopping the transmitter and receiver must be synchronised with time and frequency where as in DSSS only timing of chips need to be is synchronise.

### **Latency issue:**

In DSSS signal can grip the PN sequence in just a few bits where as in FH-SS needs more time to search the signal and lock to it. As a result, the latency time is usually longer.

### 4.2.3 DIRECT SEQUENCE SPREAD SPECTRUM WITH BPSK

Direct sequence spread spectrum (DSSS) is a transmission technology used in local area wireless network transmissions. In this technology, a data signal at the sending station is combined with a high data rate bit sequence, which divides user data based on a spreading ratio. This term is also known as direct sequence code division multiple access (DS-CDMA).

#### Mathematical analysis of DSSS with BPSK:

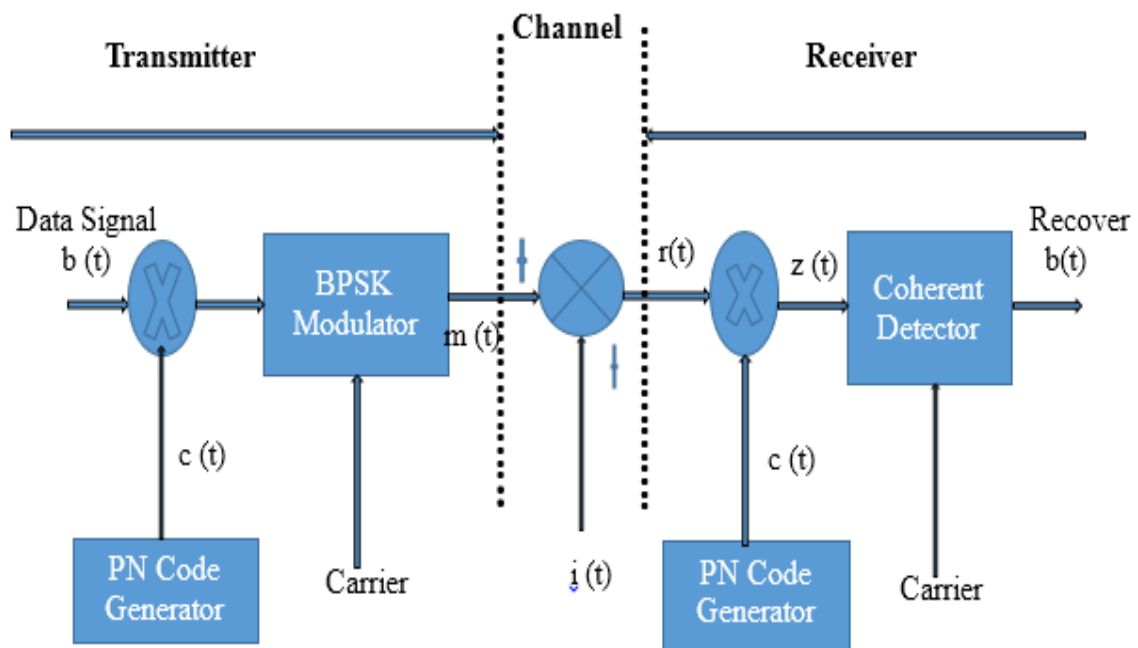


FIGURE 15. MODEL OF A DIRECT-SEQUENCE SPREAD BPSK SYSTEM

Input data signal represent :  $b(t)$

PN code :  $c(t)$

Noise signal :  $i(t)$

Carrier Signal :  $A \cos 2\pi f_c t = \sqrt{\frac{2E_b}{T_b}} \cos 2\pi f_c t$

Energy bit per Second :  $E_b$

Time per bit of message sequence :  $T_b$

The transmitter output is given by :  $m(t) = b(t)c(t)\left(\sqrt{\frac{2E_b}{T_b}} \cos 2\pi f_c t\right)$

The channel output is given by :  $r(t) = m(t) + i(t)$

$$= b(t)c(t)\left(\sqrt{\frac{2E_b}{T_b}} \cos 2\pi f_c t\right) + i(t)$$

The receiver i/p is given by :  $z(t) = r(t)c(t)$

$$= [m(t) + i(t)]c(t)$$

$$= b(t)c^2(t)\left(\sqrt{\frac{2E_b}{T_b}} \cos 2\pi f_c t\right) + i(t)c(t)$$

$$= b(t) + i(t)c(t), \quad c(t) \times c(t) = 1, \forall t$$

The original signal ( $b(t)$ ) recover through balance demodulator at coherent detector block used at receiver end and noise signal is spreaded by PN sequence  $c(t)$ . We applied this technology in our simplified smart grid dynamic model and verified the simulation result for single observer as well as multiple observer case in MAT lab software.

### 4.3 SIMULATION RESULT OF SMART GRID MODEL USING SINGLE OBSERVER

We have verified the simulation result in simplified smart grid model for single observer case using direct sequence spread spectrum technique through MATLAB software by following steps

- Simulated wave form at transmitter end
- Simulated wave form at wireless channel
- Simulated wave form at input to the receiver end
- Simulated wave form at receiver output

The parameter taken for simulation in single observer case is given below

Carrier frequency ( $F_c$ ) = 1.2MHz

Energy per bit ( $E_b$ ) = 2.

Time per bit of message sequence ( $T_b$ ) = 1.

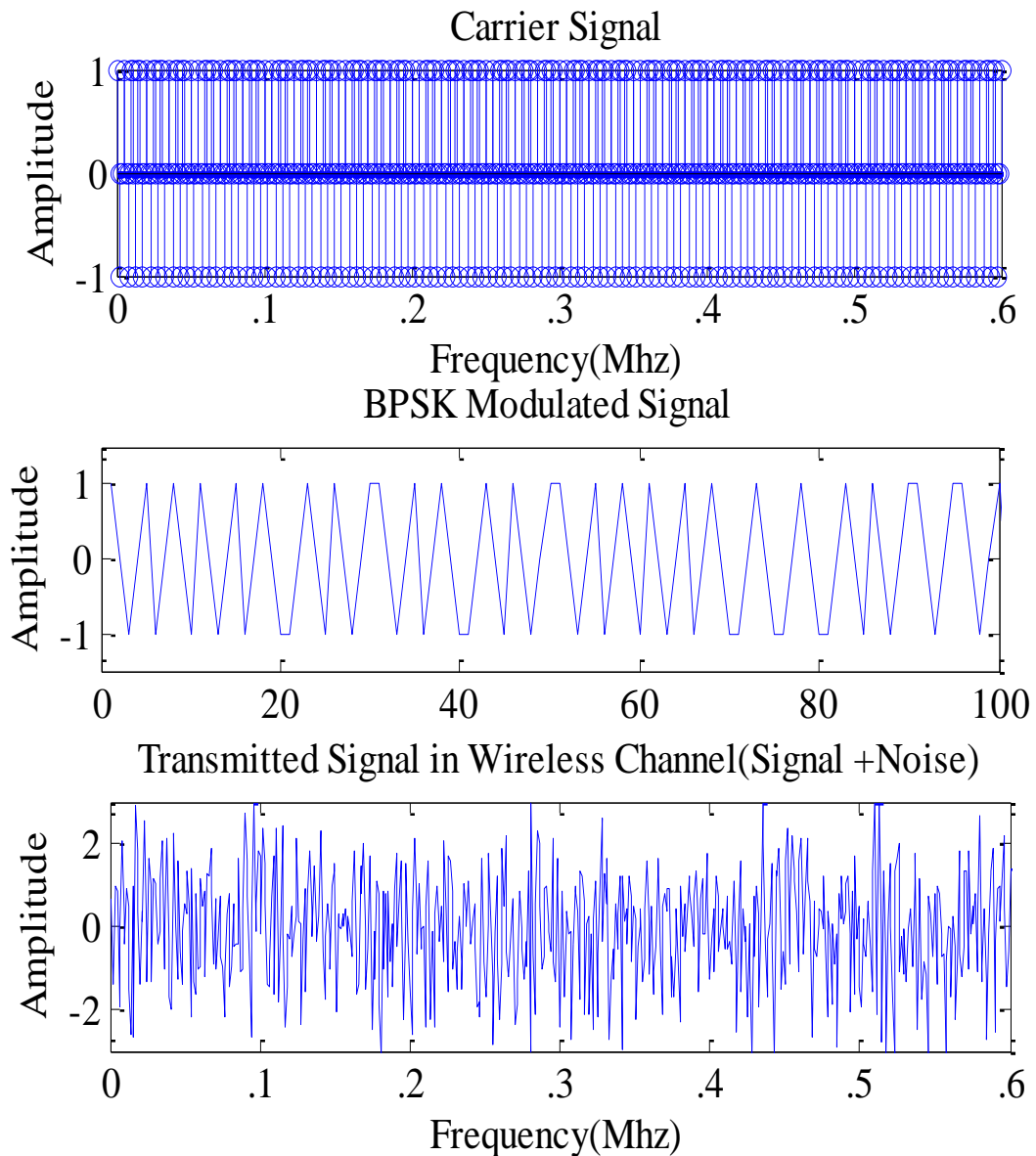
Processing gain ( $N$ ) = 10

Signal to noise ratio (SNR) = 10 dB



### 4.3.2 SIMULATED WAVE FORM AT WIRELESS CHANNEL

As per below simulated figure , we generate a carrier wave having frequency 1.2MHz and verified the changes in BPSK modulated output signal i.e. phase shift during 0 degree and 180 degree taking small samples .

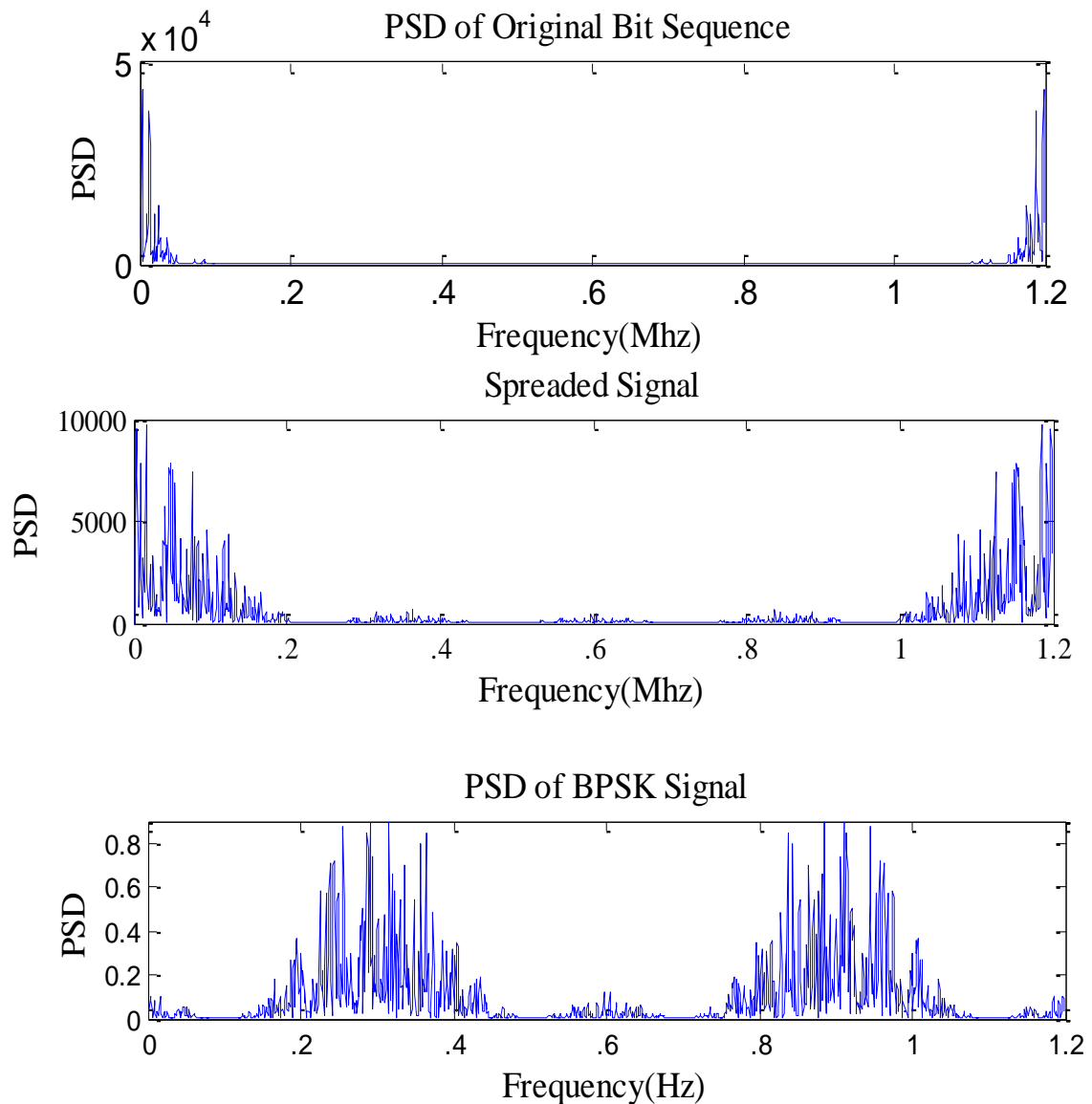


**FIGURE 19. WAVEFORM OF CARRIER SIGNAL, BPSK MODULATED SIGNAL AND TRANSMITTED SIGNAL (SIGNAL + NOISE (SNR=-10DB)) AT WIRELESS CHANNEL.**

**Result:** The transmitter output is contaminated by noise signal in wireless medium is verified through MATLAB simulation.

### 4.3.3 SIMULATED FREQUENCY RESPONSE AT TRANSMITTER END

The simulated frequency response of original bit sequence, spreaded signal and output of BPSK (Spreaded signal.\*Carrier) signal where frequency in MHz in X-axis and signal in Power spectral density (PSD) in Y-axis is shown below.



**FIGURE 20. WAVEFORM OF FREQUENCY RESPONSE OF ORIGINAL SIGNAL, SPREADED SIGNAL AND BPSK MODULATOR OUTPUT SIGNAL AT TRANSMITTER END.**

**Result:** The simulated result verified that the power spectral density of spreaded signal is less in compared to original signal because original signal is spreaded over wide frequency after multiply with PN sequence.

#### 4.3.4 SIMULATED WAVE FORM AT RECEIVER INPUT

##### Description:

The contaminated output of transmitter signal is received at receiver or control centre of smart grid model and then modulated or multiplied with the replica of synchronised pseudo noise sequence then

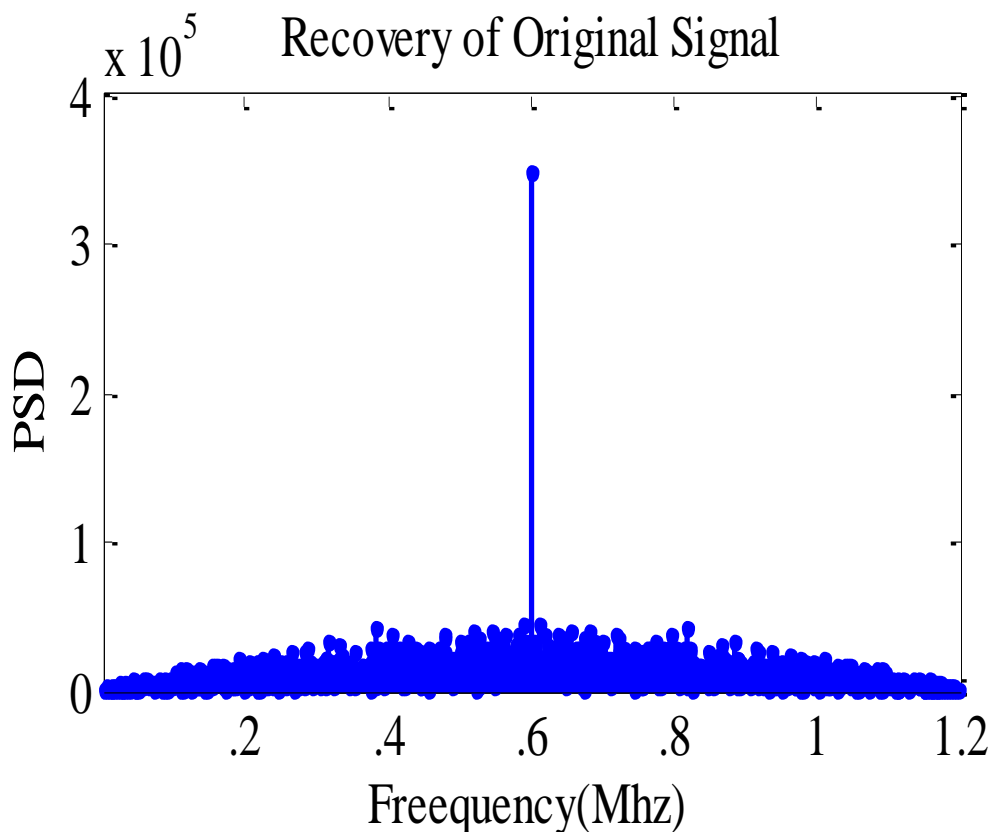


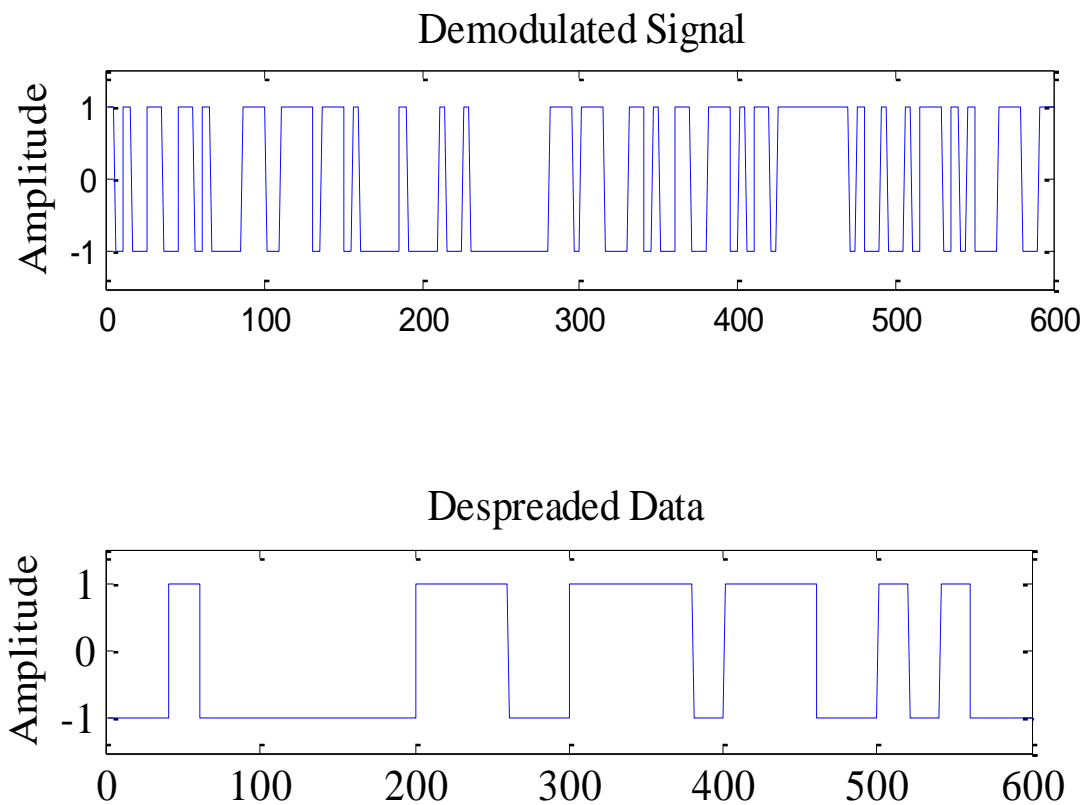
FIGURE 21. WAVEFORM OF DE-SPREAD SIGNAL WITH NOISE AT RECEIVER END

##### Result :

The simulation result shows the noisy transmitted signal received at receiver end that multiply with the replica of PN sequence and isolate the original signal and noise signal. The noise signal become spreaded below the noise power spectral density that is verified in MATLAB simulation.

### 4.3.5 RECEIVER OUTPUT OBTAINED FROM SIMULATION

**Description :** The isolated original signal is input to integrator (or low pass filter) and recover the original signal by demodulation and decision device [1 volt if  $v > 0$ , & -1 if  $v < 0$ ] and reject the interference is verified through MATLAB simulation as given below result .



**FIGURE 22. WAVEFORM OF DEMODULATED AND DE-SPREADED DATA WITHOUT NOISE AT RECEIVER END**

**Analysis:**

At receiver or control centre of smart grid model get error free observer input data successfully.

**Conclusion:**

Actual transmitted signal received at receiver side without error in real time that verified using direct sequence spread spectrum (DSSS) technology in simplified smart grid model for single observer case through MATLAB simulation.

#### 4.4 SIMULATION RESULT OF SMART GRID MODEL USING MULTIPLE OBSERVER

The parameter taken for simulation of multiple observer case is given below

$$\text{Observer1} = [1 \ 0 \ 0 \ 1 \ 1 \ 0]$$

$$\text{Observer2} = [1 \ 1 \ 0 \ 1 \ 0 \ 0]$$

$$\text{Carrier frequency ( } F_c) = 1\text{MHz}$$

$$\text{Energy per bit ( } E_b) = 32$$

$$\text{Time per bit of message sequence ( } T_b) = 1$$

$$\text{Processing gain ( } N) = 10$$

$$\text{Signal to noise ratio (SNR) = 10 dB}$$

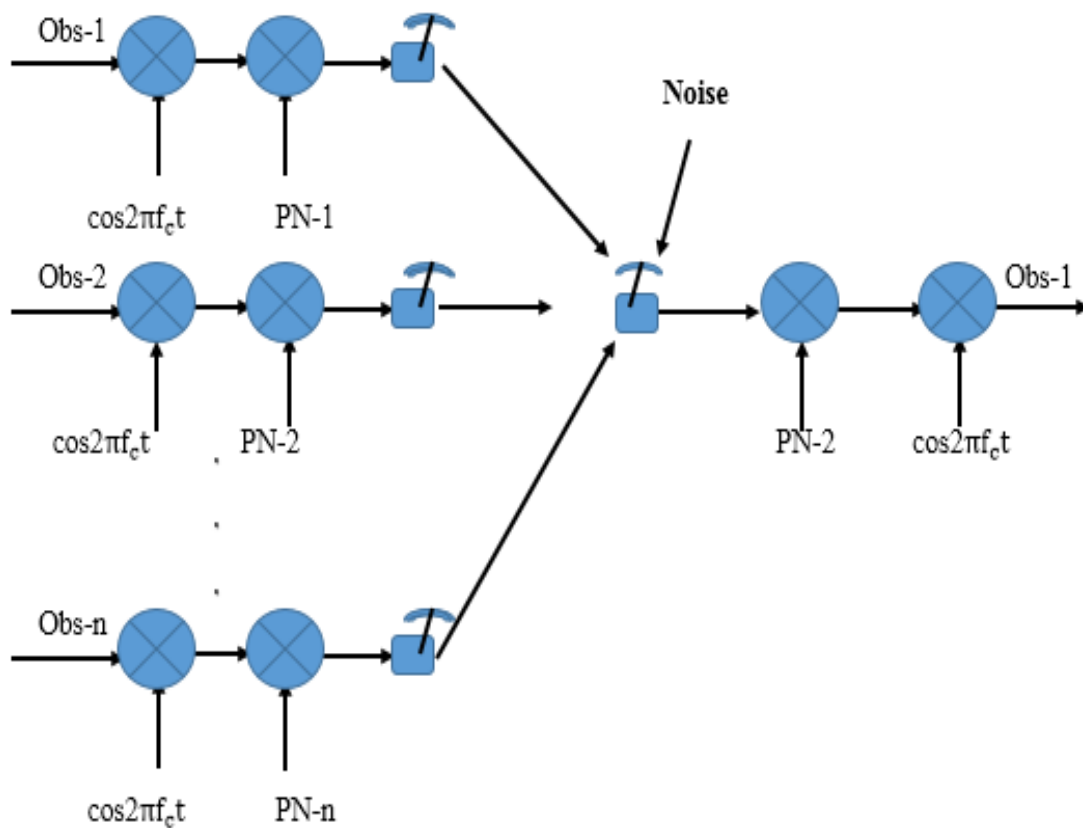
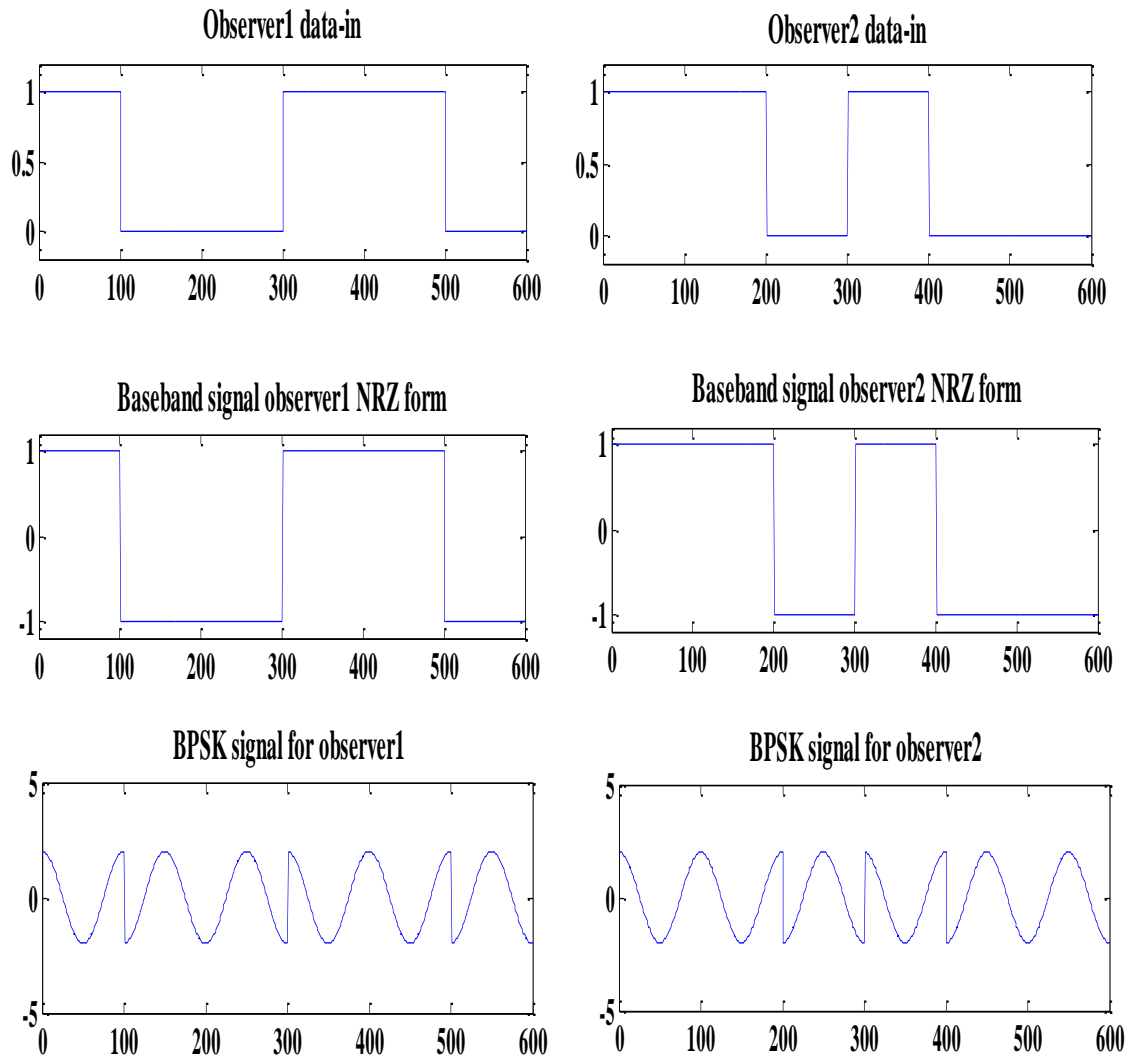


FIGURE 23. MULTIPLE OBSERVER IN SIMPLIFIED SMART GRID MODEL

#### 4.4.1 SIMULATED WAVE FORM AT TRANSMITTER END

**Description:** Here we take two input bit stream for observer-1[1 0 0 1 1 0] and observer-2[1 1 0 1 0 0] and convert to non-return to zero (NRZ) format (1 is consider as = +1volt and 0 is consider as = -1volt) and BPSK modulation is done for propagation of the signal.



**FIGURE 24. WAVE FORM OF INPUT SIGNAL, NRZ FORM OF INPUT SIGNAL AND BPSK MODULATOR OUTPUT SIGNAL OF OBSERVER1 AND OBSERVER2 AT TRANSMITTER END**

#### **Result:**

The simulation result of input signal, NRZ form of input signal and BPSK signal of observer1 and observer2 is verified.

## 4.4.2 PN SEQUENCE GENERATION AT TRANSMITTER END

**Description:** We generate two different pseudo noise sequence to scramble the input data of observer means multiply BPSK modulated input sequence to PN sequence of observer-1 and observer-2 respectively. The simulated PN sequence and spreaded signal of observer1 and observer2 is given below

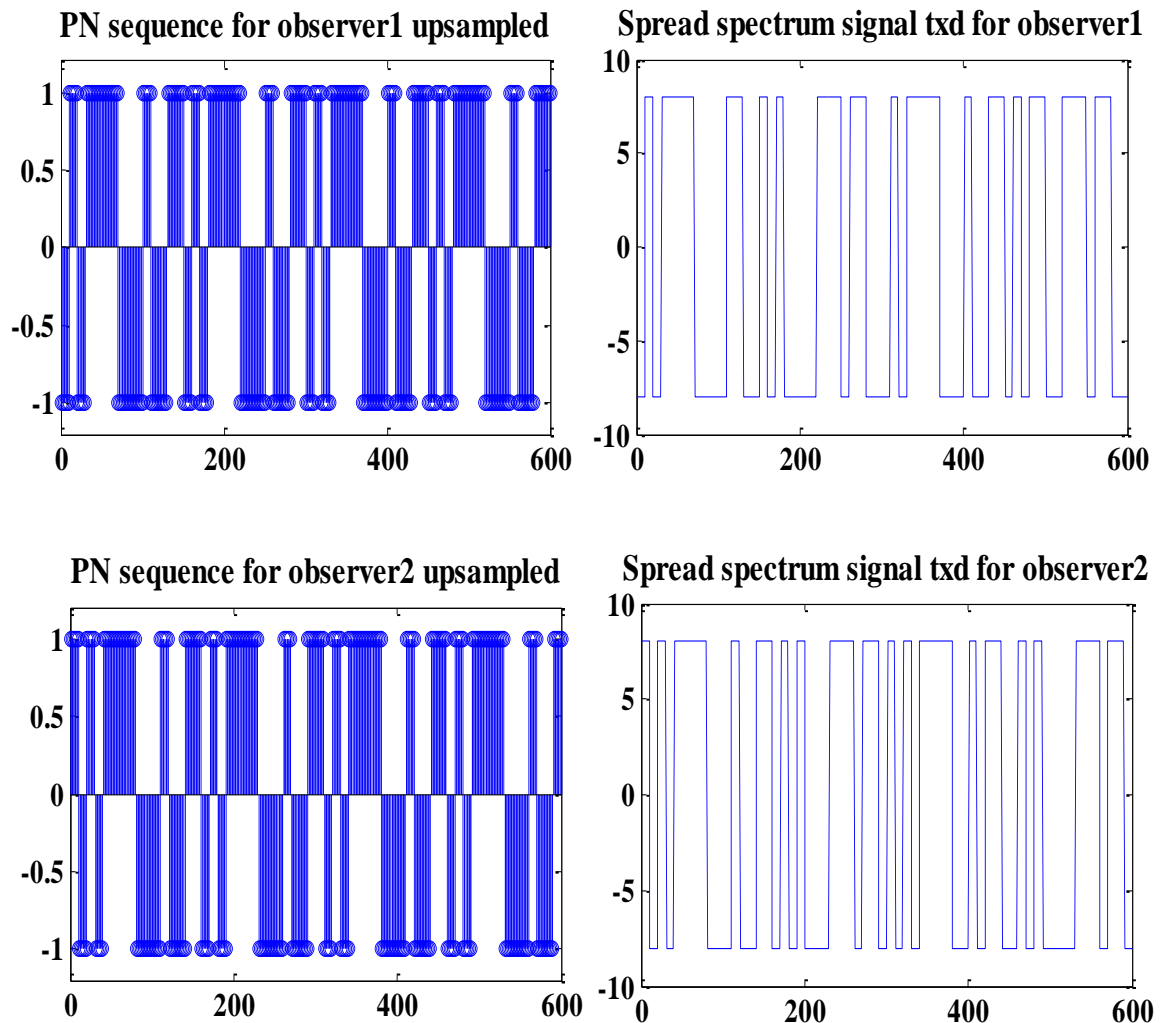


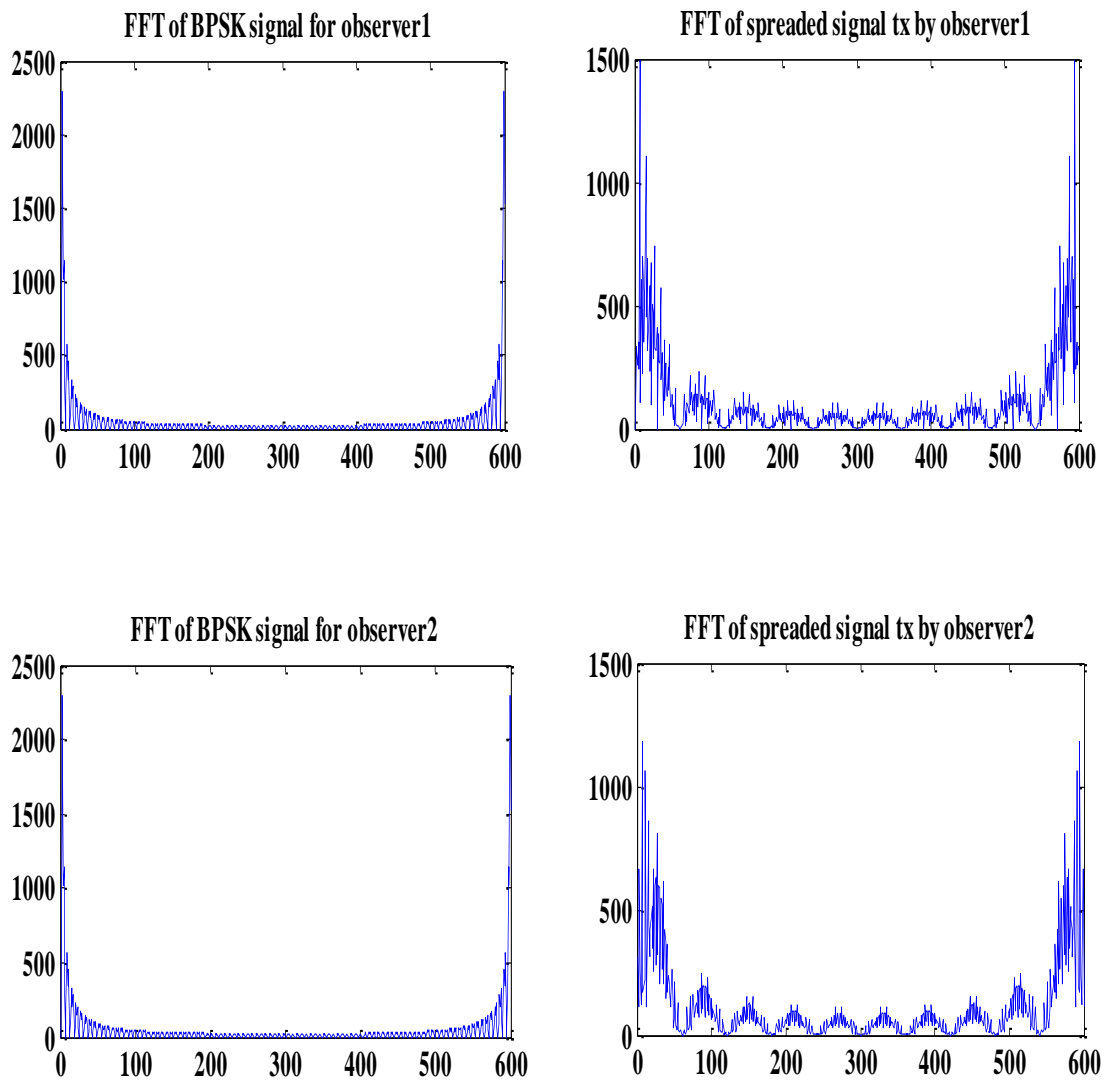
FIGURE 25. WAVE FORM OF PN SEQUENCE AND SPREADED SIGNAL OF OBSERVER1 AND OBSERVER2

### Result:

We analysis that after multiply the PN sequence to the input streams or narrow band information get spreaded over wide band of frequency and difficult to detect the signal information.

### 4.4.3 FREQUENCY RESPONSE AT TRANSMITTER END

**Description:** The simulated result of frequency response of original signal and spreaded signal of observer1 and observer2 respectively where power spectral density taken in y-axis and samples per bit in x-axis is shown below.



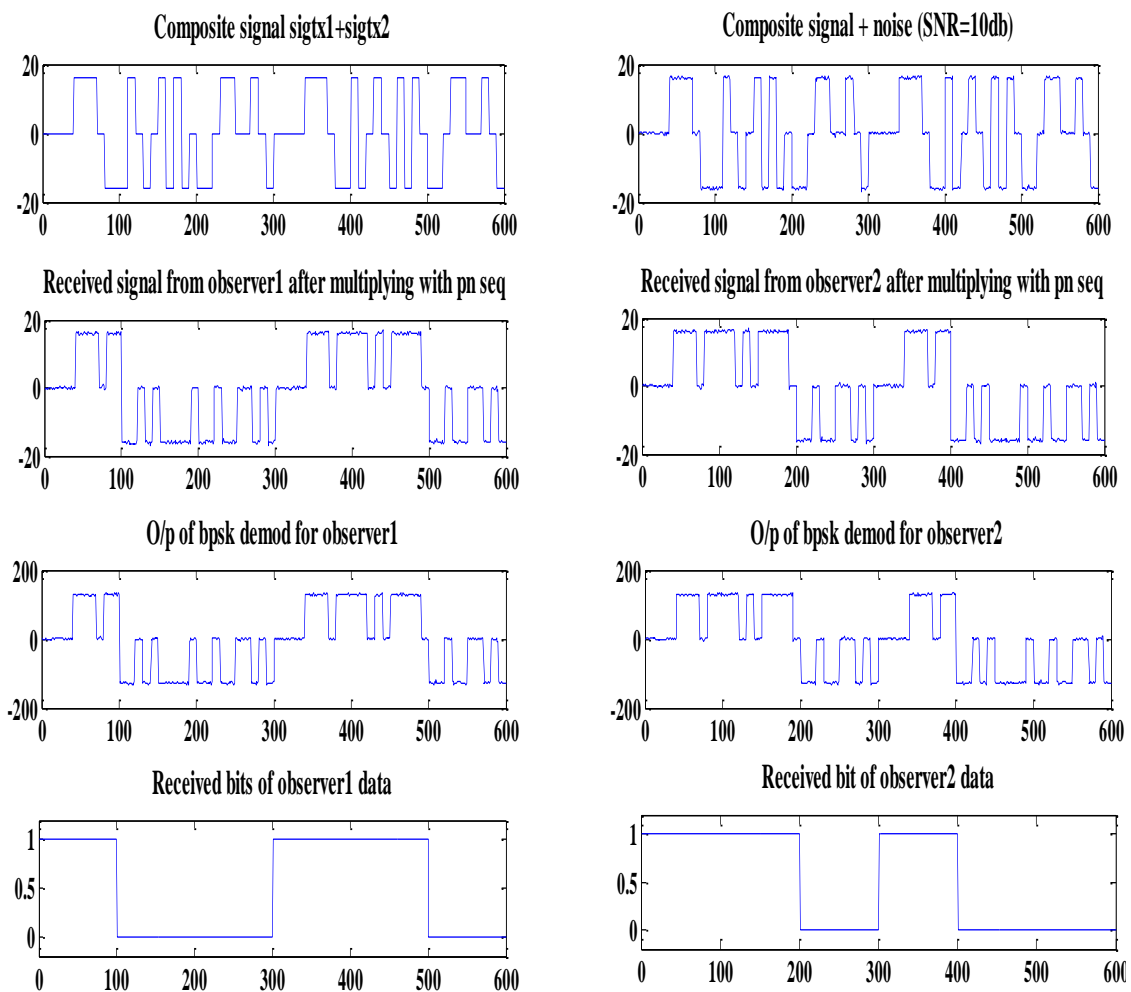
**FIGURE 26. WAVEFORM OF FREQUENCY RESPONSE OF ORIGINAL SIGNAL AND SPREADED SIGNAL OF OBSERVER1 AND OBSERVER2 AT TRANSMITTER END.**

**Result:**

From simulation result we analysed that power spectral density of spreaded signal is lower than the original signal.

#### 4.4.4 WAVE FORM OF WIRELESS CHANNEL & RECEIVER O/P OBTAINED FROM SIMULATION

**Description:** At transmitter output we get composite signal i.e. mixture of observer-1 and observer-2 input data and add noise to it. Then contaminated composite signal is multiplied respective synchronised PN sequence and demodulate the output of BPSK signal. The simulated waveform of contaminated wireless channel and receiver end signal is given below



**FIGURE 27. WAVEFORM OF COMPOSITE SIGNAL, COMPOSITE SIGNAL WITH NOISE, O/P OF DEMODULATED BPSK SIGNAL AND RECEIVED BIT SEQUENCE OBSERVER1 AND OBSERVER2 AT RECEIVER END.**

**Analysis:** The contaminated mixture signal of multiple observer is easily isolated using PN sequence at receiver end i.e. Code division multiple access property is proved.

**Chapter Summary:** Actual transmitted signal received at receiver end or control centre of SG model without error for multiple observer is verified using DSSS technology through MAT lab simulation.

# **CHAPTER 5**

## **CONCLUSION AND SCOPE FOR FUTURE WORK**

# 5 CONCLUSION AND SCOPE FOR FUTURE WORK

---

## 5.1 CONCLUSION

To resolve communication issue as well as privacy of the system state information in dynamic system a simplified SG model is studied where control centre and sensors are communicated through wireless channel. In this thesis general dynamics of power market system and spread spectrum technique are applied in SG model and draw the below conclusion

- Implemented the numerical values of general dynamic of power system market in SG model and result shown that the transmission of system state information require some channel capacity and the secrecy capacity of channel is sharply decreases with increase the strength of eavesdropper means information is completely lost during transmission.
- Implemented spread spectrum technique in SG model for secure communication and found that the pseudo random bit sequence protect from interference as well as maintain the privacy of system state information by reducing their spectral power density i.e. likely below the noise power spectral density.
- Result from MATLAB simulation shows that the system state information is securely received at receiver end in real time manner in case of single and multiple observer system in presence of eavesdropper using DSSS in SG model.

This study will help to power engineers to supervise and control the system.

## 5.2 SCOPE FOR FUTURE WORK

- Research can be carried out for performance of DSSS in presence of different type of jamming signal and calculate bit error rate (BER) in real time manner.
- There are different other kinds of attack that can be performed against the state estimation model that will need to be researched.

## REFERENCES

- [1]. P. M. Anderson and A. A. Fouad, Power System Control and Stability, 2nd ed. New York: IEEE Press and Wiley-Inter science, 2003.
- [2]. Smart Grid Working Group (2003–06), “Challenge and opportunity: Charting a new energy future,” Working Group Reports, 2008.
- [3]. S. Matveev and A. V. Savkin, Estimation and Control Over Communication Networks. Basel, Switzerland: Birkhauser, 2009.
- [4]. J. Nutaro and V. Protopopescu, “The impact of market clearing time and price signal delay on the stability of electric power markets,” IEEE Trans. Power Syst., vol. 24, pp. 1337–1345, Aug. 2009.
- [5]. T. S. Rappaport “Wireless Communications principle and practice”, second edition, prentice-Hall, Inc., 2000.
- [6]. F. L. Alvarado, The Dynamics of Power System Markets, Dept. Elect. Comput. Eng., Univ. Wisconsin, Madison, WI, Tech. Rep. PSERC-91-01, Mar. 1997.
- [7]. “Multi-Carrier and Spread Spectrum Systems”, 2nd edition K.Fazel & S.Kasier.
- [8]. R.C. Dixon “Spread Spectrum System”, 2nd edition JOHN WILEY and SONS.
- [9]. B. P. Lathi “Modern Digital and Analog Communication Systems”, Oxford University Press 1998.
- [10]. Y. Liang, H. V. Poor and S. Shamai, Information Theoretic Security, Now Publishers Inc., 2009.

- [11]. K. Moslehi and R. Kumar, "Smart grid - A reliability perspective," in Proc. of IEEE Innovative Smart Grid Technologies Conference (ISGT), 2010.
- [12]. V. C. Gungor, B. Lu, and G. P. Hancke , "Opportunities and challenges of wireless sensor networks in smart grid, "IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.
- [13]. Li, Husheng , Li feng Lai , and Robert C.Qiu " Communication Requirement for Reliable and Secure State Estimation and Control in Smart Grid ", "IEEE Trans. Ind. Electron., vol.2, no. 3,Spt. 2011.
- [14]. Communications Requirements of Smart Grid Technologies. Washington, DC: Dept. Energy, 2010.
- [15]. X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation", 3rd International Conference on Signal Processing and Communication Systems, pp. 1–5, Sep. 2009.
- [16]. L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," in 2010 first IEEE International Conference on Smart Grid Communications, 2010, pp. 226-231.
- [17]. G. Dan and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," in 2010 First IEEE International Conference on Smart Grid Communications, 2010, pp. 214-219.
- [18]. Li, Husheng , Li feng Lai , and Robert C.Qiu " Communication Capacity Requirement for Reliable and Secure State Estimation in Smart Grid ",in 2010 first IEEE International Conference on Smart Grid Communications.