VOL. 14, NO. 7, APRIL 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ROBUST COOPERATIVE CONTROL IN MULTI-AREA POWER SYSTEM USING DIFFERENTIAL GAME THEORY UNDER WEAK GRID CONDITION

Shaik Khadar Vali[1], V. Madhusudhan[2] and R. Kiranmayi[3]
[1]Department of Electrical and Electronics Engineering, Jawaharlal Nehru Technical University, Anantapur, India
[2]Department of Electrical and Electronics Engineering, VNR VJIET, Hyderabad, India
[3]Department of Electrical and Electronics Engineering, Jawaharlal Nehru Technical University, Anantapur, India
E-Mail: skhadarvali1985@gmail.com

ABSTRACT

The penetration of renewable energy conversion system in power system becomes very important because of green energy in recent power system. The incorporation of renewable energy resource in multi-area power system is proposed with Area-1 and Area-2 consist of thermal reheat power plant where as area-3 and area-4 as hydro power plant and area-5 as renewable energy system. The cyber security threat may cause the operation of power system to blackout and due to that the economy of power industries effected and it may cause the power failure in many busy cities. If the cyber security attack is done in 5 area system, the system has to work in perfect operating condition in lesser time. Here the differential game theory-based control strategy is imposed for formulating the problem of cyber security threat. And the performance evaluation is carried out using PI controller and differential game theory based robust controller with MATLAB software is used for evaluation and comparison of results.

Keywords: game theory, multi-area power system, loads frequency control.

INTRODUCTION

The electric power is one of the most important resource in the world. Recently there is a need of more secure operation in power system, as a small component failure also makes huge loss in power due to cascading failures. It affects the entire system operation. To enhance the security of the system, electric power utility is increasingly integrated advanced information system in power infrastructure for wide area control and monitoring, protection and control. So, the power system is now composed of phasor measurement unit (PMUs), small circuit breakers and distributed generators of renewable resources that use the communication interfaces to make sure the system security even with distributed generators. As this security system uses the cyber network as communication protocol there is a possibility of cyber-attack. These attacks may be a false data injection as discussed in [1]. Using eavesdropping estimate the system state [2] and denying the service attacks on the communication network [3]. Risk analysis is done in the potential physical impact of these cyber-attacks in [4-6]. In recent, the cyber-attacks are done in the point of system weakness. In [7] it is demonstrated that attackers can design the effective sequence of binary on-off pulses for circuit breakers and it can trip the generators. In [8] false data injection is one of the attack models which makes the power grid inoperable. Bad data injection makes the PMUs to provide wrong data to power system control. This makes the central control to operate with wrong data which may cause blackouts or economical losses. One example is coordinated switching attack of a binary control oriented stealthy attack model that uses corrupt smart circuit breakers to progressively build physical instability at various points in power grid [11].

To rectify these problems control targets of multi area power system and conventional power plants must be capable of adjusting output timely to meet the variation of renewable energy resources. in a typical power system consist of coal, hydro and gas. Each unit has different operations in capacity, cost, generation limit, unit response time etc. In [12] many methods are used for multi area power system but it is done with either coal or hydro, which is not the real time power system. In recent power system many sources are available in power system. In [13] & [14] multiarea with multi sources are considered. Even though the controls for each unit is considered as same. To solve these issues the differential game theory provides an effective solution by considering the cost function and solving it with the new flower pollination algorithm. This paper applies the game theory in multi area power system including solar distributed generation with hydro and coal or steam generation the changes in the solar power causes the weak grid system condition which makes easy for cyber-attack. So here the response of the frequency and tie power deviations made faster by using the new control strategy. It makes faster settling time and reduces the attack vulnerability.

CONTROLLER DESIGN

There are many kinds of differential games which can be applied to different situations. In this paper, the nonzero-sum non-cooperative differential games will be used. Nonzero sum means that in a game with more than two players, the sum of all the players' performance index is neither zero nor constant. And cooperation among the players is inadmissible or difficult to enforce [15], hence the players are assumed not to collaborate in trying to minimize their own performance index.

Consider a system with N players described by the linear differential equation

$$\dot{x}(t) = Ax(t) + \sum_{i=1}^{N} B_i u_i(t) \quad \ldots.(1)$$

where $x(t_0) = x_0$
where, $x(t) \in R^{n\times t}$ is state varable vector
$u_i(t)$
$\in R^{m_i\times 1}$ is a control strategy vector used by ith player
$A \in R^{n\times n}$ and
$B \in R^{n\times n}$ are constant real matrix

And each player desires to minimize his own quadratic performance index, i.e., cost function. In this paper we adopt the following type cost function for simplicity.

$$J_i = \int_{t_0}^{\infty}\{x(t)^T Q_i x(t) + u_i(t)^T R_i u_i(t)\}dt \quad (2)$$

where $Q_i \in R^{n\times n}$ is symmetric semi $-$ positive definite
$R_i \in R^{m_j\times m_j}$ is symetric positive definite matrix

Assume current value of system state vector is available for all the players, then the constant linear feedback control strategy used by ith player can be expressed as
$u_i = F_i x$
$F_i \in R^{m_i\times n}$
$where\ (F_1, \ldots., F_N)$ belongs to the set $F = \{F = (F_1, \ldots, F_2)|A + \sum_i^N B_i F_i\} i\ s\ stable$

Flower pollination algorithm [16]

Flower constancy and pollinator behavior as the following rules:

a) Biotic and cross-pollination is considered as global pollination process with pollen- carrying pollinators performing Levy flights.

b) Abiotic and self-pollination are considered as local pollination.

c) Flower constancy can be considered as the reproduction probability is proportional to the similarity of two flowers involved.

d) Local pollination and global pollination is controlled by a switch probability p ∈[0, 1].

Due to the physical proximity and other factors such as wind, local pollination can have a significant fraction p in the overall pollination activities. Obviously, in reality, each plant can have multiple flowers, and each flower patch often release millions and even billions of pollen gametes. However, for simplicity, we also assume that each plant only has one flower, and each flower only produce one pollen gamete. Thus, there is no need to distinguish a pollen gamete, a flower, a plant or solution to a problem. This simplicity means a solution x_i is equivalent to a flower and/or a pollen gamete.

From the above discussions and the idealized characteristics, we can design a flower-based on algorithm, namely, flower pollination algorithm (FPA). There are two key steps in this algorithm; they are global pollination and local pollination. In the global pollination step, flower pollens are carried by pollinators such as insects, and pollens can travel over a long distance because insects can often fly and move in a much longer range. This ensures the pollination and reproduction of the fittest, and thus we represent the fittest as g*. The first rule plus flower constancy can be represented mathematically as

$$x_i^{t+1} = x_i^t + L(x_i^t - g_*) \quad (4)$$

where x_i^t is the pollen ior solution vector x_i at iteration t, and g_* is the current best solution found among all solutions at the current generation/iteration. The parameter L is the strength of the pollination, which essentially is a step size. Since insects may move over a long distance with various distance steps, we can use a L´evy flight to mimic this characteristic efficiently. That we draw L>0 from a levy distribution

$$L \sim \frac{\lambda\Gamma(\lambda)\sin\left(\frac{\pi\lambda}{2}\right)\left(\frac{1}{s^{1+\lambda}}\right)}{\pi}(s \gg s_0 \gg 0) \quad \ldots. (5)$$

Psuedo code:

Objective min $J_i(x)$, x = (x1, x2, ..., xd)
Initialize a population of n flowers/pollen gametes with random solutions
Find the best solution g_ in the initial population
Define a switch probability p ∈[0, 1]
while (t <Max Generation)
for i= 1 :n (all n flowers in the population)
if rand < p,
Draw a (d-dimensional) step vector L which obeys a L´evy distribution
Global pollination via

$$x_i^{t+1} = x_i^t + L(x_i^t - g_*) \quad \ldots(6)$$

else
Draw ǫ from a uniform distribution in [0, 1]
Randomly choose j and k among all the solutions
Do local pollination via

$$x_i^{t+1} = x_i^t + \varepsilon(x_j^t - x_k^t) \quad \ldots.(7)$$

end if
Evaluate new solutions
If new solutions are better, update them in the population
end for
Find the current best solution g_*
end while

RESULTS AND DISCUSSIONS

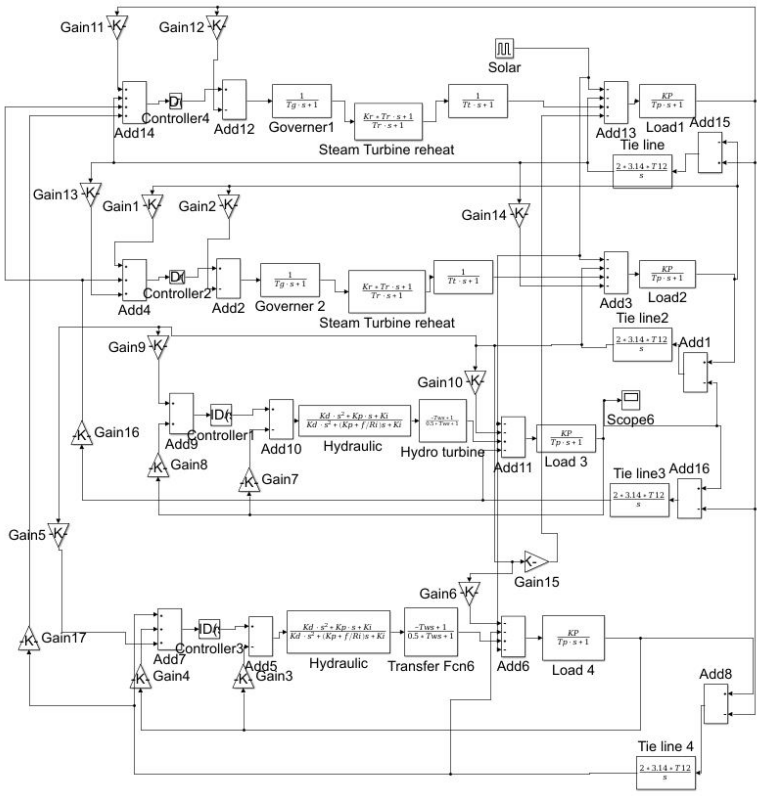

Figure-1. Proposed test system with 5 areas including solar.

Scenario 1 is considered as renewable energy-4 area system implementation, scenario 2 is considered as 4-area, two hydro and two thermal system, scenario 3 is considered as 5-area, where thermal, hydro and renewable energy are hybrid. The security threat is created at the renewable energy point due to that the frequency change and power change is compared which is otherwise known as weak grid condition. And it can be seen that differential game theory make the stability even with cyber treat created.

Then for different controls considered as different cases. Case1 is applied with PI controller, case 2 is applied with Robust controller. Figure-1 shows the proposed test system with 5-area including solar.

Figures 2, 4, 6, 8, 10 & 12 shows the tie line power of three different scenarios and cases. Figures 3, 5, 7, 9, 11 and 13 shows the frequency deviation of three different scenarios and cases. Here it can be seen that all the tie line power and frequency are made as zero which shows the controllability. But the settling time is different for all the scenarios and cases. The security threat is solved and the system stability indicates that.

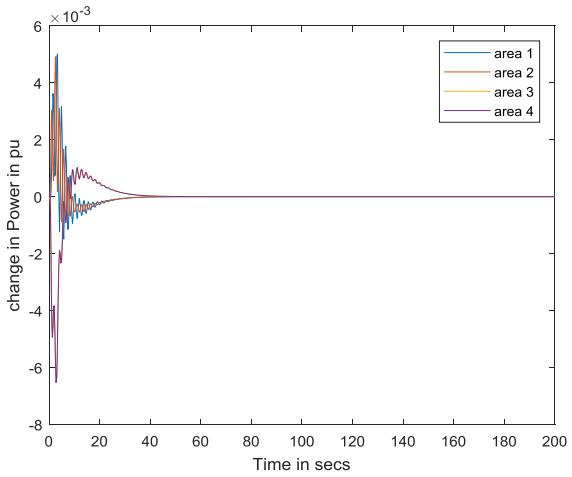

Figure-2. Tie line power in p.u with PI controller.

Scenario 1: Thermal, hydro 4-area

Case 1: PI controller

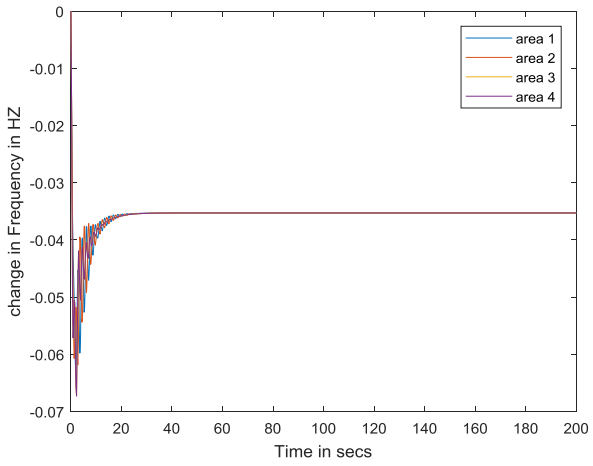

Figure-3. Frequency Deviation in hz with PI Controller.

Case 2: Robust control

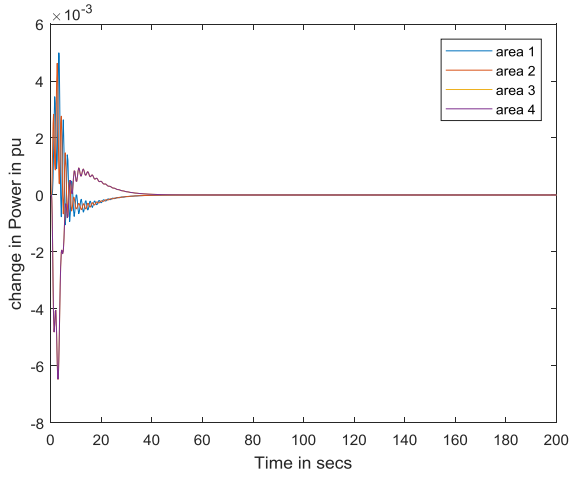

Figure-4. Tie line power in p.u with Robust controller.

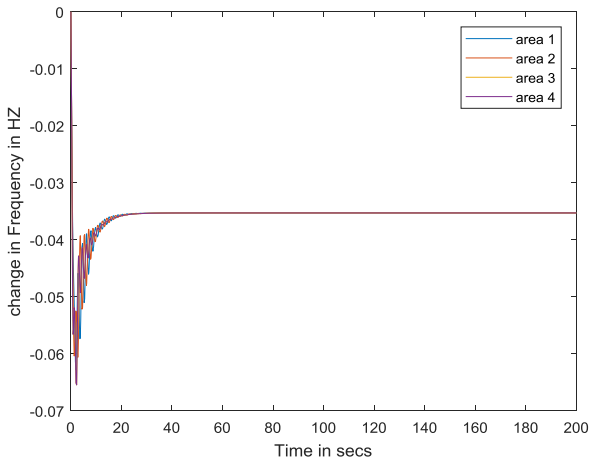

Figure-5. Frequency Deviation in hz with robust Controller.

Scenario 2: SOLAR – 4 area

Case 1: PI controller

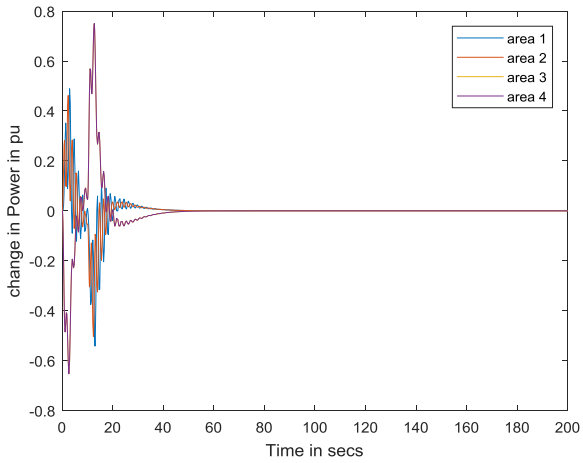

Figure-6. Tie line power in p.u with PI controller.

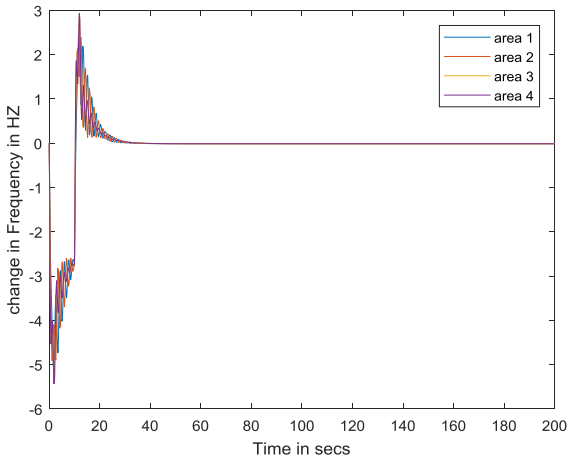

Figure-7. Frequency Deviation in hz with PI Controller.

Case 2: Robust controller.

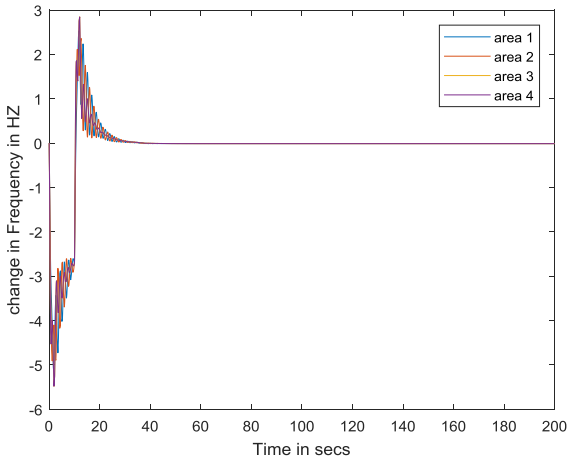

Figure-8. Tie line power in p.u with Robust controller.

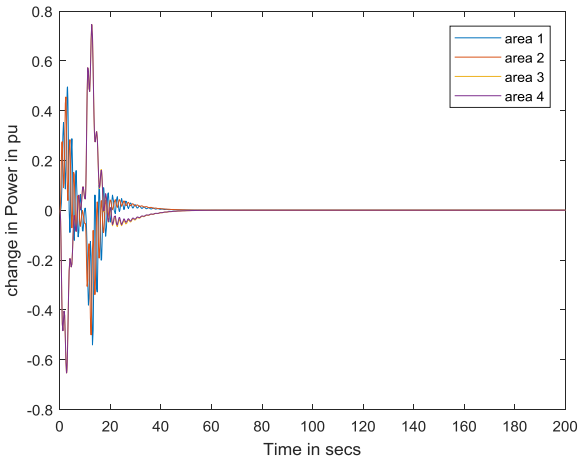

Figure-9. Frequency Deviation in hz with Robust Controller.

Scenario 3: Thermal, hydro and SOLAR - 5 area system

Case 1: PI controller

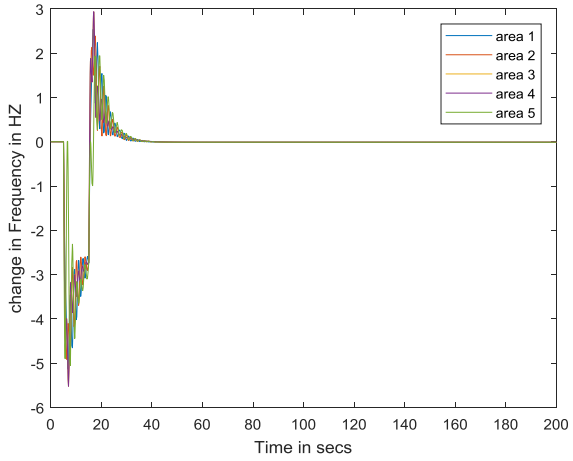

Figure-10. Tie line power in p.u with PI controller.

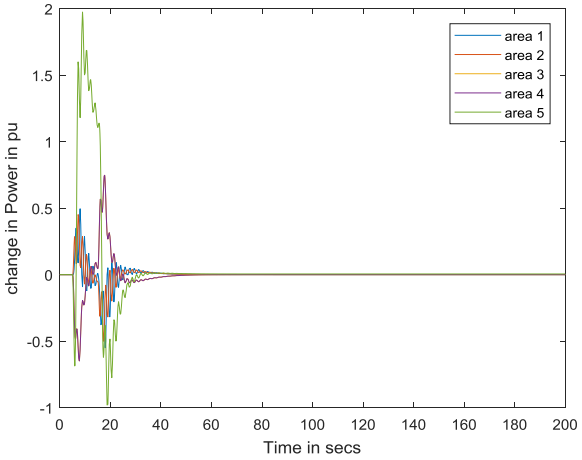

Figure-11. Frequency Deviation in hz with PI Controller.

Case 2: Robust Controller.

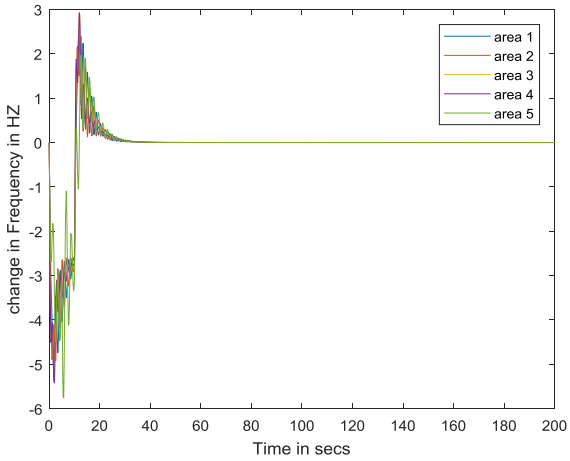

Figure-12. Tie line power in p.u with Robust controller.

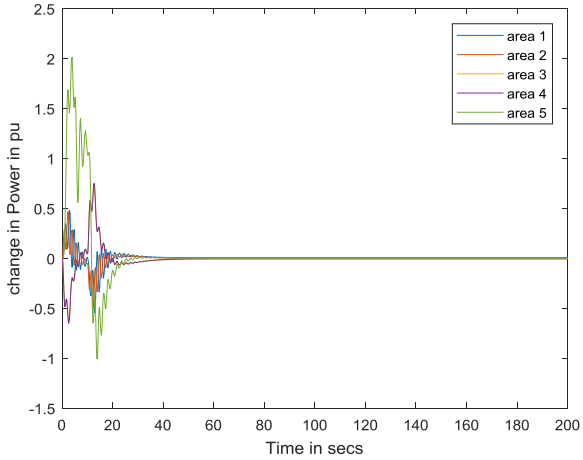

Figure-13. Frequency Deviation in hz with Robust Controller.

Table-1. Performance comparison table.

	Scenario 1		Scenario 2		Scenario 3	
	PI	**Robust**	**PI**	**Robust**	**PI**	**Robust**
RiseTime(s)	4.1134	0.033927	0.4659	0.033927	2.0968	0.038871
SettlingTime(s)	21.502	10.611	26.421	8.1247	34.451	16.685
SettlingMin	0.14117	0.14117	0.046908	0.04677	0.063062	0.015
SettlingMax	0.26143	0.25803	21.327	21.415	25.779	26.341
Overshoot	85.183	82.769	45192	45407	40315	1.7524e+05
Undershoot	0	0	0	0	0	0
Peak	0.26143	0.25803	21.327	21.415	25.779	26.341
PeakTime (s)	5.6118	2.3388	3.3785	1.3073	9.5024	3.1117

CONCLUSIONS

The PI controller and robust control using differential game theory is used to solve the problem created due to the security attack. The performances show the robustness of the new control system and it can be seen that in all the cases the stability is achieved in lesser time. So, the controller proves that the multi-area with renewable resources stable even in cyber-attack.

REFERENCES

[1] Y. Liu, P. Ning, and M. K. Reiter. 2009. False data injection attacks against state estimation in electric power grids. in Proc. 16th ACM Conf. Comput. Commun. Security, Chicago, IL, USA. pp. 21-32.

[2] M. El-Halabi, A. Farraj, H. Ly, and D. Kundur. 2012. A distortion-theoretic perspective for redundant metering security in smart grid. in Proc. IEEE Can. Conf. Elect. Comput. Eng. (CCECE), Montreal, QC, Canada, Apr./May. pp. 1-5.

[3] D. Kundur. 2014. Power system reliability, security and stability, class notes for ECE1518: Seminar in identity, privacy and security. Dept. Elect. Comput. Eng., Univ. Toronto, Toronto, ON, Canada.

[4] S. Sridhar, A. Hahn, and G. Manimaran. 2012. Cyber-physical security for electric power grid. Proc. IEEE. 100(1): 210-224.

[5] A. Hahn and G. Manimaran. 2011. Cyber attack exposure evaluation framework for the smart grid. IEEE Trans. Smart Grid. 2(4): 835-843.

[6] P. Rezaei, P. Hines, and M. Eppstein. 2015. Estimating cascading failure risk with random chemistry. IEEE Trans. Power Syst. 30(5): 2726-2735.

[7] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry. 2014. A coordinated multi-switch attack for cascading failures in smart grid. IEEE Trans. Smart Grid. 5(3): 1183-1195.

[8] T. Liu *et al.* 2015. Abnormal traffic-indexed state estimation: A cyber - physical fusion approach for smart grid attack detection. Future Gener. Comput. Syst. 49: 94-103.

[9] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng and Z. Han. Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst. J., DOI: 10.1109/JSYST.2014.2341597.

[10] M. Esmalifalak, Z. Han, and L. Song. 2012. Effect of stealthy bad data injection on network congestion in market based power system. in Proc. IEEE Wireless Commun. Netw. Conf., Shanghai, China. pp. 2468-2472.

[11] S. Liu, B. Chen, D. Kundur, T. Zourntos, and K. Butler-Purry. 2013. Progressive switching attacks for instigating cascading failures in smart grid. in Proc. IEEE Power Energy Soc. Gen. Meeting, Vancouver, BC, Canada. pp. 1-5.

[12] H. Shayeghi, H. A. Shayanfar and A. Jalili. 2011. Load frequency control strategies: a state-of-the-art survey for the researcher. Energy Conversion and Management. 50(2): 344-353.

[13] K. S. S. Ramakrishna1, P. Sharma and T. S. Bhatti. 2010. Automatic generation control of interconnected power system with diverse sources of power generation. International Journal of Engineering Science and Technology. 2(5): 51-65.

[14] K. P. S. Parmara, S. Majhi and D. P. Kothari. 2012. Load frequency control of a realistic power system with multi-source power generation. Electrical Power and Energy Systems. 42(1): 426-433.

[15] J. C. Engwerda. 2005. LQ dynamic optimization and differential games. New York: Wiley.

[16] Xin-she Yang. 2012. Flower Pollination algorithm for Global Optimization. Unconventional Computation and Natural Computation 2012, Lecture Notes in Computer Science. 7445: 240-249.