International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

INVESTIGATION OF FALSE DATA INJECTION IN SMART GRID TO MINIMIZE THE SECURITY RISKS IN AGC

S.Shanthi[1], N.Loganathan[2]

[1] *PG student, Department of Electrical and Electronics Engineering, K.S.Rangasamy College of Technology, Tamil Nadu, India*
[2] *Professor, Department of Electrical and Electronics Engineering, K.S.Rangasamy College of Technology, Tamil Nadu, India*

Abstract- ***In smart grid, when the false data is injected to electronic monitoring system, the AGC will directly affects and potentially leads to blackouts. The main objective of this paper is to examine the attacks due to injection of false data in smart grid for the purpose of minimizing the risks in AGC. In the previous research, the Intrusion Detection System was used, in which they implemented Intrusion Detection Algorithm for the grid security system. But this method can't be employed often due to mathematical complexity and difficulty in practical implementation. This paper presents a Game-Theory based method for the security of smart grid by relating the quantifiable risk managing techniques with decision making for protective measures. The significances of the injected data attacks are computed using risk assessment process. The calculated risks are then unified into the stochastic (Markov) security game classic as input parameters. The decisions of protective measures are attained by resolving the game using dynamic programming approach which considers the resource constraints. The Nash equilibrium results are used to acquire the Game Matrix. The simulation result indicates that the different risk events will leads to different security approaches. The attacker-defender interaction and the AGC risk minimization are validated through extensive simulation results using MATLAB/SIMULINK.***

Key Words: *False Data Injection (FDI), Smart grid security, Automatic Generation Control (AGC), Game theory*

1. INTRODUCTION

AGC is an essential part of the central nervous system of a power network called the Energy Management System (EMS), and possibly the only spontaneous closed loop between the Information Technology (IT) and power system of a control area; due to these reason, it is subject to attacks broadcasted through the IT system. The commonly found attacks are in the form of false data instillation [1]. If these false data are not detected instantly, they may affect the AGC and may lead to blackouts. Thus the detection of false data injection is necessary to maintain the stability and secure operation of the grid. Traditionally, network security solutions employ either protective devices such as firewalls or reactive devices such as Intrusion Detection Systems (IDSs) and both of them are used in conjunction [2]-[3]. And many detection algorithms were used. But in case of those conventional techniques, many drawbacks are there because of which, the false data injected in smart grid may not be detected efficiently, which may affects the performance of the AGC.

The power grid, on which most economic activities rely, is a Critical organization that must be protected against potential dangers. Advanced monitoring technologies at the center of smart grid progression increase its efficiency but also make it more vulnerable to mean attacks such as injection of false data [4]-[6]. While security is an important issue for grid operators, real-world limitations such as resource limitations necessarily force assumption of a risk management approach to the problem rather than complete elimination of all prospective threats.

As the number of contact points increase, compared with traditional power grids, smart grids are more disposed to to cyber-attacks. Among these attacks, the most serious attack is False Data Injection (FDI). When the false data injection is done in the smart metering system, the performance of the AGC will get affected and may lead to the blackout. To detect these false data injection in the smart grid, many detection techniques are there. The security game theory is one of those method used for minimizing the security risks in AGC [7]-[9]. The foundation of rich mathematical is provided by the field of game theory, which enables validating the intentional struggle between attackers and defenders for the control of the smart grid. Using the risk background and some of the concepts of earlier studies, this project work applies theory of game to the enhancement of attacks and

defenses for the critical power system component, Automatic Generation Control (AGC) [10]-[13]. In game theory model, there will be a number of players for performing the attacks and defense actions. By performing this Game theory approach, we can detect the false data injection in the smart grid and can minimize the security risks in AGC.

2. AGC IN POWER GRID

In an interconnected power system, as the load varies, the frequency and tie-line power interchange also vary. The basic function of AGC is to split up the loads among the system, station and generator to achieve maximum efficiency of economy and precise control of the programmed interchanges of tie-line power while keeping a reasonably uniform frequency. An interconnected power system can be deliberated as being divided into control areas which are interconnected by tie lines. In each control area, all generator sets are considered to form a intelligible group. A control signal made up of tie line flow deviation added to frequency deviation biased by a bias factor would achieve the desired objective. When the false data is injected to the grid, the frequency might get corrupted, due to which the performance of the AGC may affect and lead to the blackout.

3. ATTACKS BASED ON INJECTION OF FALSE DATA

A new and significant type of cyber-attacks in contradiction of smart grids' wide area measurement systems has newly been referred as false data injection attacks. In an attack due to the false data injection, an opponent aims to hack the interpretations of multiple sensors and Phasor Measurement Units (PMUs) to deceive smart grid's decision making process.

The main aim of these types of attacks is to compromise the measurements and readings from smart grid metering system and the phasor measurement units in order to deceive the operation of the control centers. Recent revisions have shown that if an opponent has complete information on the power grid topology and transmission-line admittance values, he can modify the injection of false data attack vector such that the attack remains unnoticed and it successfully permits the residue-based test for bad data detection that are usually used in power system state estimation.

3.1 Injection of False Data against State Estimation

We established the least-exertion attack prototype, which proficiently classifies the optimum set of meters to takeoff attacks due to injection of false data for a fixed number of state variables. We also established an exploratory algorithm to develop the results efficiently. The simple idea is listed as follows: the large power grid network is split up into a number of overlying areas; the brute-force search method is used to recognize the optimum set of meters for specific small areas and derive the optimum set of meters for the whole network.

3.2 Injection of False Data against Energy Distribution

Smart grid shall incorporate the distributed energy resources and perceptively transmit energy to meet the requests from users. The protection the distributed energy transmission and distribution process that uses the distributed energy incomes and minimizes the energy transmission overhead is serious in smart grid. Earlier we studied the susceptibility of distributed energy transmission and distribution process and explore novel injection of false data attacks against distributed energy transmission and distribution process.

Let us consider several types of illustrative attacks, in which the opponent may operate the amount of energy supply, the amount of energy response, and link status of energy transmission. The fake data injected by those outbreaks will cause unfair demand and supply, which may increase the energy distribution cost, dislocate the energy distribution causing outages in some nodes in smart grid, and even manipulating the cost of the energy price.

4. PROPOSED METHOD OF SECURITY GAME THEORY

At first we formulate the security risk assessment problem as a decision making problem and then performs the game-theoretic management, and further show how our security game based model, based on the outline in, can be implemented. By considering the state transition as Markovian, the decision making problem can be framed as a Markov decision process, considered to have the form of 4-tuple (S, A^D, M, r)

Where, $S \stackrel{def}{=} \{s_{1,\dots,}s_{N_s}\}$ is the state space of the system,

$A^D \stackrel{def}{=} \{d_1, \dots., d_{N_D}\}$ is the action space of decision maker.

$$M_{s,s'}(d) \stackrel{def}{=} Pr\{s[t+1] = s' | s[t] = s, d[t] = d\}$$

is the probability of state transition for,

$s, s' \in S$ and $d \in A^D$;

$r_d(s, s')$ is the recompense for state transition of triggering, $s \to s'$ by action $d \in A^D$.

The objective of the decision maker is to maximize the reward by performing the decision on the optimum result based policy. The effect as a result of the attack demonstrates as a change to M, which is assumed to be the correspondent to exhibiting attacks as the actions at the every stage of the "attacker" agent, which will takes an action from a given set of actions We basically define a security game as a stochastic game with the model of a finite state space, and the game consists of two players (attacker versus defender) that choose their movements from their relevant finite action space; or more formally, as a state space considered to have a form of 6-tuple $(S, A^A, A^D, M, G^A, G^D)$

Where, $S \stackrel{def}{=} \{s_{1,\dots,}s_{N_s}\}$ is the state space of the system

$A^A \stackrel{def}{=} \{a_1, \dots, a_{N_A}\}$ is the state space of the attacker.

$A^D \stackrel{def}{=} \{d_1, \dots, d_{N_D}\}$ is the state space of the defender.

$M(a, d) = [M_{s_i,s_j}(a, d)]_{N_s \times N_s}$ is the state transition matrix of the system corresponding to the action $a \in A^A$ and defense action, $d \in A^D$

The expected payoff for the given action is given by, $G^A(s) = [G^A{}_{a,d}(s)]_{N_A \times N_D}$ $a \in A^A$ against defense action $d \in A^D$ in the state of the system, $s' \in S$.

The different risk level at each state is considered. In this paper, the risk state is defined by the way as tuple $(\Delta f_1, \Delta f_2)$: generally; a tuple may consist of the frequency deviation in area 1 and the deviation in area 2. By integrating $(\Delta f_1, \Delta f_2)$, the four risk states may written as,

- State s_{00}: $-0.35 < \Delta f_1$ *and* $-0.35 < \Delta f_2$;
- State s_{00}: $-0.35 < \Delta\Delta f_1$ *and* $\Delta f_2 \leq -0.35$
- State s_{00}: $\Delta f_1 \leq -0.35$ *and* $-0.35 < \Delta f_2$;
- State s_{00}: $\Delta f_1 \leq -0.35$ *and* $\Delta f_2 \leq -0.35$;

4.1 Payoffs in Attacker and Defender

The attacker or defender sustains a net gain or loss in the each state. These gain or loss can be formulate as,

Attacker's net gain = Attacker's gain – Attacker's cost,
Defender's net loss = Defender's loss – Defender's gain
= Defender's loss

Here, we consider that the net gain of the attacker is to be very close to the net loss of the defender. Thus, the security game is considered as the zero-sum game, i.e.

Attacker's gain – Attacker's cost = Defender's loss

The defender's loss is initially estimated, which is more freely assessable from a power system perception, we can also estimate the net gain of the attacker.

With Cumulative Distribution Function (CDF), the reactive power at significance level α is,

$$VaR_\alpha(P_{shed}) \stackrel{def}{=} \inf\{F_{P_{shed}}(\varepsilon) \geq 1 - \alpha\} = F^{-1}{}_{P_{shed}}(1-\alpha) \quad (1)$$

Here, the last equality is valid only for the smooth and continuous $F_{P_{shed}}$. Arithmetically, the CVaR value at significance level α is,

$$VaR_\alpha(P_{shed}) \stackrel{def}{=} E\{P_{shed} | P_{shed} \geq VaR_\alpha(P_{shed})\} = \frac{1}{\alpha}\int_{1-\alpha}^{1} F^{-1}{}_{P_{shed}}(a)da \quad (2)$$

A false positive value refers to the situation where a protective action is in the form of a detection based on the intrusion detection algorithm which will misdiagnoses a meaningless irregularity as an attack.

The expected value of the cost of false positives is c_{fp}, p_{fp}. Where, c_{fp} is false positive cost in the same unit as in the load shed and p_{fp} is the function of the probability of attainment of a false positive. According to these assumptions, we afford two alternate definitions of $G_{a,d}(s)$,

$$G^{mean}{}_{a,d}(s) \stackrel{def}{=} E\{P_{shed}(a, d, s)\} + c_{fp}p_{fp}(a, d, s), \quad (3)$$

$$G^{CVaR}{}_{a,d}(s) \stackrel{def}{=} CVaR_\alpha(P_{shed}(a, d, s)) + c_{fp}p_{fp}(a, d, s) \quad (4)$$

The aim of a coherent attacker or defender is to maximize or minimize its estimated collective payoff,

$$\bar{Q} \stackrel{def}{\equiv} \sum_{t=0}^{\infty} \gamma^t G_{a[t],d[t]}(s[t])$$

Where, $a[t] \in A^A, d[t] \in A^D, s[t] \in S.$ (5)

As per the concept of game theory, the strategy of the attacker is given as a probability distribution given as $A^A$for a given state is,

$$p^A(s[t]) \stackrel{def}{\equiv} [\Pr\{a(s[t]) = a1\}, \ldots., \Pr\{a(s[t]) = aN_A\}]^T$$

(6)

The given problem can be computed recursively using dynamic programming to get the static optimal strategy at the each state. At stage t, the optimum cost $Q_{t+1}(a, d, s)$ is given by,

$$Q_{t+1}(a,d,s) = G_{a,d}(s) + \gamma \sum_{s' \in S} M_{a,a'}(a,d) \cdot \min_{p^D(s')} \max_{a} \sum_{d \in A^d} Q_{t+1}(a,d,s')\, p_d{}^D(s')$$

(7)

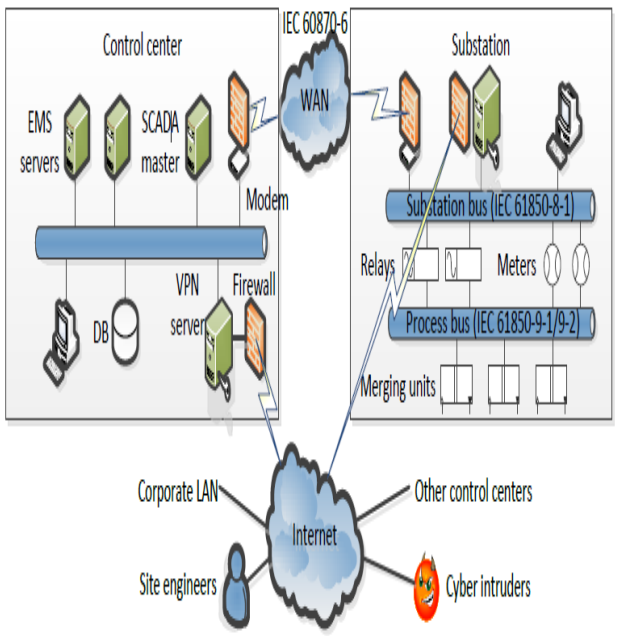

Fig-1: Ease of access of Control Center and Substation of Power System from the Internet

The value iteration algorithm is prescribed here due to its ease of computation. To describe the algorithm, we first fragment the equation (7) into the mutually recursive Bellman equations:

$$V(s) = \min_{p^D(s)} \max_{a} \sum_{d \in A^d} Q_{t+1}(a,d,s)\, p_d{}^D(s) \quad (8)$$

$$Q_{t+1}(a,d,s) = G_{a,d}(s) + \gamma \sum_{s' \in S} M_{s,s'}(a,d) V(s') \quad (9)$$

We can express (8) as a linear program:

$$\min_{p^D(s)} V(s) \text{ s.t.}$$

$$V(s) \geq \sum_{d \in A^d} Q_{t+1}(a,d,s)\, p_d{}^D(s) \quad (10)$$

$$p_d{}^D \geq 0, \sum_d p_d{}^D = 1. \quad (11)$$

The approach $p_d{}^D$ calculated from (9) is the mini max strategy. The fixed points obtained from the equations (8) and (9), (V^* and Q^*) lead to the optimum minimax solution for the defender.

4.3 Attacker – Defender Interaction Model

Figure-1 shows the architecture developed for the communication involving a control center and a substation. These are based on the standard of the international standard IEC 61850. The control center can be accessed through the control system in either the control center or the substation. This control center is enabled through a virtual private network (VPN).

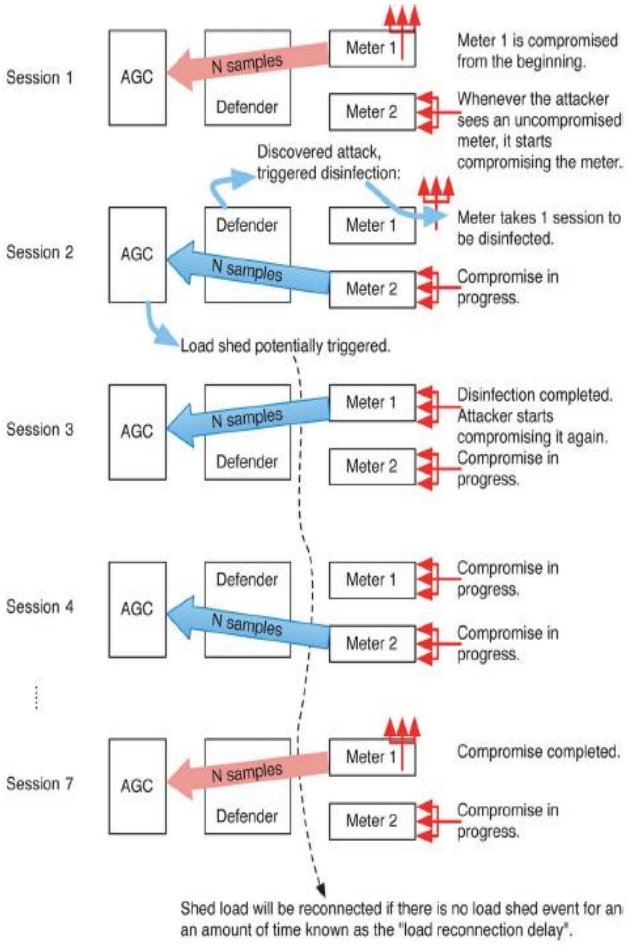

Fig-2: Sample Sessions of Attacker-Defender Interaction Model

The workflow of the simulation is carried out through the following steps:
1) First define the actions of the attack and defense;
2) Simulate interaction effect between the actions o the attacks and the actions of the defense on an AGC system, to obtain the state transition matrix $M(a,d) = \left[M_{s_i,s_j}(a,d)\right]_{N_S \times N_S}$ and the game matrix $G^A(s) = [G^A{}_{a,d}(s)]_{N_A \times N_D}$
3) Feed the observed $M(a,d)$ and $G^A(s)$ to value iteration algorithm.

Attack Actions: The chosen attack actions are:
a_1 Attack at "half power": corrupt half of the observed samples;
a_2 Attack at "full power": corrupt all of the observed samples.

The attack actions are established on the successful conciliation of the meter. To compromise Meter 1 and Meter 2 respectively, the attacker takes 4 sessions and 8 sessions respectively. The attacker-Defender interaction model is shown in Figure-2. The attacker sets a false Δf to -4.5Hz if the true $\Delta f$is negative or 3.5 Hz if the true Δf is positive. Thus the overcompensation attack gets implemented and takes into account the saturation filter.

Defense actions: The saturation filter and redundancy measure are implemented by the defender. For idleness, the N consecutive samples are read alternately by the defender from two frequency meters of different form, (one is more secure when compare to the other). Upon gathering samples, the defender tracks a clustering-based algorithm on the latest N samples to detect intrusions.

The defense actions are defined as follows:
d_1 after collecting the N samples, the algorithm 1 will run with the attack detection probability,

$$1 - \alpha_1 \left(\frac{x}{N}\right)^{\beta_1}.$$

d_2 Upon collecting N samples, run Detection algorithm 2 with attack detection probability,

$$\frac{1}{\left[1+e^{-\alpha_2\left(\frac{x}{N}-\beta_2\right)}\right]}.$$

where x is the number of malicious samples among N samples; $\alpha_1, \alpha_2, \beta_1$and β_2, are constants.

5. SIMULATION STUDY

The simulation work is carried out using the MATLAB/Simulink. Here, the two area AGC system is modeled with the Attacker-Defender interaction model.

Using the detection algorithm, the defender detects the attack with the performance of the UFLS relay. When system frequency deviates from the nominal frequency, the under frequency load shedding relay starts tripping. Figure-3 shows the simulation diagram of the two area AGC system with attacker and defender model. The attacker sets a false Δf to -4.5Hz if the true $\Delta f$is negative or 3.5 Hz if the true Δf is positive. . This implements the overcompensation attack, and takes into account the saturation filter. For this work, we use the two-area AGC system model and associated simulation parameters in table 6.1. The attacker can inject the false frequency deviation in the form of constant injection,

bias injection, over compensation or negative compensation.

In our work, we consider the overcompensation attack, as it inflicts maximal damage in terms of directly triggering both generator tripping and load shedding.

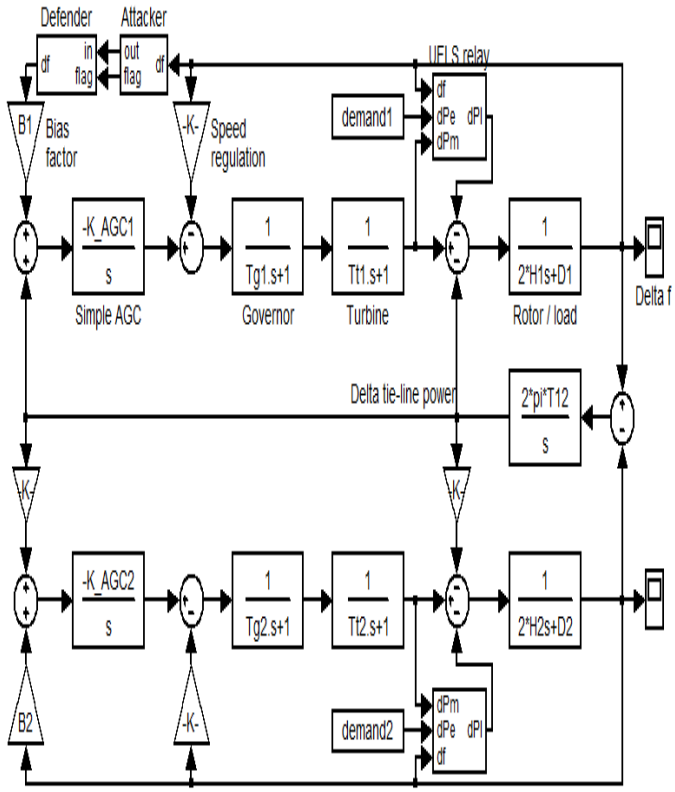

Fig-3: Simulation Diagram for a Two Area AGC System

Table-1: Simulation Parameters of Two Area AGC System

Parameters	Area	
	i = 1	i = 2
$K_{AGCi}(s)$	0.3	0.2
$D_i(p.u./Hz)$	0.015	0.016
$2H_i(p.u.s)$	0.1667	0.2017
$R_i(Hz/p.u.)$	3.0	2.73
$T_{gi}(s)$	0.08	0.06
$T_{ti}(s)$	0.40	0.44
$B_i(p.u./Hz)$	0.3483	0.3827

5.1 Frequency Deviation in Area 1

The two area AGC is simulated with the simulation parameters given in Table-1

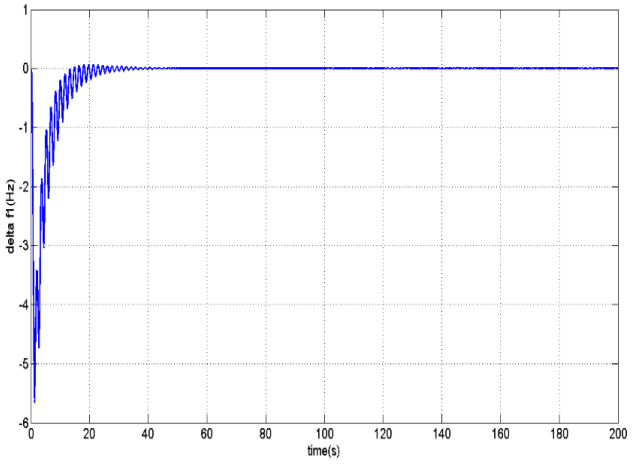

Fig-4: Frequency Deviation in Area 1

The result of frequency deviation in area 1 is shown in Figure-4. This is the normal frequency deviation Δf.

5.2 Corrupted Frequency Detected by the Defender

When the frequency deviation is given as a feedback to the attacker, it injects the false frequency by means of the overcompensation attack. It means that injecting 8 times the normal frequency deviation.

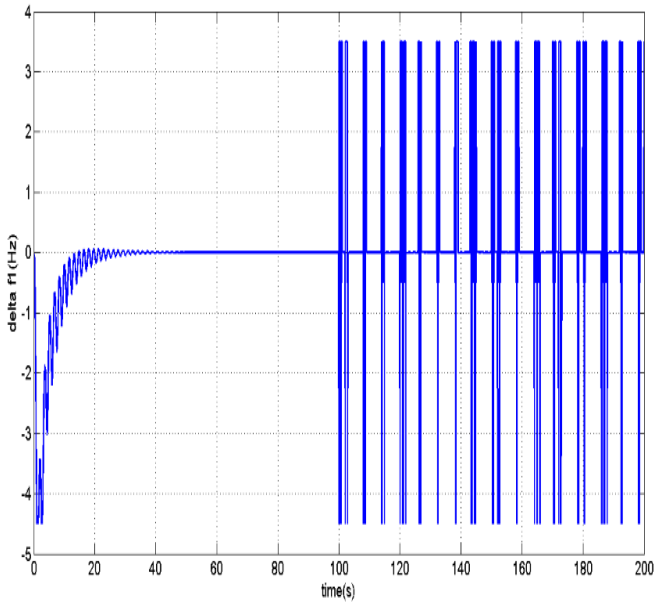

Fig-5: Corrupted Frequency Detected by the Defender

During this condition, the generator tripping may occur. Using the detection algorithm, the defender detects the corrupted frequency in the frequency deviation. This corrupted frequency detected by the defender is shown in Figure-5.

5.3 Load Shed by UFLS Relay

Based on the Under Frequency Load Shedding relay, the load shedding can be rescheduled in the system.

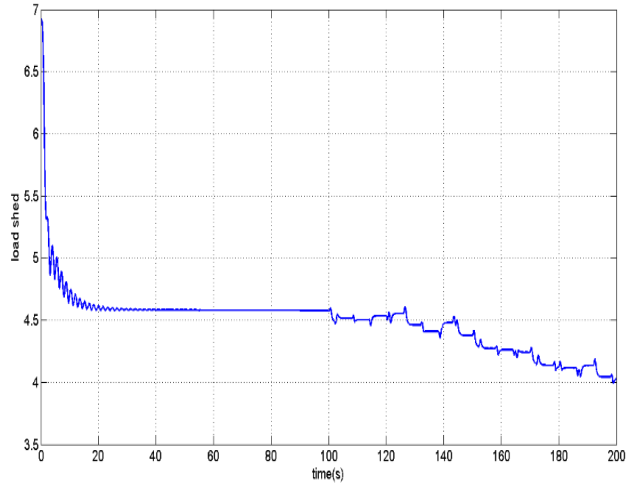

Fig-6: Load Shed by UFLS Relay

Here, when the time exceeds the timer value, the UFLS relay starts to shedding the load. The load shedding by UFLS relay is shown in the Figure-6. These load shed occur after the connection and disconnection of the meters due to the defenders action.

6. CONCLUSION

This paper presents the impact of the False Data Injection (FDI) attack in the smart grid and the method to overcome these attacks. The Security Game theory with the Attacker-Defender interaction model is considered as the solution to detect the false data attacks injected by the hackers. It is the cheapest option compared to any other conventional solution to overcome the problem. It will not only detect the false data but also improves the performance of the AGC by shedding the load through UFLS relay.

Performance evaluation of the AGC is carried out by the simulations using MATLAB Simulation Tool. A simulation model of the AGC with the Attacker and Defender subsystem has been developed and verified. Simulation results show that the Defender detects the false data injection by detecting the corrupted frequency. Simulation results proved that the proposed Security Game method minimizes the security risks faced by the AGC.

REFERENCES

[1] Alpcan.T and Başar.T, (2011) "Network Security: A Decision and Game Theoretic Approach", Cambridge Univ Press.

[2] Ashfaqur Rahman Md. and Hamed Mohsenian, (2013) "False Data Injection Attacks Against Nonlinear State Estimation in Smart Power Grids", IEEE Transaction on Smart Grid, Vol. 6, no. 3

[3] Ashfaqur Rahman and Hamed Mohsenian, (2014) "False Data Injection Attacks with incomplete information against Smart Power Grids", IEEE Transaction on Smart Grid, Vol. 7, no. 5

[4] Bommannavar.P, Alpcan.T, and Bambos.N, (2011) "Security risk management via dynamic games with learning," IEEE Int. Conf. Communications (ICC), pp. 1–6.

[5] Kebina Manandhar, Xiaojun Cao, Fei Hu and Yao, (2008) "Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter", IEEE Transactions on Control of Network Systems, pp. 2325-5870.

[6] Kundur.P, (1994) "Power System Stability and Control" ,New York, NY, USA: McGraw-Hill Professional.

[7] Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A. Emesih, and Zhu Han, (2014) "Detecting False Data Injection Attacks on Power Grid by Sparse Optimization", IEEE Transactions On Smart Grid, Vol. 5, no. 2.

[8] Law .Y.W, Alpcan.T, and Palaniswami, (2012) "Security games for voltage control in smart grid," IEEE 50th Annual Allerton Conf. Communication, Control, and Computing.

[9] Lei Yang and Fengjun Li, (2014) "Detecting False Data Injection in Smart Grid In-Network Aggregation", IEEE smart grid communication.

[10] Liu.S, Liu.X and Saddik.A, (2013) "Denial-of-Service (DoS) attacks on load frequency control in smart grids", IEEE PES Innovative Smart Grid Technologies (ISGT), pp. 1–6.

[11] Liu.N, Zhang.J, Zhang.H, and Liu.W, (2010) "Security assessment for communication networks of power control systems using attack graph and MCDM", IEEE Trans. Power Del., vol. 25, no. 3, pp. 1492–1500.

[12] Mohsenian-Rad.A and Leon-Garcia.A, (2011) "Distributed internet-based load altering attacks against smart power grids", IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 667–674.

[13] Mounzer.J, Alpcan.T, and Bambos.N, (2010) "Dynamic control and mitigation of interdependent IT security risks", IEEE Int. Conf. Communications (ICC), pp. 1–6.

[14] Po-Yu Chen, Shusen Yang and Xinyu Yang, (2009) "Detection of False Data Injection Attacks in Smart- Grid Systems", IEEE Transaction on Smart Grid, Vol. 7, pp. 1-9.

[15] Shapley.L (1953) "Stochastic games", Proceedings on National Academy for Science, vol. 39, pp. 1095–1100.

[16] Shoham.K and Leyton-Brown.L (2009) "Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations", Cambridge, U.K.: Cambridge Univ Press.

[17] Sridhar.S and Manimaran.G (2011) "Data integrity attack and its impacts on voltage control loop in power grid", IEEE Power and Energy Society General Meeting.

[18] Xiaoxue Liu, Peidong Zhu and Yan Zhang (2015) "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", IEEE Transactions On Smart Grid, PP. 1949-3053.

[19] Yi Huang, Husheng Li and Kristy A. Campbell, (2011) "Defending False Data Injection Attack On Smart Grid Network Using Adaptive CUSUM Test", IEEE, PP. 4244-9848.

[20] Yun Gu, Ting Liu, Dai Wang, Xiaohang Guan and Zhanbo Xu, (2013) "Bad Data Detection Method for Smart Grids Based on Distributed State Estimation", Selected Areas in Communication Symposium, IEEE, PP. 4673-3122.