

A personalized Wireless Sensor Network Communication Model for computerization of Electric Power Distribution

S.V.Saravanan, Dr.C.Sharmeela, Dr.Chandan Majumdar

Research Scholar, ECE Dept, Allahabad University,

EEE Dept, Anna University, Chennai,

ECE Dept, Allahabad University,

Abstract: Automation of electric power distribution in a load point by providing reliable manner and cost-efficient can be accomplished by complete automation of the central control centre which coordinates the operation of several area centers while ensuring security of supply against loss of generation, transmission capacity, maintaining the voltage, current and frequency of the system within specified limits, temperature, pressure, and oil level of the transformers is required. Currently, automation is done with the help of Supervisory Control and Data Acquisition (SCADA) and Intelligent Electronic Devices (IEDs). A novel method is proposed in this paper about communication among the sensors. In this paper the cooperative wireless sensor network architecture for communication of the monitored signals and the employment of a virtual MIMO model, which would considerably reduce errors due to transient surge of charges and other interferences were discussed. Further, the paper proposes the use of a location aware protocol, GEAR, which is suitable for the sensor network architecture, as compared to the currently used protocols. The appropriate placement of sensors and adoption of additional signaling schemes can also prevent theft of electrical power, which is not a new problem in many areas.

Key words: Geographic and Energy Aware Routing (GEAR), Supervisory Control and Data Acquisition (SCADA), Intelligent Electronic Devices (IEDs).

I. Introduction

The application of sensor networks is becoming ever-present, and this paper introduces a new area of application of the sensor nets viz. in the automation of electrical power distribution. The automation of power distribution can be made well-organized in terms of energy utilization, speed, and bandwidth necessities from beginning to end to the application of sensor nets. The efficient elements that achieve security control and monitoring of the various signals are the sensor networks. The essential fault analysis system should provide results of a complete system-wide analysis of an event to the system dispatchers and safety engineers within seconds of the event happening. This may not be feasible with the existing SCADA technology. Wei Ye et al. [4] mention that the major drawback of current SCADA systems is that they are static, inflexible, and often have a centralized architecture. Further, there may be increased operational risks [8] associated with an inconsistent level of staff operational competency. In that case, the human intervention in decision making has to be minimized. In the proposed communication model, the processing of data signals by a single control centre (master) processor is decentralized, and the processing of information may be done in a distributed manner. Each sensor node may have a battery for its operation. The nodes are asleep, and unless there is a significant change in the measured parameters, only then they transmit. This avoids redundant transmission and hence saves a considerable amount of power and complex wiring to link all these sensors to the control equipment is eliminated through low power wireless transmission. The bandwidth requirement is least since the transmissions are mostly limited and are done only when necessary. The process of communication among the sensors is divided into the following phases: The long-haul transmission of signals to the monitoring (HMI) stations by strategic placement of the sensor clusters and implementing the location-based GEAR protocol and the communication of signals within clusters of the sensors that are in close proximity to each other on a virtual MIMO basis.

The paper proposes the use of a location-based routing protocol called GEAR (Geographic and Energy Aware Routing) that implements energy efficient geographic packet forwarding techniques. The GEAR protocol is energy efficient on its own, and it would make possible faster communication. The location of sensors can be obtained by means of a hardware system (GPS) or by irregular beaconing. Since in the electric distribution network the sensors are rather static, the location information need not be transmitted frequently. This reduces the overhead in routing, as compared to other sensor networks scenarios. The broadcasting of information sensed by the sensors or a question that is sent by the base station is a primary need in the automation of power distribution. The broadcasting of data is done in a faster manner by use of the GEAR protocol. The assumption made [2] is that the energy consumed for processing is far

less than the energy required for transmission or reception. Therefore, with the aim of achieving an energy efficient routing, the number of transmissions and the transmission power are minimized considerably.

II. Current Scenario

The substation automation and integration can be broken down into five levels:

- ❖ The uppermost level is the utility enterprise level that consists of software that is integrated with the entire system.
- ❖ The middle levels implement the Intelligent Electronic Devices (IEDs), which integrates using data concentrators, and substation automation applications.
- ❖ The lowest level is the power system equipment, such as transformers and circuit breakers.

The single processor of the data concentrator, or similar equipment, aggregates the readings of a number of sensors. The readings may be current, voltage level, or frequency readings from the IEDs [6], circuit breaker status, winding temperature, and oil level in the transformers, etc. Apart from this at the power station water level, volume of flow, fuel consumption, and many other data are monitored. A microcontroller-based static relay may take switching decisions. In this process, there may be protocol translations [3] to identify data from the various IEDs. The IEDs are all connected through high-speed LANs to the data concentrator. In other words, there is one processor to process and combined readings from a number of sensors. Then, the RTUs (Remote Terminal Unit) may transmit information carrying signals to the SCADA centers or control signals to the appropriate equipment based on the information available. Kezunovic et al. [7] explain that the system level monitoring of CB status can be monitored and analyzed by CBMAs. There is constant monitoring of signals at SCADA master centers with the help of human machine interface. For a large interconnected power system, the tasks of operation, coordination, supervision, and protection become complex, and the automation system faces the following problems:

- ❖ Generated active and reactive power of each station in the group.
- ❖ Net active power and reactive power transfer from the group.
- ❖ Voltage and frequency from selected points.
- ❖ Extensive monitoring of network operations, load dispatching, and load frequency control operations should be done.
- ❖ The complexity of these operations is too much.
- ❖ Power consumption by the controlling-processing unit has to be minimized.

III. Proposed Model for communication

This paper explains a sensor network-based approach for communication of the control signals, as fine as the data swap. The sensor nodes in the transmission network are grouped to form clusters among themselves & communicate their readings within themselves. Each sensor in the cluster communicates with every other sensor in the cluster or in its surrounding area. This transmission is performed only when there is a change in the recorded readings. This approach minimizes the transmission power considerably, and hence, the lifetime of sensors is increased. One or two of the sensors may assume the cluster-head position and merge the data sent from other sensors to process it. In case of any fault detection, the appropriate decision may be made at the sensor level itself. When the overall system is measured, the various sensors along the electrical transmission path have set the locations. The sensors broadcast the information they receive from fault locations progressively to the SCADA monitoring/data logging centers or to the preservation team, as required. This long-haul transmission could be done using the GEAR protocol for routing, which takes into consideration the proximity of the next node to be considered for transmission to the destination, as well as the remaining energy of the nodes along the path. Since the site of sensors is already known and almost static, the use of a location aware protocol. Also, an optimal database required for comparison of values can be maintained in the sensor clusters themselves on a cooperative basis.

IV. Decentralized Result Making

The protection schemes applied for preventing the communication of transient overshoots, they may be avoided by the proposed virtual MIMO scheme. The sensor nodes that are in closeness at a particular unit level are grouped into clusters. One or two nodes among the clustered architecture may assume the position of cluster-head. Each node broadcasts the information it has locally using a time division multiple access scheme. Thus, all nodes have information from all other nodes in the cluster. The comparison of values is done in each node, and decisions are made. The database of each sensor node can be updated simply, since dispensation involves only evaluation of measured values with certain verge values.

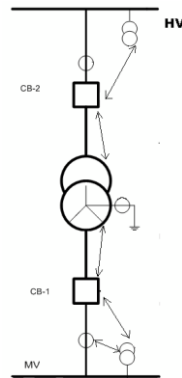


Fig.1: Virtual MIMO Transmission among the Sensors

Fig.1 shows a typical sensor network scenario in the automation of electrical power distribution. The communications of various sensors among themselves in a virtual MIMO basis, processes the information, and later transmit the information to a cluster-head. The cluster-head will now be able to differentiate signals due to transient voltages by comparing the reported signals from multiple nodes. The choice of cluster-heads may be based on a probabilistic approach, and the nodes may take turns attractive the cluster-head. The failure of any node in the cluster can then be immediately reported, and appropriate action can be taken.

V. Data Reporting

In sensor network architecture, GEAR uses energy aware and geographically conversant neighbor selection heuristics to route a packet to the target region. In case of failure of any of the nodes in the optimal path, there is a hole around where the packets are to be sent, and the new cost factor has to be incorporated henceforth while deciding the next node for transmission. The clusters are placed tactically along the lines so that the data reaches the target gradually. The cluster-head decide the next transmission node based on the GEAR protocol learned cost and forward the data to the target cluster by cluster. This has the following advantages:

1. The transmission power is significantly condensed because the clusters are not too distant away from each other.
2. The clusters can cross check the information and aid in the scattered dispensation.

Fig.2 illustrates the implementation of GEAR protocol in sensor network architecture with clusters of sensors. The next node is chosen based on its proximity to the destination and the remaining energy level of the node. This avoids continuous depletion of node energy and, hence, increases the lifetime of the nodes.

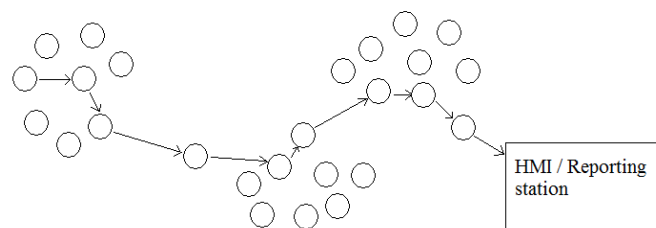


Fig.2: Location and Energy Aware Route Selection to Transmit Information

VI. Detection of Power Theft

The electrical power theft can be detected by insertion of sensor nodes deliberately along the transmission path. Any excessive changes in the electrical parameters can be instantly reported to the suitable target so that necessary action pursues. Fig.3 shows the placement of sensor clusters along the transmission path. The sensors continuously monitor the power levels, current, and voltage.. The placement of sensors along the transmission path has to be strategic. Placement of sensor clusters too close to each other along the transmission path would lead to needless redundancy. At the same time, if the distance between clusters is too far, that would lead to decreased potential of theft detection.

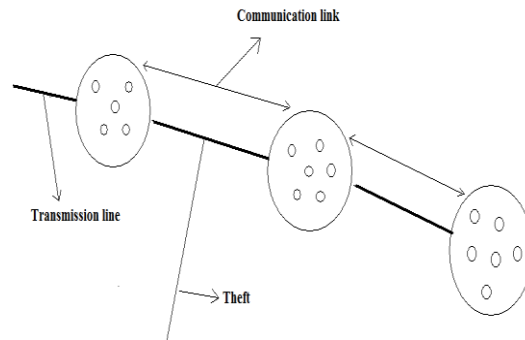


Fig. 3: Electricity Theft Detection Using Sensor Networks

VII. Future Works

The design of sensor nodes that would meet the requirements would be the prime area of research. They should be suitable for the harsh environment in the electrical transmission network. The processors need to be integrated with the transducers. This integration needs careful design of equipment, taking into consideration the parameters to be measured and the processes to be executed.

The protocols employed should address how to take advantage of the more powerful SCADA processes. The data management protocols should specify how to describe, collect, and manipulate different types of sensor data. The need for protocol translation can be eliminated by converting the measured data in all sensors to the same format at the node level. The designing of proper frame formats and incorporating the GEAR protocol for routing is another issue to be considered.

The strategic placement of sensors to enable theft detection may differ from place to place. That has to be carefully worked out. Further, the medium access contention has also to be taken care of in the intra-cluster communication.

VIII. Conclusion

The proposed communication model attempts to bring about a reasonable change in the power distribution and automation sector with the introduction of sensor networks. A fault developing in the transmission line or any other component may lead to grave spoil to equipment, and it tends to weaken the entire system. The proposed communication model has the following advantages:

- ❖ Decentralized result-making allows the SCADA system to be more flexible.
- ❖ The application of sensor networks avoids multifaceted wiring, as compared to high speed LANs and Ethernet.
- ❖ The dispersed processing of information speeds up the control operations and prevents lethal damages to equipment.
- ❖ Geographic routing improves the performance of the system, even in case of failure of some sensor nodes.
- ❖ The bandwidth requirements are considerably reduced.

References

- [1] I.F. Akyildiz, "Wireless sensor networks: A survey," *Computer Networks* (Elsevier), Vol. 38, March 2002, pp. 393–422.
- [2] Yan Yu, Ramesh Govindan, and Deborah Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks," UCLA Computer Science Department, Tech.Rep. UCLA-CSD TR-01-0023, May 2001.
- [3] William J. Ackerman, "Substation automation and the EMS," *Transmission and Distribution Conference*, IEEE 1999.
- [4] Wei Ye and John Heidemann, "Enabling interoperability and extensibility of future SCADA systems," University Southern California, USC/ISI Technical Report, ISITR-625, October 2006.
- [5] Sudharman K. Jayaweera, "Energy efficient virtual MIMO based cooperative communications for wireless sensor networks," *IEEE Transactions on Intelligent Sensing and Information Processing*, 2005.
- [6] Sunil S Rao, ed., *Switchgear Protection-Theory, Practice and Solved problems*, 1997, Khanna Publishers: Nai Sarak, New Delhi.
- [7] M. Kezunovic and N.A. Ved, "Circuit breaker on-line monitoring using wireless communications," *Wireless Technologies in the Power Industry*, Toronto, Canada, May 2005.
- [8] Scott Humphreys, "Substation Automation Systems in review," *IEEE Transactions, Computer Application in Power*, April 1998.
- [9] C. Hoga and G. Wong, "IEC 61850 Open Communication in practice in Substations," *Power Systems Conference and Exposition, IEEE PES*, 2004.
- [10] Alexei Makarenko, Alex Brooks, Stephen Williams, and Hugh Durrant-Whyte, "A decentralized architecture for active sensor networks," *Robotics and Automation 2004 Proc., ICRA*.