31st Youth Academic Annual Conference of Chinese Association of Automation
Wuhan, China; November 11-13, 2016

Detection Technique for Power System under Cyber Attack

Mohsin Ali, Jing Wu, Chengnian Long, and Shaoyuan Li
Department of Automation
Key Laboratory of System Control and Information Processing, Ministry of Education
Shanghai Jiao Tong University
Shanghai, 200240, China
Emails: (mohsinpak, jingwu, longcn, syli)@sjtu.edu.cn

***Abstract*—In order to maintain the security and reliability of smart grid, more efficient operations of relays are required. In this paper, an innovative scheme has been introduced to distinguish the fault and power swing condition, which arise due to change of heavy load and cyber-attack. Microprocessor based relays are proposed to control circuit breakers command signal in case of power swing and fault. A Magnitude-Derivative check algorithm(M-DC) for microprocessors based relays is presented to discriminate faults and power swings condition on the basis of the rate of change of current and reactive power. To make the microprocessor relays more reliable, an efficient scheme is proposed, in which attack detector monitors the command signal of microprocessor relays and determines whenever, adversary tries to manipulate the command signal.**

Keywords—smart grid; microprocesso; based relays; phasor measurement unit; fault detection; power swing; cyber-attack

I. INTRODUCTION

Recently, electrical grids are converted into smart grids which are more sensitive, complex and have large number of interconnections. Stability is the most important concern that must be taken into account. It is lost due to several reasons like load encroachment, current instability, power swing and cyber-attack. Transmission lines are the back bone of smart grids. Hence, the protection of transmission lines from any type of high resistance single phase fault, power swing due to anonymous attack and load change, is very necessary because any incorrect operation of relays completely demolish the stability of smart grids. Some techniques are available to protect the transmission lines, such as distance or impedance relays. There are also various research techniques under study to determine the fault and power swing and differentiate them. Power swing is the phenomenon which occurs due to the change of heavy loads, clearance of faults, switching on/off circuit breakers, line switching, power source disconnection and some other system disturbances.

Protection of transmission line has been done by compensating fault resistance with apparent resistance across the relay. In reference [1] fault location was detected by a two-terminal algorithm and by using the equivalence sequence network fault voltage was calculated. This method is time consuming and may not work when very high impedance fault exist, which will be a problem of synchronization. To detect high resistance fault prony method was proposed in references [2]-[4]. Initially it was used for signal processing and now it is widely used for the protection of power system, detection of fault, and power swing. This method is efficient and easy to implement but author has neglect to consider the high resistance single phase fault and parallel line outage, which is covered by zone protection. Distance relay has different protection zones and various reach. For example, backup protection for zone 3 is for whole adjacent lines. It takes several seconds as corresponding to zone 1 and zone 2 tripping time. Protection of zone 3 need to be taken seriously since it prevents such mal-operations and thus, more reliable smart grid can be envisaged. Hence, in reference [5] used positive-sequence phase angle of impedance with zone 3 of distance relay to discriminate three phase fault and load change or parallel line outage, which is highly admire-able but it takes time to determine unstable power swing. To overcome this problem, Fast Fourier transform (FFT) was proposed to speed up discreet Fourier transform (DFT). It calculated the impedance of transmission lines to make distinction between fault and power swing by using the area of triangles, which is established by angles of three consecutive instantaneous power phasor of harmonic component [6], [7].

Algorithm was designed to control the command signals of circuit breakers and operate them when fault has occurred and block them in case of power swing. In [8], [9], adaptive out-of-step detection methods were formulated to detect the fault, power swing and control circuit breaker command signal. These methods are based on different schemes of smart grids, like approximate stability boundaries, but they regret the stability issues of smart grid. So, Out-of-step (OOS) relays were used at the generator terminal to maintain the stability issues, where power angle and frequency are determined and keep the generator within plane but uncontrolled tripping of circuit breakers due to cyber-attack may cause equipment damage [10]. Therefore, swift-calculating-digital-signal-processor based numerical relays were proposed to optimize the security of transmission line and power swing was identified with variation of load angle. This scheme is only reliable to detect slow and fast power swing, while it is destructive for scenarios such as symmetrical fault and cyber-attack on communication channel. Moreover, a diverse PSB scheme was utilized to solve all kinds of fault by rate of change of impedance [11]. The logic behind the scheme is that when fault is occurred change in impedance from load point impedance to fault point impedance will be very quick from normal impedance changing set time [12], [13].

This work was supported by National Nature Science Foundation of China (61473184, 61590924, 61590920, 61673275).

978-1-5090-4423-8/16/$31.00 ©2016 IEEE

In last decade smart grid not only had accidental faults and power swing but also cyber-attack vulnerability seeking to damage the smart grid. A new concept to build the software based microprocessor relays is good engineering practice to control the circuit breaker command signal in case of power swing and fault. But how could we protect command signal from adversary, which retrieving the confidential information and operate the smart grid with ease. This process of hacking changes the integrity of command signal [14], [15]. Hence, Public channel is no longer trust worthy for the essence of power system. It's a severe problem that malicious breaker tripping attack demolishes the reliability and stability of power system. Very simple logical scheme was applied to mitigate cyber-attack like breaker command supervision, time delay on breaker closing, time delay on breaker closing, redundant reclosing supervision, local generator island detection logic, frequency variation [16]-[20]. To make coordination between protection units, agent protection relays were developed. These agents were microprocessor relays where attacker may inject the malicious breaker tripping command signal which spoil the integrity of signal and result in an out-of- synchronism, power swing, also damage the rotating machine [21]. So the fact is that the introduction of a technique to protect and monitor the commands sent from software based microprocessor relays has become an inevitable necessity and a call for professional engineering and security. Hence, software based microprocessor relays are proposed which used an innovative algorithm to distinguish the fault and power swing by using the rate of change of current magnitude and reactive power magnitude. Credibility of command signal of microprocessor is very important and need to monitor. So, we have also proposed software based relays command signal are authenticated by attack detector which is working properly.

II. Formulation of Problem

A smart grid is bi-directional flow of information as well as power between consumer and service provider. The role of transmission lines are a main bridge to supply high power from grid to consumer, any mishap which harmful for the credibility of transmission lines need to control. When transmission lines are hit by lighting, change in heavy load, or some other faults occurs in a grid, a loss of voltage which cause a momentary reduction in the amount of electric power transmitted and a power swing phenomenon will occur. If there is a large swing, the disturbance can spread throughout the entire grid, resulting in a major power outage. Hence, the transmission lines of a power grid are required to operate within the operational limitations, and it is also extremely important to differentiate the power swing and fault to keep the smart grid in synchronized state.

Hence, software base microprocessor base relay method is proposed, which takes local voltages and current to calculate the reactive power. Any change of magnitude in current and reactive power helps to discriminate between stable and unstable swing. To evaluate the efficacy of the proposed algorithm, we have designed a large smart grid infrastructure which includes interconnection of large number of nodes. A node of typical physical architecture of smart grid is shown in Fig. 1. In this architecture a power source is connected to transmission line through transformer to step up the voltages,

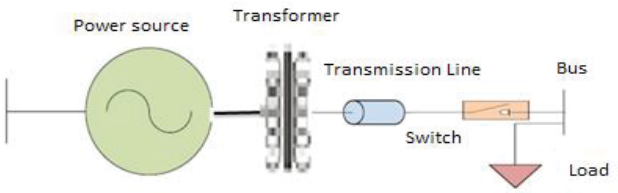

Fig. 1. Single line diagram.

and an electrical load is connected with buses to get stable voltages. Control switches (C-Si=1~C-Si=n) are operated through software base microprocessor relay to protect the transmission line from different type of faults (L-L, L-g, L-L-g) and power swing.

III. Main Result

A. Magnitude-Derivative Check Method to Detect Fault and Power Swing.

It was extremely important to differentiate the power swing and fault to keep the smart grid in synchronized state. As we know, power swing phenomenon is developed due to several reasons, such as line outage, heavy load change, which exists at all time and bring potential safety hazards. In this paper software base microprocessor base relay method is proposed which is capable of detecting any ups and downs in currents and reactive power magnitude measurements of electrical smart grid very quick and highly effective as compared to the other slow-moving and time consuming methods.

Since the complexity of smart grid is higher, Phasor measurement units (PMU) provided us pre and scheme post event data measurements to decrease the computation burden execution time of algorithm [22]. This new technology is very important to check the real time status of power system. Apparent impedance across the relay is calculated from the data that is collected from PMU. In case of fault, there is reduced voltage and increased current level and also decrease in measure impedance. The idea behind the proposed method is that the current and reactive powers are used as decisive factors which are the key weapons. Once the short circuit is occurred on the transmission lines, the change in current magnitude is increased drastically. However, this swift change can also be acquired by change in load increase.

Therefore, we presented Magnitude-Derivative check (M-DC) algorithm, which is based on the current and reactive power measurement, to detect the fault and power swing. Magnitude-Derivative check (M-DC) algorithm is flow chart is shown in Fig. 2.

The core idea of M-DC is based on dI/dt and dQ/dt. When the measure impedance enters into the critical zone-3 element, then proposed algorithm decides whether it is a fault condition or not, which is decided on bases of following two scenarios below.

Case 1: $dI/dt > dI/dt(limit)$

Case 2: $dQ/dt < dQ/dt(limit)$

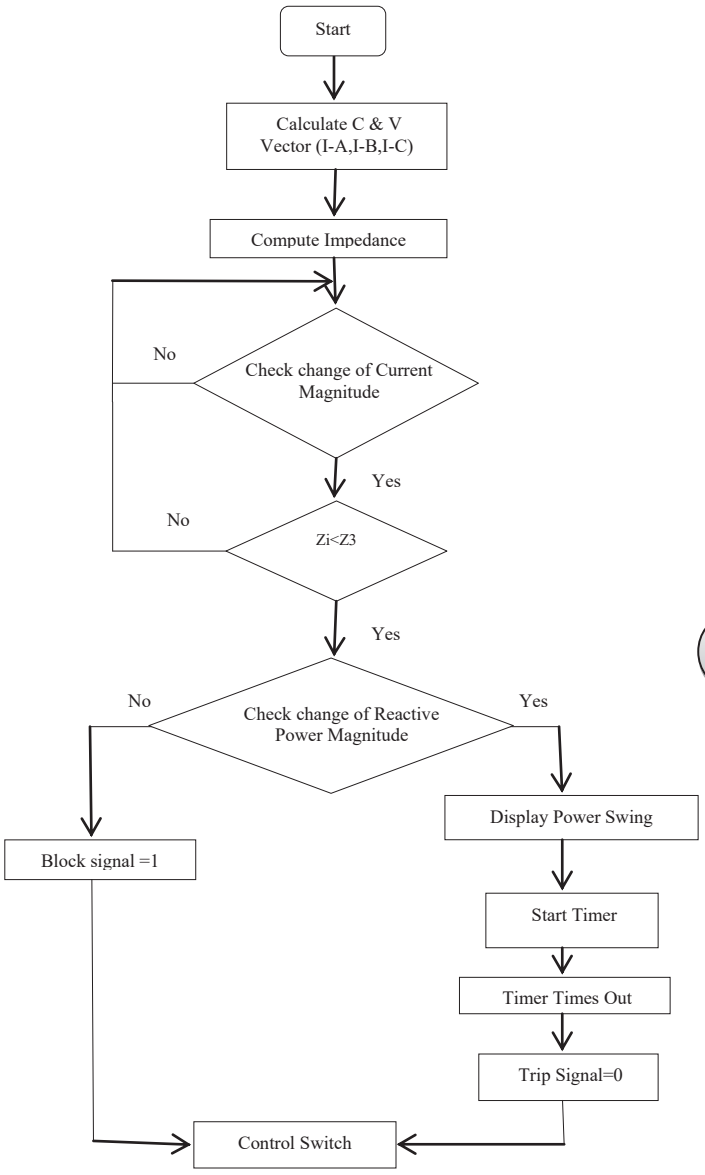

Fig. 2. Flow chart of M-DC algorithm.

In case of the first condition evaluates to be true, the impedance is checked whether it is in zone-3 or not. Once the impedance enters zone-3, then second condition is executed and if it evaluates to true a timer is turned on that is set to send a trip signal when the time runs over.

B. Nounce-Operation Method to Detect Cyber-Attack

Credibility of smart grid is challenged day by day due to the involvement of internet. As a result the breaker status signals altered and unintentional circuit breaker tripping occurred, which may cause power swing in power.

In this paper malicious breaker tripping command attack is implemented in the form of integrity attack. Integrity attack is assumed that microprocessor based relays are hacked by altering its settings. Transmission lines which damage the

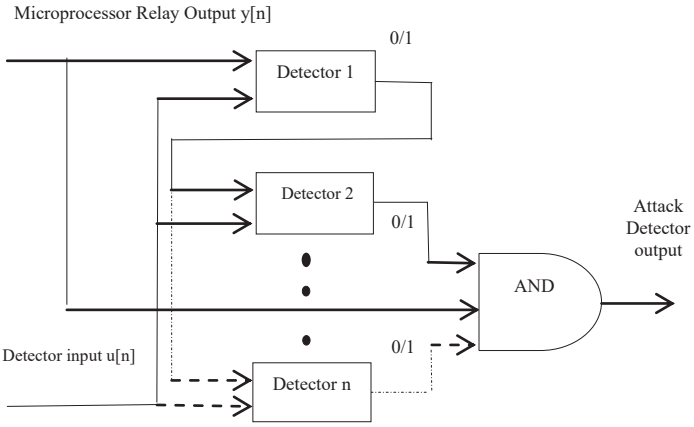

Fig. 3. Malicious Breaker Tripping Attack Detector.

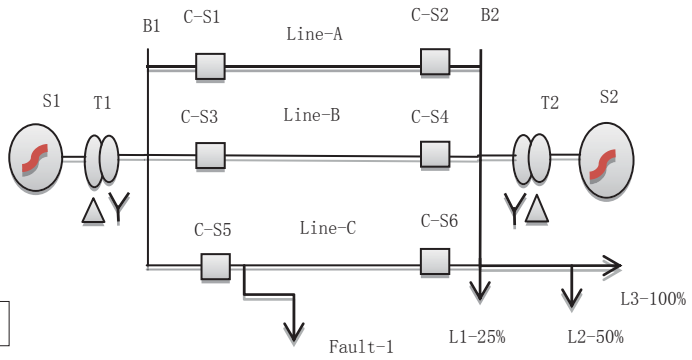

Fig. 4. Schematic of a Single Line Diagram of Power System Model.

healthy power system. This problem should be taken more seriously and a reliable system is required to protect the circuit breaker signal. We have designed an attack detector, which is shown in Fig. 3.

The attack detector informs if adversary changed circuit breaker command signals. Nounce-operation method has been used to determine the malicious breaker tripping attack. In this method two detectors are used to determine if adversary tries to make any changes in command signal. Detector has its input u[n] and also takes output from microprocessor relays y[n]. The input that have been taken from microprocessor relays have been secured by Nounce-operation implement authentication if adversary manipulates it. If the authentication result is evaluated to true, it means adversary has manipulated the circuit breaker command signal.

IV. SIMULATION

To evaluate the effectiveness of our proposed method, a 220kv smart grid model in Fig. 4 is considered.

In this model, there are two equivalent dynamic power sources (S1 & S2), which are connected by parallel transmission lines. Detail parameters of these power sources are found from [23] and given in Table I. Buses B1 and B2 are send end bus and receive end bus, respectively. Interconnection between two power sources are obtained by three transmission

lines Line-A, Line-B and Line-C. The detail parameters of these transmission lines are given in Table II. Two equivalent sources (S1 & S2) are connected to buses B1 and B2 by transformer T1 and T2 of equivalent capacity respectively and their details are also given in Table III.

TABLE I. POWER SOURCE DATA (S1,S2)

Nominal power	615MV
Voltages	13.8kv/220kv
Frequency	50HZ

TABLE II. TRANSMISSION-LINE DATA

Line-A	Length=120km
Line-B	Length=120km
Line-C	Length=120km
Positive-Sequence Impedance =0.00297+j0.33Ω/km	
Zero-Sequence Impedance = 0.162+j1.24Ω/km	
Positive-Sequence capacitance = 12.99nf/km	
Zero-Sequence capacitance = 8.5nf/km	

TABLE III. TRANSFORMER T1,T2 AND LOAD DATA

Nominal power	615MV
Voltages	13.8kv/220kv
Frequency	50HZ
Load 1	200MW
Load 2	400MW
Load 3	500MW

A. Application of Power Swing and Its Protection

In order to check the efficiency of the Magnitude-Derivative check algorithm various loads have been applied and it concludes from the results that microprocessor based relays is working appropriately. It has also dealt with the consequences of the microprocessor relays which are under the danger of cyber-attack. Nounce-operation method is used to detect the attack and found working properly. As shown in Fig. 5 various percentages (25%, 50% and 100%) of full load are provided to simulate the cases of power swing.

Application of load is provided with the time slots such as t=1sec, t=2sec, t=3sec. simultaneously. During the condition of power swing, variations in the magnitude of voltage and changes in current and reactive power are occurred. The rate of change of current and reactive power is increased gradually. After evaluation of the system, these parameters are found within the range of threshold. Hence, Magnitude-Derivative check algorithm remains stable and does not issue trip signal.

B. Application of Fault and Its Remedy

Various faults were simulated on Line-C. Power swing due to these faults can be observed by isolation of fault on Line-C. In this simulation, a random fault has been applied at t=1 sec on Line-C. Therefore unstable power swing is generated by fault and algorithm is found working properly and sent the trip signal to circuit breaker. Fig. 6 shows the value of the current and reactive power magnitude during fault isolation of parallel

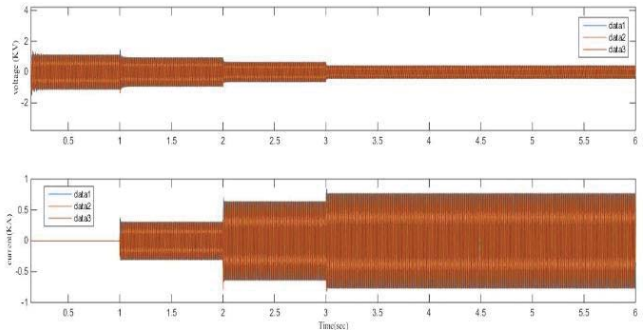

Fig. 5. Variation in voltage and current magnitude during change in load.

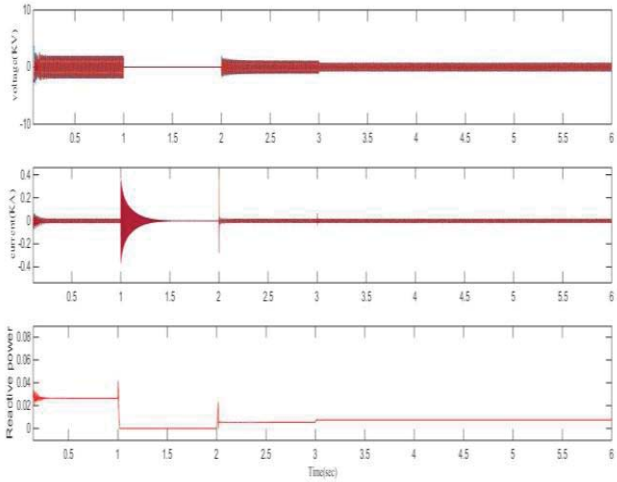

Fig. 6. Performance of Magnitude-Derivative check algorithm to discriminate fault and power swing.

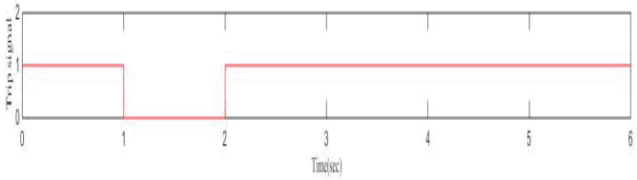

Fig. 7. Magnitude-Derivative check algorithm (M-DC) response during fault on line.

lines. Fault has been removed at t= 2sec from Line-C produces power swing effects. However Magnitude-Derivative check algorithm has been working properly in fault swing case and issued the trip signal that shown in Fig. 7, while in stable swing case it remain stable and does not issue any trip signal. To make it more clear the GUI provide user friendly interface, Hence, students can change the smart grid data such as transmission line data, load data and implement different faults [24] .

C. Simulation Result of Attack Detector

To keep track of Nounce-operation basis attack detector, an integrity attack is set to start at different time slots. The attack is attempted by injecting a set of malicious signal "0"and "1"which flows like an "AND" logic to original circuit breaker signal. This malicious signal is intended to make changes in the circuit breaker status signal as well as to

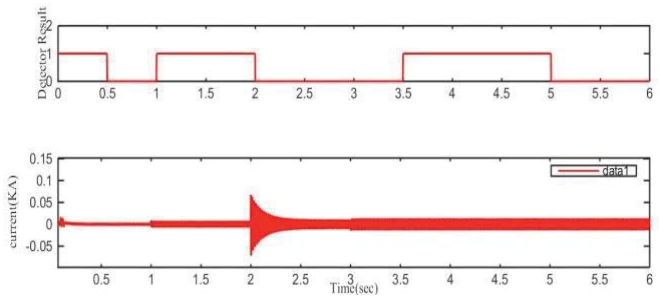

Fig. 8. Magnitude of current and response of attack detector.

hammer the normal operation of the circuit breaker. This scenario can be assumed in a way that the integrity attack is executed by an adversary who has knowledge about protocol of Microprocessor relays setting. Proposed algorithm of attack detector has been working properly as shown in Fig. 8. As there is no fault current flow through the Line-B and the output of attack detector is determine that if it is off its mean adversary has might change the signal and tried to manipulate it.

V. Conclusion

We have introduced a Magnitude-Derivative check (M-DC) algorithm to distinguish fault and power swing condition on basis of rate of change of current and reactive power magnitude. Smart grid model and algorithm is designed and simulated using Matlab Simulink. Software base microprocessor relays command signal are shielded from attack through Exclusive-Or logical operation, which works efficiently. The simplicity and efficiency of this method makes it to be recommended for it implementation for the protection of diverse power systems.

References

[1] M. H. Idris, M. S. Ahmad, A. Z. Abdullah, and S. Hardi, "Adaptive Mho type distance relaying scheme with fault resistance compensation," *International Power Engineering and Optimization Conferenc*, Malaysia, 2013.

[2] A. Thakallapelli, R. Mehra, and H. A. Mangalvedekar, "Differentiation of faults from power swings and detection of high impedance faults by distance relays," *Condition Assessment Techniques in Electrical Systems Conference*, Kolkata, India, 2013.

[3] S. Lotfifard, J. Faiz, and M. Kezunovic, "Detection of symmetrical faults by distance relays during power swings," *IEEE Trans. Power Del*., vol. 25, pp. 81-87, 2010.

[4] L. Zhen and Z. J. Zhang, "Studies of distance protection with a microprocessor for short transmission lines," *IEEE Trans. Power Syst*., vol. 3, pp. 330-336, 1988.

[5] Nayak, P. Kumar, A. K. Pradhan, and P. Bajpai, "Secured zone 3 protection during stressed condition," *IEEE Trans. Power Del*., vol. 30, pp. 89-96, 2015.

[6] İ. G. Tekdemir and B. Alboyaci, "Improvement of power swing detection performance of a distance relay by using k-NN algorithm," *International Conference on Electrical and Electronics Engineering*, Melaka, Malaysia, 2015.

[7] Abdlrahem, A. Abdlmnam , and H. Sherwali, "Modelling of numerical distance relays using MATLAB," *IEEE Symposium on Industrial Electronics and Applications*, Kuala Lumpur, Malaysia, vol. 1, pp. 389-393, 2009.

[8] Y. W. Wei, S. Paudyal, and B. A. Mork., "Out-of-step detection using Zubov's approximation stability boundaries," *IEEE Power and Energy Society General Meeting*, Denver, 2015.

[9] S. I. Lim, C. C. Liu, S. J. Lee, M. S. Choi, and S. J. Rim, "Blocking of zone 3 relays to prevent cascaded events," *IEEE Trans. Power Syst*., vol. 23, pp. 747-754, 2008.

[10] Zare, Javad, and F. Aminifar, "Synchrophasor-assisted line outage identification: A simple and iterative algorithm," *Iranian Conference on Electrical Engineering*, Tehran, 2015.

[11] Afzali, Milad, and A. Esmaeilian, "A novel algorithm to identify power swing based on superimposed measurements," *International Conference on Environment and Electrical Engineering*, Venice, 2012.

[12] X. Z. Dong, Y. Z. Ge, and J. L. He, "Surge impedance relay," *IEEE Trans. Power Del*., vol. 20, pp. 1247-1256, 2005.

[13] Khan, U. Naseem, and L. Yan, "Power swing phenomena and its detection and prevention," *7th EEEIC International Workshop on Environment and Electrical Engineering*, Poland, 2008.

[14] A. H. Mohamad, Auday, and E. G. Ahmed, "MATLAB-Simulink S-Function for modeling a digital MHO distance relay," *International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering*, Sudan, 2015.

[15] A. H. Mohamad and A. Abdelkareem, "A new MATLAB-Simulink S-Function for modeling a digital MHO distance relay based on fast fourier transform algorithm," *International Journal of Power and Renewable Energy Systems*, vol. 2, pp. 101-108, 2015.

[16] P. Thangarathinam, N. Suganya, T. Praddeep, and S. Vignesh, "Synchrophasor Technology for Cyber Security in Smart Grid," *International Journal of Students' Research in Technology and Management*, vol. 3, pp.436-439, 2015.

[17] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, "Mitigating the aurora vulnerability with existing technology," *36th Annual Western Protective Relay Conference*, Spokane, 2009.

[18] D. Anderson, "Securing Modern Substations With an Open Standard Network Security Solution," *11th Annual Western Power Delivery Automation Conference*, Spokane, 2009.

[19] A. Szentagotai and D. David, "Rational emotive behavior therapy versus cognitive therapy versus pharmacotherapy in the treatment of major depressive disorder: Mechanisms of change analysis," *Psychotherapy: Theory, Research, Practice, Training*, vol. 45, pp. 523, 2008.

[20] M. M. Frey, C. Hancock, and G. S. Logsdon, *Cryptosporidium: answers to questions commonly asked by drinking water professionals*. New Jersey: American Water Works Association, 1997.

[21] S. Rahman, H. R. Pota, and J. Hossain, "Cyber vulnerabilities on agent-based smart grid protection system," *IEEE PES General Meeting Conference and Exposition*, Washington DC, 2014.

[22] A. Mechraoui and D. W. P. Thomas, "A new blocking principle with phase and earth fault detection during fast power swings for distance protection," *IEEE Trans. Power Del*., vol. 10, pp. 1242-1248, 1995.

[23] N. G. Chothani, and V. Sharma, "A new relaying method to discriminate between fault and power swing condition," *International Conference on Recent Developments in Control, Automation and Power, Engineering*, India, 2015.

[24] M. H. Idris, S. Hardi, and M. Z. Hasan, "Teaching distance relay using Matlab/Simulink graphical user interface," *Procedia Engineering*, vol. 53, pp. 264-270, 2013.