Issue 1 vol 4 ISSN: 2321-8134

IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

Differential Protection of Transmission Line Using Wi-fi Protocol : A Review

Nikhil S. Bijwe[1], Kavish K. Morey[2], Atul S. Dakhare[3], Pratik P. Jadhao[4]

[1]*Nikhil S. Bijwe, Dept. of Electrical Engg. JDIET Yavatmal, Maharashtra, India,* ***nikhilsbijwe96@gmail.com***
[2]*Kavish K. Morey, Dept. of Electrical Engg. JDIET Yavatmal, Maharashtra, India,* ***kavishmorey123@gmail.com***
[3]*Atul S. Dakhare, Dept. of Electrical Engg. JDIET Yavatmal, Maharashtra, India,* ***dakhare70@gmail.com***
[4]*Pratik P. Jadhao, Dept. of Electrical Engg. JDIET Yavatmal, Maharashtra, India,* ***pratk.jadhao7@gmail.com***

Abstract

The probability of fault occurrence on the overhead lines is much higher due to their larger lengths and contact with atmospheric conditions. There are quite a few methods available for the protection of transmission lines and distribution lines. Pilot wire differential protection is one of the most common technique for protecting short transmission lines. Current differential protection using pilot wire is applied typically on transmission line as the main protection. The conventional protection scheme has downsides, such as failure due to line disconnection and limited line length. A review on of transmission line protection using Wireless Fidelity (Wi-Fi) communication protocol for data sharing between the relays located at the two ends of the transmission line is presented in this paper. The protection algorithm is based on current signals measured at both ends of the transmission line. The data is exchanged through the wireless communication network. The relay resolve is based on data sharing obtained through wireless communication network. The suggested technique satisfies high degree of reliability and stability.

Index Terms—Digital protection, transmission lines protection, wireless communication, Wi-Fi protocol.

---------- *** ----------

1. INTRODUCTIONS

Nowadays there are several problems associated with electricity. The flashover of lightning and other faults in the transmission line leads to shortage of electricity. There are several methods to overcome this problem and one such method is implemented in this paper. Differential protection can be done through pilot wires and also throughout wireless communication. Pilot wire differential protection is one of the most common methods for protecting short transmission lines. The main requirements of line protection are that in the case of a short circuit, the circuit breaker approximate to the fault should open, all other circuits remaining in a closed position. The conventional protection scheme has several drawbacks. The differential protection is applied only with the help of pilot wires. These methods are previously used in transformers, generators and bus bars since small length of pilot wires are required. The pilot wires are made up of aluminium and copper wires, but the cost is large. The transmission line requires lengthy wires to follow the procedure so it is not economical.

The length of the line that can be protected by the pilot wire differential protection is limited by the effect of resistance and capacitance of the pilot wire. More over the relay function may be lost due to line disconnection. The wire link also needs additional protection. Communication system approaches and interface techniques are one of the most important parts in the process of monitoring, control and protection of power systems. There are several advanced communication techniques that can be used to better protection, control, speed outage restoration, operation analysis, maintenance and planning. These communication facilities also allow engineers to exchange operation, test and maintenance information with the neighbouring utilities, and access real time and historical relay information [4]. In this paper the wireless communication network allows the exchange of information among the protection relays. The exchange of information among the relays assists the protective relays to make the correct resolve.

a) Differential protection using pilot wire

In differential pilot wire protection the receiving end substation primary CT connected to sending end substation secondary CT through pilot wire. Both CT currents are compared and if any variation in current value is absorbed the relay starts to operate which in turn operates a circuit breaker. The resistance in the wires will limit the use on long distance lines. The use is mostly restricted to distance upto 15 km.

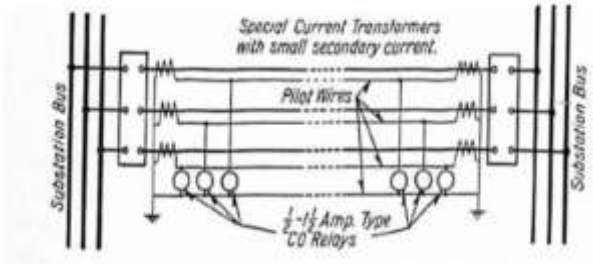


Fig 1 schematic diagram of exciting system – i

Drawbacks of differential pilot wire protection

- If length of pilot wire increases cost is much higher
- Due to long length capacitance and inductance effect increases changes in current value is absorbed.

b) Carrier line differential protection

Receiving end CT current is converted to digital signal with high frequency transmitted through same power line to the sending end. At sending end higher frequency digital signal is converted to analog current value using line trap, coupling capacitor, etc.

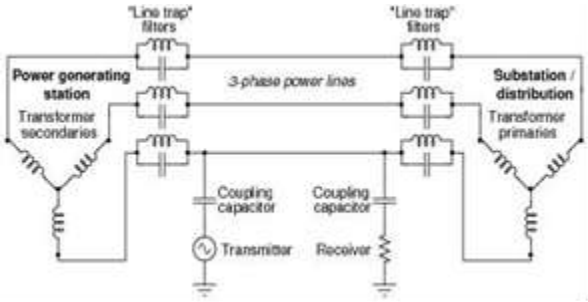


Fig 2 schematic diagram of exciting system - 2

Drawbacks of carrier line protection

- If there is any fault in long transmission line power frequency signals are not absorbed.
- Additional equipment's are required.

The protection system for transmission lines proposed in this paper consists of two relays, one located at the sending end and the other at the receiving end. The two relays make the final resolve based on the shared information (current signals) sent through a wireless communication network [5], Fig. 3. Communication protocols are the rules that govern the transmission of data in the system. Selecting protocols is as critical as selecting the physical media to determine the performance of the communication network. The protection scheme is based on sharing the measured current signals throughout a wireless communication network. The wireless network standard, Wireless Fidelity (Wi-Fi), is used in this work.

Applying this technology in transmission line protection satisfies the following features.

- Synchronized measurements.
- Resolve is not stand alone based.
- Information exchange with the neighbours.
- Relays behave adaptively according to any change in system parameters.
- Wireless communication (no need for pilot wires).
- Lower cost compared to leased lines.
- Faster response time.

A differential protection using Wi-Fi communication protocol for data sharing between two relays located at the two ends of the transmission line is presented in this paper.

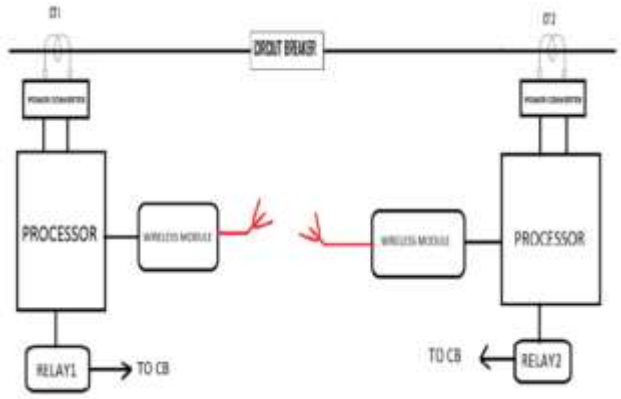


Fig. 3 Basic Block Diagram Of Wireless Communication

2. OVERALL STRUCTURE OF THE LABORATORY MODEL

The system consists of four main parts.

- Power system physical model.
- Transducers and data acquisition cards.
- Wireless Communication protocol (Wi-Fi).
- Two Digital (Computer) Relays.

Main parts of the system used to test the proposed technique for protecting the transmission line are shown in Fig.3.

breakers, two sets are used at the two ends of the transmission line and the third breaker is used to apply the fault along the transmission line.

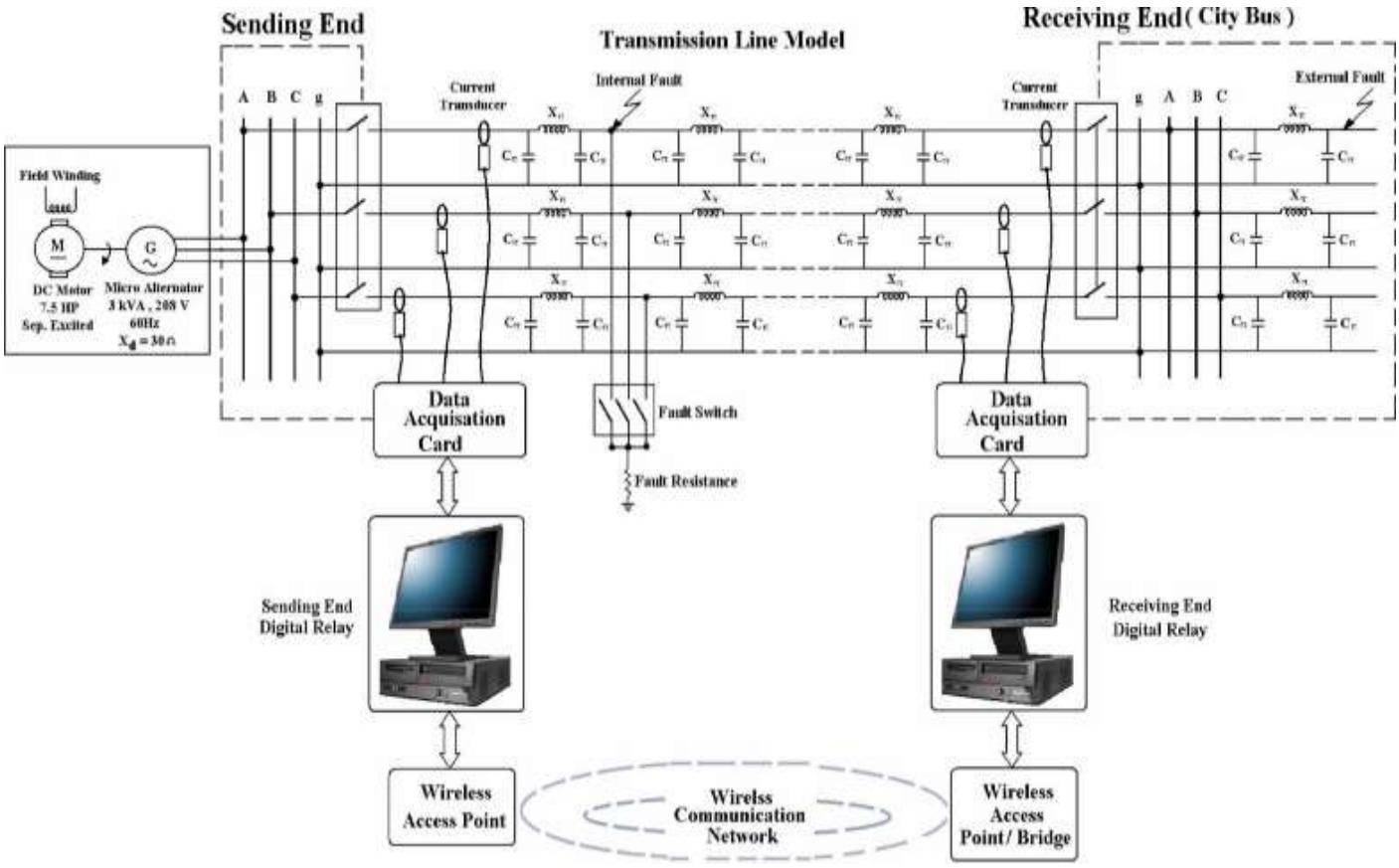


Fig. 4. Main parts of the protection system.

2.1. Power System Physical Model

A single machine infinite bus power system was physically model in the power research laboratory at the University of Calgary. The physical model represents a large system of approximately 600 MVA.

A three-phase 3-kVA, 20 8-V synchronous micro- alternator driven by 7.5 hp separately excited dc machine is employed to model the generating station. The station is connected to a constant voltage system (infinite bus) through a transmission line. The micro-alternator has a 60-Hz direct axis inductive reactance, X_d, of approximately 30 Ω. The amount of transferred power as well as the power factor at the micro-alternator terminals can be adjusted.

The transmission line was model by a lumped element physical model consisting of six identical Π-sectio8ns, each section representing 50 km of a 500-kV transmission line, cascaded together to form 300-km line length [6]. Each Π section consists of two shunt capacitors, C_Π, with capacitance 7.5 μf each and one inductor with a 60-Hz inductive reactance, X_Π, of 0.7 Ω and an internal resistance of approximately 0.1 Ω. A system of three 3-phase circuit breakers (CBs) controlled by a ROM based logic circuit is used. Out of the three sets of breakers, two sets are used at the two ends of the transmission line and the third breaker is used to apply the fault along the transmission line.

The proposed protection scheme is recommended to apply for short transmission lines up to 30 km even though the studies in the lab have been performed on a 300-km equivalent transmission line model to test the performance of the protection scheme.

Any type of fault can be applied to the power system model. Fault location and fault resistance can also be changed. By changing the armature and field currents of the dc motor, the power of the micro-alternator and thus the load on the transmission line also can be changed.

2.2. Transducers and Data Acquisition Cards

Line currents are used as the input signals to the current differential relay. The currents are obtained through three current transducers. The current transducers convert the current signals to low voltage signal suitable for the input channels of the data acquisition card which operates with input voltage signals The purpose of the data acquisition card is to convert the analog data into a form usable by a digital processor (DAC). The data acquisition card is characterized by 14-bit input resolution, eight input channels single ended or

four input channels differential and the sampling rate is 48 kHz. The digital to analog convert is adjusted to operate in differential

mode. Three input channels for three phase currents are used with a sampling frequency of 10 kHz for each channel.

2.3 Wireless Communication Protocol (Wi-Fi)

The wireless network technology is defined by the IEEE 802.11 family of specifications. There are currently several specifications in the family: 802.11, 802.11a, 802.11b, 802.11g, and 802.11n. All of them use the protocol Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The 802.11 standard applies to wireless networks and provides 1- or 2-Mbps transmission in 2.4-GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

Wi-Fi is 802.11b standard, which operates in the 2.4-GHz band, transfers data at 11 Mbps and uses only Direct Sequence Spread Spectrum (DSSS). There are two different types of Wi-Fi technology.

1) The first type is called Peer-to-Peer networking, which consists of a number of stations, each equipped with a Wireless Networking Interface Card (WNIC). Each station can communicate directly with all of the other wireless en-abled stations. They can share files but may not be able to access wired network resources.
2) The second type of Wi-Fi is called an Access Point (AP). In this type, the AP acts like a switch, providing connectivity for the wireless stations. It can connect or bridge the wireless network to another wireless network or to a wired network. The AP, even called "Hotspot", transmits a radio
frequency over an area of several hundred feet.

The second type of Wi-Fi technology is applied in this paper. Wi-Fi is a powerful advance in computer networks and communications. As any new technology, Wi-Fi has its own advantages. Unlike packet radio systems, Wi-Fi uses unlicensed radio spectrum. As a result, the economic basis for its implementation is completely different. The success of Wi-Fi has made it possible to look to the unlicensed spectrum as the future of wireless ac-cess, rather than the spectrum licensed and controlled by large corporations.

2.4 On Site Data Preparation

As a first step, the relay at each end receives current signals. The current signals are stored in a data file at that end. A common format for the data and control files are needed for interchange of the data and fault types between the communicating stations.

The relays receive analog signals. So the second step is to convert the measured signals to digital values. The conversion from analog to digital is carried out through three processes: sampling, quantizing and encoding. For efficient reconstruction at the receiving end, a proper anti-aliasing filter and high sampling rate must be used. The recorded values in the data file are applied in a sequence of row by row to the Analog-to-Dig-ital (A/D) conversion device. As a result, the output of the analog to digital is a bit stream which is compress in Wi-Fi frame prior to ex-changing the data with other stations.

To construct this frame, the digital values are picked up as an application data and passed through the layers of the Open System Interconnection (OSI) model as shown in Fig. 4. Each

layer defines a family of functions needed to allow the transmitted frame to reach its destination in a right way. The frame structure for Wi-Fi data frame is shown in Fig. 4.

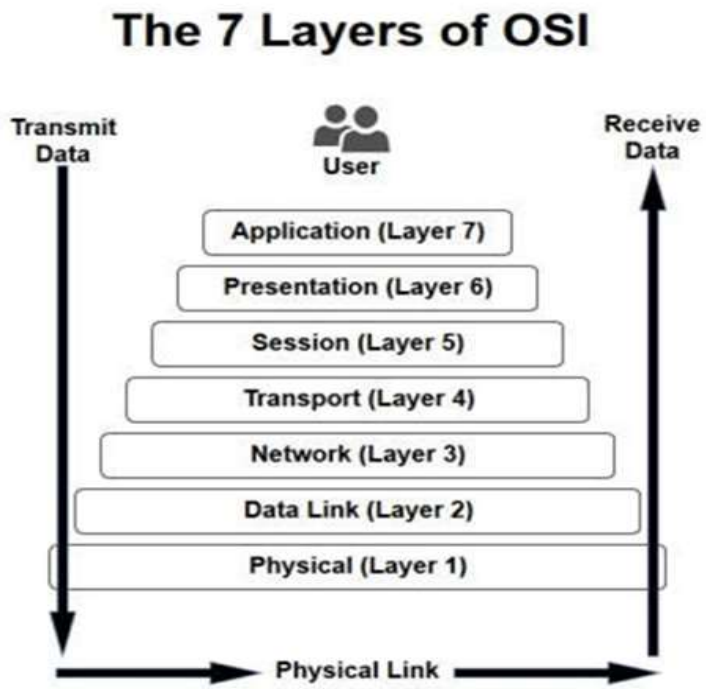


Fig. 5. Open System Interconnection (OSI) model.

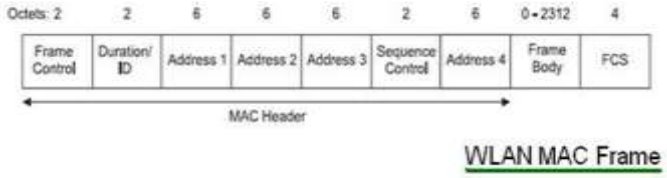


Fig. 6. Wi-Fi packet frame format.

The data frame holds up to the following four addresses given below.

- The Source Address (SA).
- The Destination Address (DA).
- The Transmitter Address (TA).
- The Receiver Address (RA).

The SA is defined as the Medium Access Control (MAC) address of the device that originated the frame. The TA is the address of the device that sends the frame into the wireless medium. The RA is the MAC address of the device that receives the wireless frame. The DA is the MAC address of the last device in the system to receive the frame. The Wi-Fi frame also contains MAC header and a variable length frame body that holds the data. The data body can vary from 0 to 2312 bytes. The MAC header is divided into a frame control field, sequence

control and the four MAC addresses. The data frame also includes a Frame Check Sequence (FCS) to check the packet

transmission error for the Wi-Fi protocol uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based Medium Access Control (MAC) protocol with Request to Send/Clear to Send (RTS/CTS) medium reservation. In this

protocol, each wireless end listens for activity in the radio channel before starting transmission. To ensure the smooth and fair functionality, Distributed Coordination Function (DCF) includes a set of delays that amounts to a priority scheme. One of these delays is known as an Inter Frame Space (IFS). Two values for IFS are used, shortest ISF (SIFS) is used for all immediate response action and Distributed Coordination Function IFS (DIFS) is used as a minimum delay for asynchronous frames contending for access.

The process of information sharing between the two ends is summarized here. When a packet is to be transmitted, the transmitting node (for example end "1") first senses the medium. If the medium is sensed free, it waits to see if the medium remains idle for a time equal to DIFS. If so, the end may transmit its packet immediately. But if the medium is sensed busy (either because the end initially finds the medium busy or because the medium becomes busy during DIFS idle time), the end defers transmission and continues to monitor the medium until the current transmission is over. Once the current transmission is over, the station then uses a back off window procedure in which a random number of time slots are select. If the media is sensed busy during the back off window, the back off timer is paused and resumed when the media is sensed free again.

In order to ensure that the data frame is successfully transmitted, the transmitting end firstly sends out a short Request-To-Send (RTS) frame. If the receiving end hears the RTS, it should immediately respond with a short Clear-To-Send frame if it is ready to receive. All other ends receive the RTS and defer using the medium.

When the frame is received successfully, as determined by a Cyclic Redundancy Check (CRC), the receiving end (end "2" in this example) transmits an Acknowledgment (ACK) frame after waiting only for an SIFS gap. When the transmitting end receives an ACK, it immediately (after SIFS) sends the next frame in the sequence [9].

The wireless network may be affected by other radios or devices operating on the same wave band which is defined by interference. In unlicensed bands like 2.4 and 5.8 GHz, there is any number of signals from other devices that might cause interference. The Smart Antenna overcomes interference from other radios with circular polarization. Unlike regular vertically or horizontally polarized antennas, circularly polarized antennas are less chances to interference from other radios operating in the same wave band. Unauthorized use of the network is a serious concern for wireless network operators. Illicit users rob the network of bandwidth and resources in addition to constituting an information security risk for the users on the network. Typical Wi-Fi security has been faulted for being weak. Smart antenna products reduce these

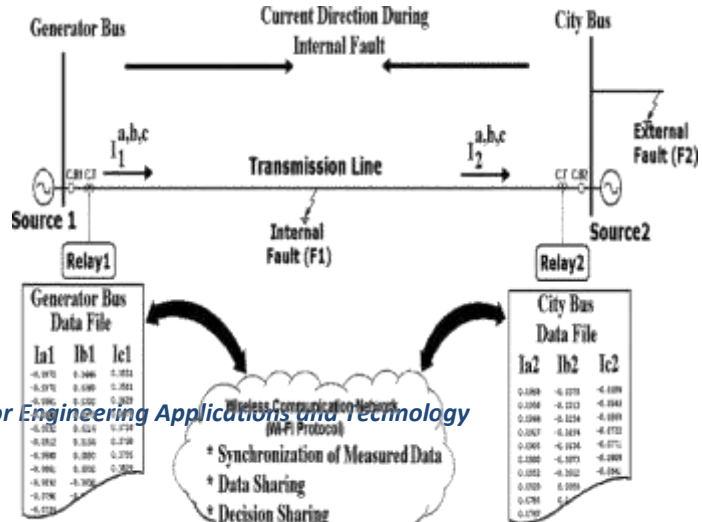
weaknesses by employing several advanced methods for securing a wireless network.

Wi-Fi Protected Access (WPA) security solves this problem with advanced coding in addition to providing confirmation.

For coding, WPA uses a method called Temporary Key Integrity Protocol (TKIP). TKIP requires that the key be changed frequently. It first determines which keys will be used, then transmits the global key to each users on the network and validates the security settings of the users.

WPA also uses Message Integrity Code (MIC) to validate the data sent and received on the network. This provides a "trusted" source for each packet of data on the network preventing rogue users from spoofing connections. WPA also confirmations users onto the network. The combination of strong coding and confirmation has made WPA the choice of several security professionals securing wireless networks. In fact, several government wireless networks now require WPA.

An additional way of controlling access to a wireless network is MAC address filtering. Each user bridge or users device that can access a wireless network has a MAC address coded into its network adapter. These addresses are unique and advertised to the access point when requesting access to the network. Smart Antenna products allow connections to be refused if their MAC address is not on an approved list of MAC addresses. To grant access to a network, the MAC address is easily entered into the access point. Any users that does not have its MAC address on the approved list is simply not granted a connection.



- Resolve Element.

Fig. 7. Power system configuration.

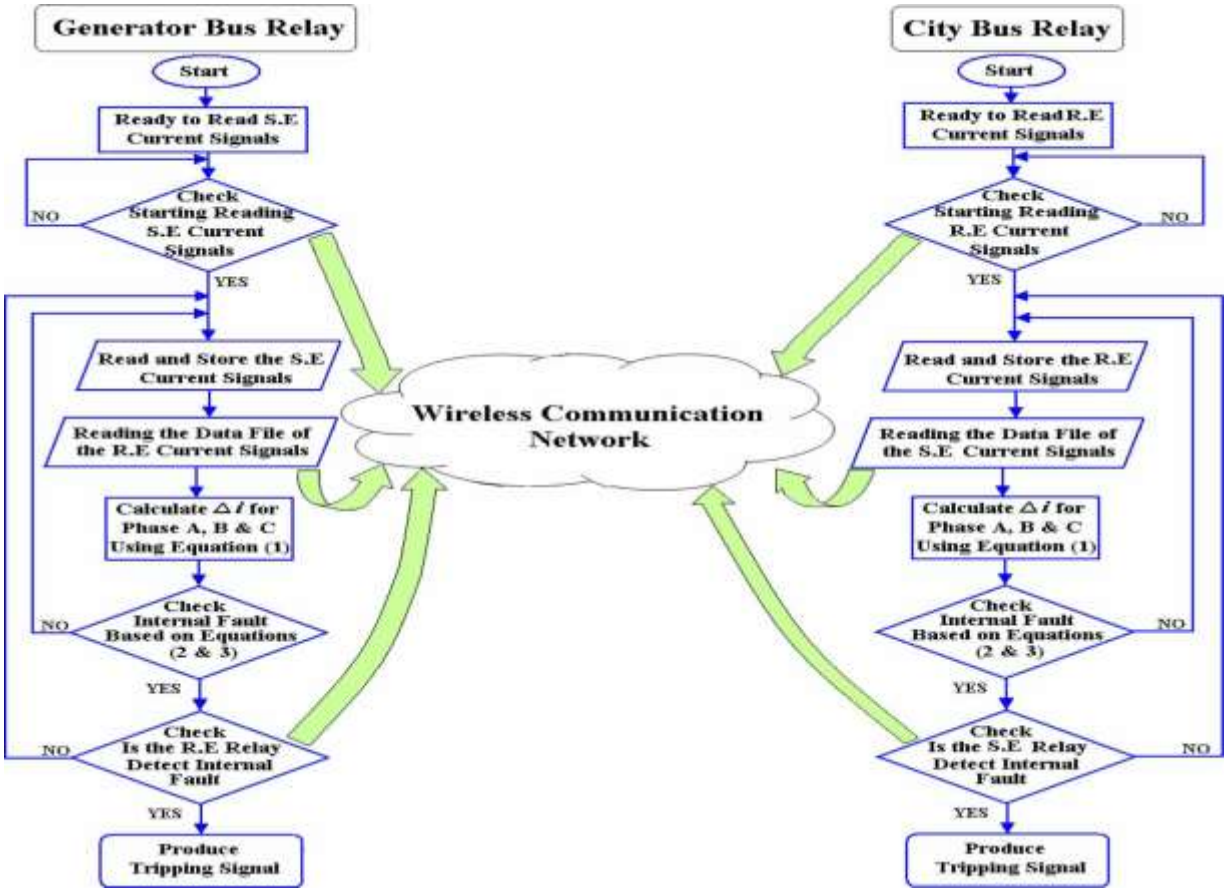


Fig. 8. Flowchart of the digital relays at both ends of transmission lines.

2.4. Digital Relays (Computer Relays)

Two PC computers are used to virtually simulate the IED relays. One of them is located at the sending end and the other at the receiving end. The computers in this case are functioning as digital relays. The two computers are identical and the specification of each one is P IV GX 1.6-GHz and 640-MB RAM.

3. PROTECTION SCHEME

The protection scheme is based on measuring the current signals only at both two ends of the transmission line. The power system configuration is shown in Fig. 6.

The suggested technique can be explained through an analysis of three key components.

- Synchronization Element.

A. Synchronization Element

To evaluate the differential protection based on current signals measured at both ends of the transmission line, the current samples have to be taken at the same time on both terminals. This requires that relay clocks be synchronized; any time difference between the relays clocks will translate into a differential current that may cause a relay to misoperate.

There are several methods used for synchronizing the data measured at both ends of the transmission line. In most of these techniques there is a need for additional equipment or connecting equipments to the satellites which increases the cost of manufacturing the relays.

In the suggested technique the wireless communication network is used for synchronization of the current signals in both relays. When the two relays are connected they are ready to read the current signals. The two relays continually check

the content of the running data file zero or one. The two relays start to read the current signals when a change in the content of the running data file changes from zero to one. The two relays have the ability to change the content of the running data file to start the relay operation. The above process of synchronization results in a time delay of about 2 μsec due to sending a Wi-Fi packet of data required to change the content of running data file to let the two relays start to record the current signals.

B. Resolve Element

These current signals are compared with the corresponding current signals for the same part of the previous cycle. The comparison can be mathematically explained as below:

For Normal Operation and External Faults:

$$|\Delta i^{a,b,c}| - |\Delta i^{a,b,c}_{pre}| . \quad (2)$$

For Internal Faults:

$$|\Delta i^{a,b,c}| > |\Delta i^{a,b,c}_{pre}| \quad (3)$$

where the subscript "pre" refers to the values in the previous cycle.

The final resolve is also exchanged between the two relays to help the relay make an accurate resolve. Flow chart of the digital relay program at both ends of the line is shown in Fig. 6.

5. CONCLUSION

A systemfor using Wi-Fi communication protocol for data sharing among the relays located at both ends of the transmission line is demonstrated. The protection algorithm applied in relays at each end of the line is based on current signals measured at both ends of the transmission line and exchanged through the wireless communication network. A wireless communication network supported with Wi-Fi protocol is suggested for data handling. The wireless communication network offers advantages over conventional techniques such as no pilot wire that can break, faster response, lower cost compared to leased lines. An accurate resolve is obtained from the proposed protection scheme because the relays exchange the quantities and the final resolve between them.

ACKNOWLEDGEMENT

As we present our paper on "Microcontroller based Agriculture System by Using Solar Power Generation.", We take this opportunity to offer our sincere thanks to all those without guidance this paper, might have remained a dream for us. We express our deepest gratitude and thanks to Prof. A.D. Borkhade whose guidance and ideas channelled our conscientious endeavours towards the paper. We have been fortunate enough to gave us freedom, support and whole hearted co-ordination for the completion of our paper.

REFERENCES

[1] S. H. Horowitz and A. G. Phadke, *Power System Relaying*. Taunton, U.K.: Research Studies Press, 1992.

[2] I. Voloh, R. Johnson, and G. E. Multilin, "Applying digital line cur-rent differential relays over pilot wires," in *Proc. 58th Annu. Protective Relay Engineers Conf.*, Apr. 2005, pp. 287–290.

[3] M. Yalla, M. Adamiak, A. Apostolov, J. Beatty, S. Borlase, J. Bright, J.Burger, S. Dickson, G. Gresco, W. Hartman, J. Hohn, D. Holstein, A. Kazemi, G. Michael, C. Sufana, J. Tengdin, M. Thompson, and E. Udren, "Application of a peer-to-peer communication for protective relaying," *IEEE Trans. Power Del.*, vol. 17, no. 2, pp. 446–451, Apr. 2002.

[4] X. R. Wang, K. M. Hopkinson, J. S. Thorp, R. Giovanini, K. Birman, and D. Coury, "Developing an agent-based backup protection system for transmission networks," in *Power Systems and Communications In-frastructures for the Future*, Beijing, China, Sep. 2002.

[5] K. M. Abdel- Latif, M. M. Eissa, A. S. Ali, O. P. Malik, and M. E. Masoud, "Laboratory Investigation of Using Wi-Fi Protocol for Transmission Line Differential Protection" ,IEEE Transaction on Power delivery, Vol. 24, no. 3, July 2009.

[6] M. M. Eissa, A. S. Ali, M. E. Masoud, and K. M. Abdel-Latif, "A new protection scheme for short transmission lines using IEEE 802.11 protocol" , in Proc. 11th Int. Conf. Transmission and Distribution Construction, Operation and Live-Line Maintenance (ESMO 2006), Oct. 15–19, 2006.

[7] I. Hall, P. G. Beaumont, G. P. Baber, I. huto, M. Saga, K. Okuno, and H. Ito, "New line current differential relay using GPS synchronization," in Proc. IEEE Power Tech Conf., Bologna, Italy, Jun. 23–26.

[8] G. S. Hope, O. P. Malik, and M. E. Ramsy, "Digital transmission line protection in real time", IEE Proc., vol. 123, no. 12, pp. 1349–1354,Dec. 1976.