21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2017 Grid of the Future Symposium

A Method for Detecting Abnormal Sensor Data Using Multi-terminal Differential Protection Functions

D. COATS, R. NUQUI
ABB Inc.
USA

SUMMARY

We propose and demonstrate a sensor data anomaly detection method which is closely related to multi-terminal differential protection which is then used to provide an additional cyber-physical security layer within digital substations. The disclosed scheme is able to utilize sensor data measurements from existing protective relays in multiple locations within a high voltage circuit and according to the physical laws of the circuit (e.g. Kirchhoff's Current Law), verify the integrity of measurements and protection functions. Measurements from each protective relay within the multi-terminal protection zone can be configured using existing communication infrastructure (Optical Ethernet SFP), time synchronization (IRIG-B), and HMI or other engineering tools. These multi-terminal differential protection measurement settings and logic are used to detect abnormal measurements by confirming a secondary transient logic indicator, based on superimposed currents, at each location and securing the protection and control systems against sensor anomalies introduced either deliberately or unintentionally. A simple notional system is simulated in MATLAB/Simulink with traditional and renewable sources and provides a comparison point between existing multi-terminal differential protection and the proposed method with fast operating Markov Decision Process confirming transient status at a majority of substation terminals.

KEYWORDS

Multi-terminal protection, differential protection, cyber security, digital substation

reynaldo.nuqui@us.abb.com

INTRODUCTION

Substations typically employ a multi-terminal differential protection scheme based on the physical laws of the circuit such as Kirchhoff's Current Law (KCL) that relies on fast communications and distributed sensors. In this scheme, a fault is indicated by the presence of either a differential current signifying a fault current internal or a zero sum indicating a fault external to the monitored multi-terminal protection zone. This type of detection employs multiple calibrated sensors at different locations and could provide a large potential surface for cyber-attack. Sensor data and the accuracy of sensors are therefore very important to protection and control devices and systems in terms of both observability and standard operation. Abnormal sensor data such as increased error or measurement drift, changed instrument transformer turns ratios, or even cyber-attacks on sensor output can cause serious consequences to the proper operations of protection and control systems.

We propose a new protection method to detect changes within a multi-terminal system. This method includes the following key advantages over existing differential protection:

1. Fast Operation: the proposed method is based on a generic Markov Decision Process (MDP), and thus operates at the same speed as such. The proposed method can operate as fast as a protection relay function unit. In principle, the proposed method operates much faster than conventional SCADA based bad data detection algorithms for state estimation by utilizing faster protection functions such as differential or overcurrent protection.
2. Security: the proposed method utilizes multiple sensor data streams and operates according to physical laws i.e. the KCL of the system given a known topology. As long as the high voltage power delivery circuit obeys the established KCL and sensors maintain established calibration, the proposed method can quickly and securely identify problems in sensors.
3. Readiness: Most state-of-art digital relays already have the required modules for MDP schemes and engineering logic built in. This algorithm depends on additional logic for superimposed component calculation such as a superimposed current comparing the instantaneous current with current in a previous historical timeframe or buffer. The proposed method can be implemented directly into modern digital relays with minimal development requirements often using the existing engineering configuration tools as needed on an application to application basis.
4. Compatibility: since the two components closely related to the proposed scheme, the MDP logic and the superimposed component calculation are already implemented and standardized in most relays, the proposed scheme can be compatible with most of the existing protection and control devices, systems, and schemes with differential protection functions. For example, in IEC61850 the PDIF designation defines the logical node for MDP wherein analog or digital input measurements may already be provided.

RESEARCH BACKGROUND AND FRAMEWORK

The core design of the detection method is the utilization and integration of multi-terminal differential protection for sensor anomaly detection. We will illustrate the principle using an example shown in Figure 1. In Figure 1, currents I_1, I_2, I_3 and I_N are measured by N sensors in distributed locations in the power grid. Using these distributed current measurements, the MDP scheme can detect and confirm that a fault happens inside the Protected Zone according to the conditions of KCL:

1. When the sum of all current is zero: No fault is detected in the Protected Zone.
2. When the sum of all current yields a current I_{diff}: A fault is detected in the Protected Zone, and the fault current is I_{diff}.

Figure 1 and conditions of KCL illustrate the basic principle of the state-of-art in multi-terminal differential protection schemes. Current measurements are assumed to be accurate, with additional settings for a bias value in the event that calibration and accuracy differ nominally from expected values. Therefore, the KCL based MDP can accurately detect the fault in the Protected Zone.

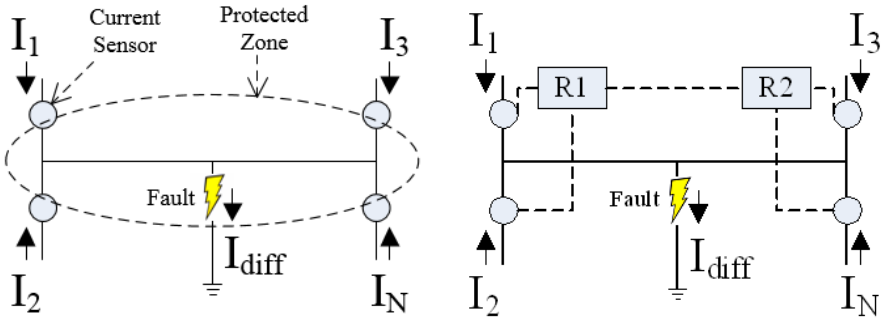

Figure 1 Example Multi-Terminal Differential Protection and Sensor Anomaly Detection using Additional MDP Logic

This provides two key equations for the underlying KCL:

$$I_1 + I_2 + I_3 + \cdots I_N = 0 \; or \; I_{bias} \tag{1}$$

$$I_1 + I_2 + I_3 + \cdots I_N = I_{diff} \; or \; I_{diff} \pm I_{bias} \tag{2}$$

However, in the case of abnormal sensor data due to sensor error, failure, or cyber-attack, the summation of I_1 to I_N may not equal to zero or may be much larger than the configured I_{bias} current. As an example, let's assume the CT turn-ratio of the current sensor measuring I_1 was suddenly changed due to a sensor's internal failure causing the measured I_1 to increase by 10%. This may cause the existing MDP scheme to detect a fault in the Protected Zone with $I_{diff} = 0.1 \cdot I_1$ depending on existing protection tolerances.

However, by circuit analysis in the typical case with normal sensor data, if there is a fault in the circuit, usually all currents I_1, I_2, I_3 and I_N should contribute to the fault current I_{diff}. Hence we should see changes in all four currents. While in sensor failure cases described in the previous scenario, only I_1 from the failed sensor changed, all other 3 currents remained unchanged. Based on this observation, a sensor data failure case rather than the fault case can be clearly detected and the failed sensor can also be identified. The detection scheme can be described as following using the same example in Figure 1:

1. Continuously calculate the superimposed component currents (I_{1F} through I_{NF}) from the current measurements (I_1 through I_N) from each sensor respectively.
2. Also continuously calculate the differential current, I_{diff}, as shown in (2);
3. If I_{diff} and a majority of the N superimposed component currents (I_{1F} through I_{NF}) are greater than predefined thresholds, confirm that internal fault was detected.
4. If I_{diff} and only one of the N superimposed component currents, for example only I_{1F}, are greater than predefined thresholds, a sensor failure was detected and the sensor that measures I_1 was the failed sensor.

The superimposed component current in previous paragraphs is also a common concept in relay protection, which may have many different implementations. The core concept of the superimposed component is to capture and represent the changes in sensor measurements over time. For example, one of the superimposed component implementations is subtracting the previous cycle's samples from the present cycle's samples to obtain the super-imposed current samples as the superimposed component current sample. If there is no change in the current between cycles, these superimposed component samples should always be zero. The following equations describe superimposed current:

$$N_S = \frac{F_s}{f} = \frac{4800}{60} = 80 \; samples/cycle \tag{3}$$

$$I_{F/phase} = I_{N/phase}\,[N] - I_{N\,Buffer}[N - N_s] \tag{4}$$

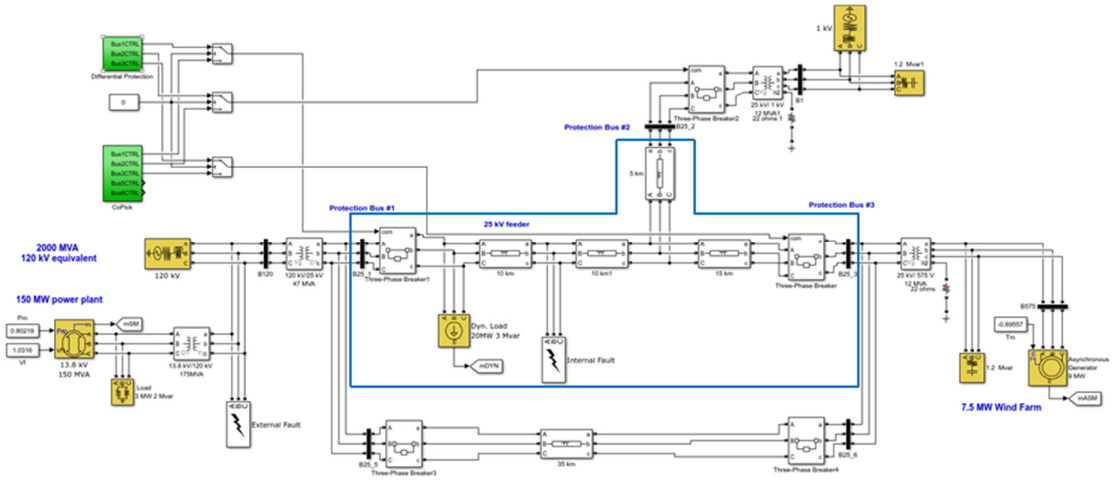

Figure 2 Example tapped line with multi-terminal protection and DER integration

At the principle level, this method for abnormal sensor data detection using multi-terminal differential protection (MDP) scheme can be integrated into state-of-art MDP protection scheme by adding only one set of logical conditions confirming the superimposed current or other transient. This method can share the same topology of most differential protection schemes such as master-master, master-slave, centralized, and distributed configuration.

SIMULATION AND RESULTS

To demonstrate this multi-terminal differential protection confirmation algorithm, a simple notional power system is developed within MATLAB/Simulink software. This simulation has a 120kV equivalent source with an additional 150MW power plant for generation. Distribution is at 25kV from a 35km section of transmission line utilizing a three phase Pi section line that has been tapped near the receiving side by a 5km segment with attached transformer and industrial load. At the receiving side there is a small amount of generation from a 7.5MW wind farm along with an industrial load. A second 35km line provides N-1 protection for the receiving side load. This is illustrated in Figure 2.

This system is simulated with two protection systems: 1) simplified differential multi-terminal detection and 2) a logical Markov decision process verifying differential protection with the superimposed current as described previously. The system is tested under conditions of a fault internal to the multi-terminal protection, an external fault, and a measurement fault caused by a sudden, unexpected change in CT ratio. To this end, the actual measuring system of the protective relay device is modelled simulating an analog front end, ratio and gain settings, measurement error and noise, and idealized 16-bit quantization and 4800 Sa/s sampling. This digitalization is shown in Figure 3. The threat modelled in this scenario is someone gaining access to the digital protective relay or merging unit and changing instrument transformer ratio gain settings or injected a false digital signal to control logic.

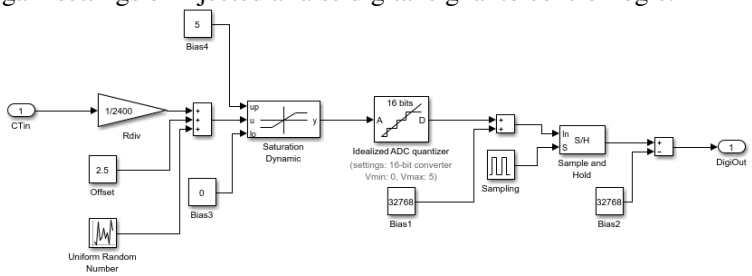

Figure 3 Measurement and digitalization of CT inputs with gain settings and added noise

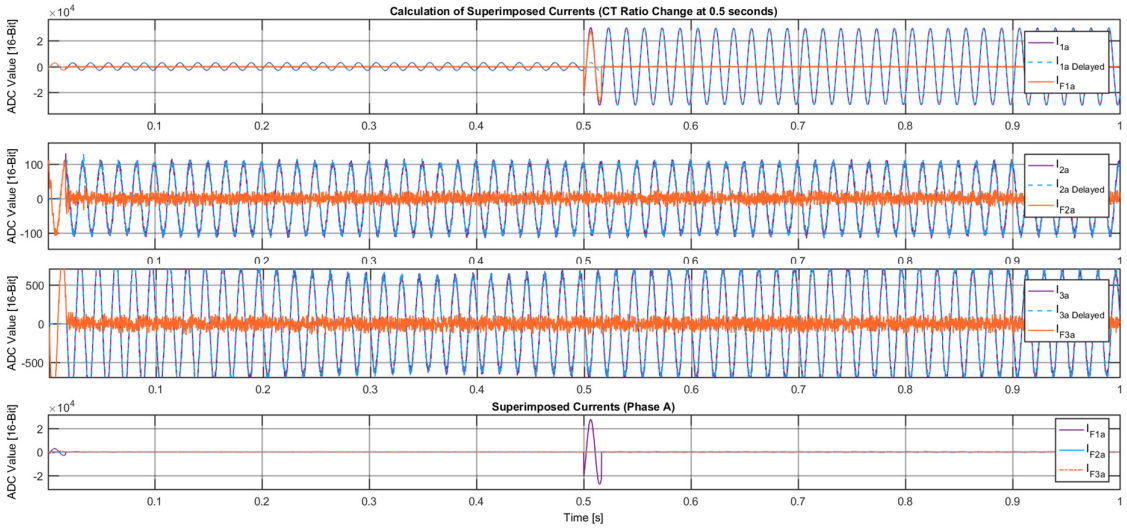

Figure 4 Change in CT ratio detected by superimposed current

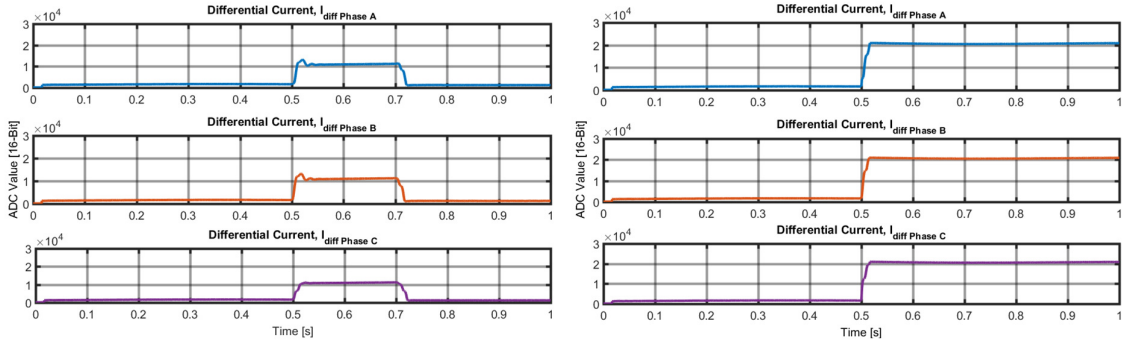

Figure 5 Differential protection function under internal 3 phase fault from 0.5 to 0.7s (Left), differential protection function with CT ratio change at 0.5s (Right)

The multi-terminal protection zone defined in Figure 2 is the current at three locations on the 25kV line shown as buses 1-3 with measured three phase currents I_1, I_2, and I_3. The goal of the simulation is to verify that differential protection does not operate in the event of an external fault but will selectively detect faults internal to the measurement zone utilizing the proposed additional logic. Part of the enhanced decision process of the proposed method is determining if a fault is confirmed at multiple locations using fast communication infrastructure, before action is taken. This may result in a decision to refrain from the typical control operation or send a warning to the HMI and operator relative to possible senor measurement tampering or anomalies.

Figure 4 shows the result of a sudden change in the current transformer gain setting from 1/2400 to 1/240 as well as the superimposed current used for the added logic of the proposed method. Each plot shows a single phase from bus 1 through bus 3 of the multi-terminal protection zone, phase A for comparison, and compares the currents I_1, I_2, and I_3 with the delayed current from the previous cycle. For each of the unchanged current measurements, the only difference between the most recent sampled data and the delayed waveform is the difference in noise and calibration, which results in a white noise floor at the noise level. However, the sudden change in CT ratio causes the measured differential current provided to protective relay logic functions to increase drastically and as shown in Figure 5, this is easily comparable to a three phase fault within the multi-terminal protection zone. Figure 5 compares an internal fault detected by multi-terminal differential protection (left plot) with the simulated sensor anomaly (right plot) where each plot represents the differential current of a single phase measurement in the digital relay. In the typical protection scenario, this type of sensor anomaly could cause a sustained trip condition and/or repeated reclosing or other mitigation action.

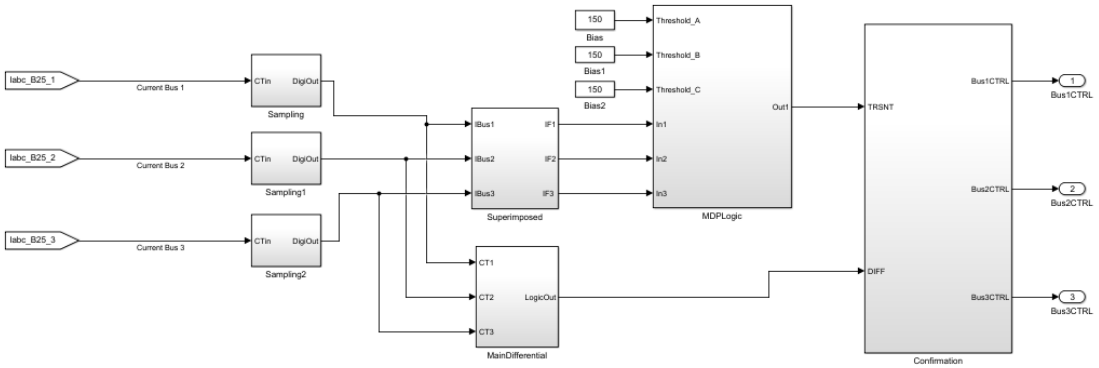

Figure 6 Overview of implemented protection and confirmation functions

The implemented logic is shown in block diagram form in Figure 6. This logic will be verified with three key conditions. First, the logic should detect internal fault conditions such as those in Figure 5 (left). When a fault is simulated inside the protection zone, the MDP provides the logic signals of Figure 7 confirming the trip signal. Second, the logic should detect measurement anomalies during normal operation and either block operation of the differential logic or issue a warning. Figure 8 shows a blocking scheme when the measured current is affected by the sudden change in CT ratio at Bus 1 and normal current within each other bus (zoomed in for more detail). This detection scenario under standard differential protection was shown previously in Figure 5 (right). Last, the logic should not provide false tripping during fault conditions external to the protection zone. This detection scenario is show in Figure 9 with magnification on I_2. Here the superimposed current detects a transient event at all protection zone buses but no trip signal is issued because there is no differential current.

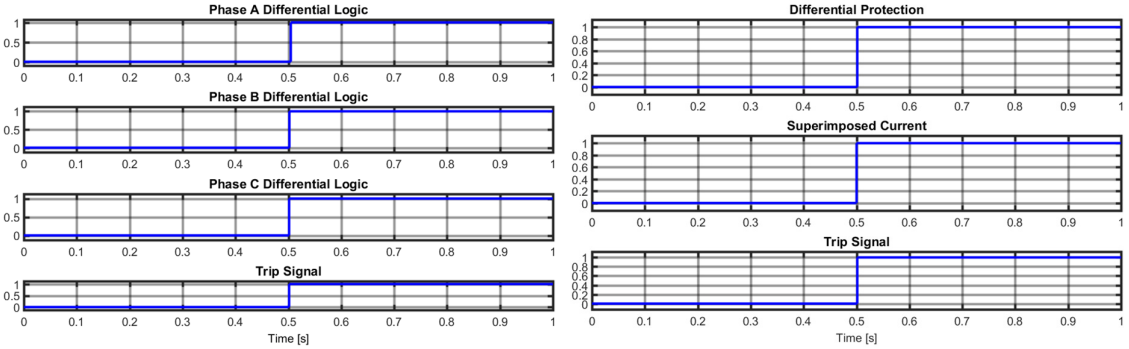

Figure 7 Modified multi-terminal differential logic during internal fault

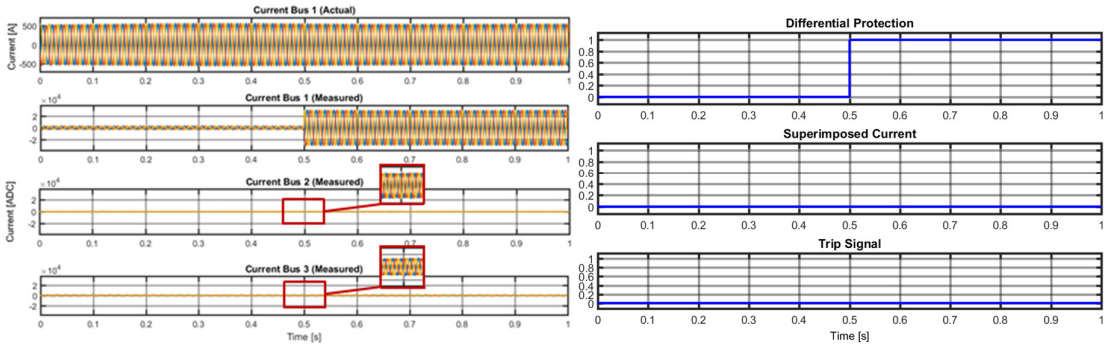

Figure 8 Modified logic during sensor ratio change, no trip signal is issued

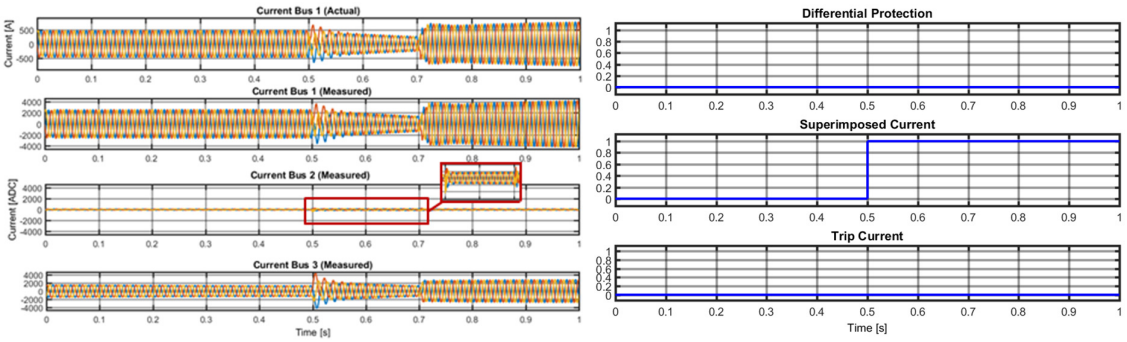

Figure 9 Modified multi-terminal differential logic during external fault, superimposed current detects a transient event but no trip signal is issued

CONCLUSION

We have proposed a multi-terminal differential protection scheme that also allows for detection and identification of sensor anomalies in measurement devices based on a transient detection logic. This technique uses existing logical variables to verify that each terminal in the protection zone sees a given internal fault and allows normal operation of differential protection with little to no additional computation overhead. Verification has been accomplish using a MATLAB/Simulink simulation. The method is fast, interoperable with existing systems, and provides and additional cyber-physical defence layer against potential malicious actors. The protection scheme could work within digital substations utilizing IEC61850 sampled values or GOOSE messaging as well as within relays capable of logical processes. Future work could focus on faster methods of transient event protection or new and emerging multi-terminal differential protection methods that further leverage the flexibility of IEC61850 communication speed and semantic features.

BIBLIOGRAPHY

[1] R. Nuqui, “Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF),” U. S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE), 2014 [Online]. Available: https://www.controlsystems roadmap.net/Efforts/Pages/CODEF.aspx

[2] R. Nuqui and L. Tang, “Collaborative Defense of Energy Distribution Protection and Control Devices,” U.S. Patent 2009/0299542 A1, Dec., 3, 2009.

[3] A. Martin, R. Nuqui, J. Hong, A. Kondabathini, W. Rees, D. Ishchenko, “Collaborative Defense of Transmission and Distribution Protection and Control of Devices against Cyber Attacks (CoDef)” Western Protection Relay Conference, October 2016

[4] S. Dambhare, S. A. Soman and M. C. Chandorkar, "Current Differential Protection of Transmission Line Using the Moving Window Averaging Technique," in IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 610-620, April 2010.