Paper # 110, IT 304

A Wireless Sensor Network Communication Model for Automation of Electric Power Distribution

M. Muthukumar
University Of Minnesota, Twin Cities
anmolmuthu@gmail.com

N. Sureshkumar
Anna University, Chennai, India.
getsureshed@gmail.com

MA. Bhadri Narayan
Anna University, Chennai, India.
badhri.sow@gmail.com

Abstract

Automation of electric power distribution in a cost-efficient and reliable manner can be accomplished by complete automation of the load dispatch centers and substations on a large scale. For efficient load balancing among the feed lines, a continuous monitoring of parameters, such as voltage, current in the line, temperature, pressure, and oil level of the transformers is required. Currently, automation is done with the help of Intelligent Electronic Devices (IEDs) and Supervisory Control and Data Acquisition (SCADA). This paper proposes a novel method of communication among the sensors. The paper proposes a 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. 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.

Introduction

The application of sensor networks is becoming ubiquitous, and this paper introduces a new area of application of the sensor nets viz. in the automation of electrical power distribution. Lack of information at the base station (generally a 33kV sub-station) on the loading and health status of the 11kV/415V transformer and associated feeders is one primary cause of inefficient power distribution. The automation of power distribution can be made efficient in terms of energy consumption, speed, and bandwidth requirements through the application of sensor nets. The functional elements that perform protection, control, and monitoring of the various signals are the sensor networks. The ultimate fault analysis system should provide

ISBN 978-1-60643-379-9

results of a detailed system-wide analysis of an event to the system dispatchers and protection engineers within seconds of the event occurring. 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. The sensor nodes are rather static and have a built-in processor, along with a transmitter cum receiver module. 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 introduces the concept of report by exception [3]. This avoids unnecessary transmission and, hence, saves a considerable amount of power. Further, complex wiring to link all these sensors to the control equipment is eliminated through low power wireless transmission. The bandwidth requirement is minimal since the transmissions are mostly local and are done only when necessary. The process of communication among the sensors is divided into the following two phases:

1. The communication of signals within clusters of the sensors that are in close proximity to each other on a virtual MIMO basis.
2. 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.

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 facilitate faster communication. The location of sensors can be obtained by means of a hardware system (GPS) or by occasional 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 dissemination of information sensed by the sensors or a query that is sent by the base station is a primary need in the automation of power distribution. The dissemination 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.

Current Scenario

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

1. The lowest level is the power system equipment, such as transformers and circuit breakers.

2. The middle levels implement the Intelligent Electronic Devices (IEDs) in the form of bay controllers, IED data integration using data concentrators, and substation automation applications.
3. The uppermost level is the utility enterprise level that consists of software that is integrated with the entire system.

Energy management systems (EMS) today employ a central coordinating unit [13] and various regional centers, which control the generating power stations in turn. There is a bay that consists of incoming feeders, outgoing feeders, transformers, and capacitor banks. The information is collected from various locations and fed as discrete inputs to the data concentrator, which may be a PLC.

The inputs are then processed, and the relevant action pursues. 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 power readings from the IEDs [6] connected to the bay controller, 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 aggregate readings from a number of sensors. Then, the RTUs 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:

1. Extensive monitoring of network operations, load dispatching, and load and frequency control operations should be done.
2. The complexity of these operations is too much.
3. The dependability on a single processing unit has to be reduced.
4. Further decentralization of decision making should be implemented in an efficient manner to speed up operations.
5. Power consumption by the controlling-processing unit has to be minimized.

W.J. Ackerman [3] explains that an enormous database has to be maintained to facilitate error-free and well-coordinated automation. For a 10-feeder substation, the database has to accommodate: 432 analog quantities, 270 status quantities, and180 control quantities.

Proposed Communication Model

The paper proposes a sensor network-based approach for communication of the control signals, as well as the data exchange. The sensor nodes in the transmission network are grouped to form clusters among themselves and communicate their readings within themselves. Every sensor in the cluster communicates with every other sensor in the cluster or in its vicinity. 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 aggregate 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 considered, the various sensors along the electrical transmission path have fixed locations. The sensors transmit the information they receive from fault locations progressively to the SCADA monitoring/data logging centers or to the maintenance crew, 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. This approach increases the lifetime of nodes considerably.

The whole of this transmission process is within distances that are many times smaller compared to the distance that the signal has to be transmitted from the RTUs directly to the SCADA monitoring/data logging centers. Hence, the signal transmission power is decreased manifold, as well as the bandwidth requirements. Since the location of sensors is already known and almost static, the use of a location aware protocol, such as GEAR, for transmission of control signals and information bearing signals is perfectly suitable. Also, an optimal database required for comparison of values can be maintained in the sensor clusters themselves on a cooperative basis.

Decentralized Decision Making

Malfunctioning of static relays may be due to transient over-voltages [6]. Besides the protection schemes applied for preventing the communication of these transient overshoots, they may be avoided by the proposed virtual MIMO scheme. The sensor nodes that are in close proximity at a particular unit level are grouped into clusters. One or two nodes among the clustered architecture may assume the position of cluster-head(s). As modeled in reference [5], instead of physically having multiple antennas at the transmitter side to implement the MIMO scheme, the sensor nodes that are close to each other communicate among themselves in a cooperative manner. 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. A space time block coding is done for transmitting the decisions made, assuming that each node is one element of a multiple antenna system. Then, they report the space time symbols they have to the cluster-head(s), which take the appropriate action. The database of each sensor node can be updated easily, since processing involves only comparison of measured values with certain threshold values.

Figure 1 shows a typical sensor network scenario in the automation of electrical power distribution. The various sensors communicate among themselves in a virtual MIMO basis, process the information, and later transmit the information to a cluster-head. The cluster-head will now be able to distinguish signals due to transient voltages by comparing the reported signals from multiple nodes. Further, this type of cooperative processing eliminates the possibility of error prone decisions that may ultimately pose dangers. The choice of cluster-heads may be based on a probabilistic approach, and the nodes may take turns becoming the cluster-head(s). The failure of any node in the cluster can then be immediately reported, and appropriate action can be taken.

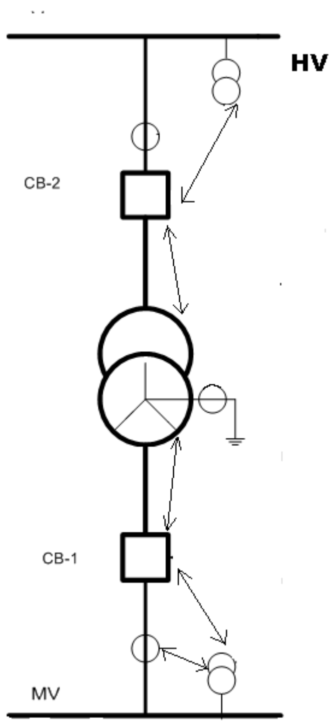

Figure 1: Virtual MIMO Transmission among the Sensors

Data Reporting

The aggregated information from each cluster-head may need to be transmitted to the SCADA master station, or to some central unit, for the data to be monitored or logged for future reference. For this transmission, GEAR protocol may be used. In sensor network architecture, GEAR uses energy aware and geographically informed neighbor selection heuristics to route a packet to the target region. Every node has an estimated cost [2] and a learned cost to reach a destination through its neighbors. The learned cost is the updated estimated cost. For instance, 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. Thus, there is periodic beaconing regarding position and health of nodes. The learned cost is propagated one hop back every time a packet reaches the destination so that the route setup for the next node can be adjusted. This beaconing of location information may comparatively be less frequent in case of the electrical transmission network. This is because the sensor nodes in the transmission network are almost static and there is not much change in terms of location of the sensor nodes. When this is the case, the use of a location-based protocol would be apt for such a network. The clusters are placed strategically along the lines so that the data reaches the destination progressively.

The cluster-heads decide the next transmission node based on the GEAR protocol learned cost and forward the data to the destination cluster by cluster. This has the following advantages:

- The transmission power is considerably reduced because the clusters are not too far away from each other.
- The clusters can cross check the information and aid in the distributed processing.

Figure 2 illustrates the implementation of GEAR protocol in a sensor network architecture with clusters of sensors. The route selection is based on a cost factor that incorporates remaining energy and distance to destination of neighboring sensor node. 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. Figure 3 shows that the lifetime of nodes is increased when the energy factor is also incorporated in the learned cost while deciding the next hop neighbor. The graph is the simulation result when energy aware and non-energy aware routing were implemented separately and the lifetime of nodes calculated.

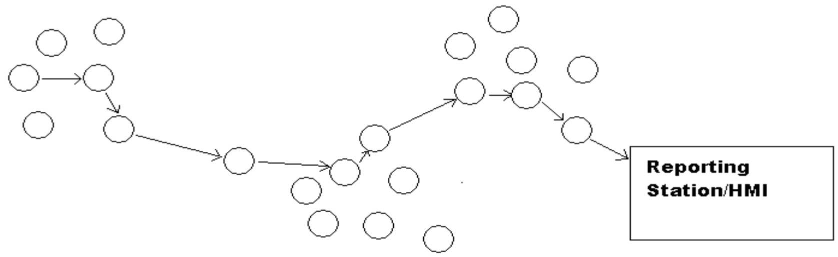

Figure 2: Location and Energy Aware Route Selection to Transmit Information

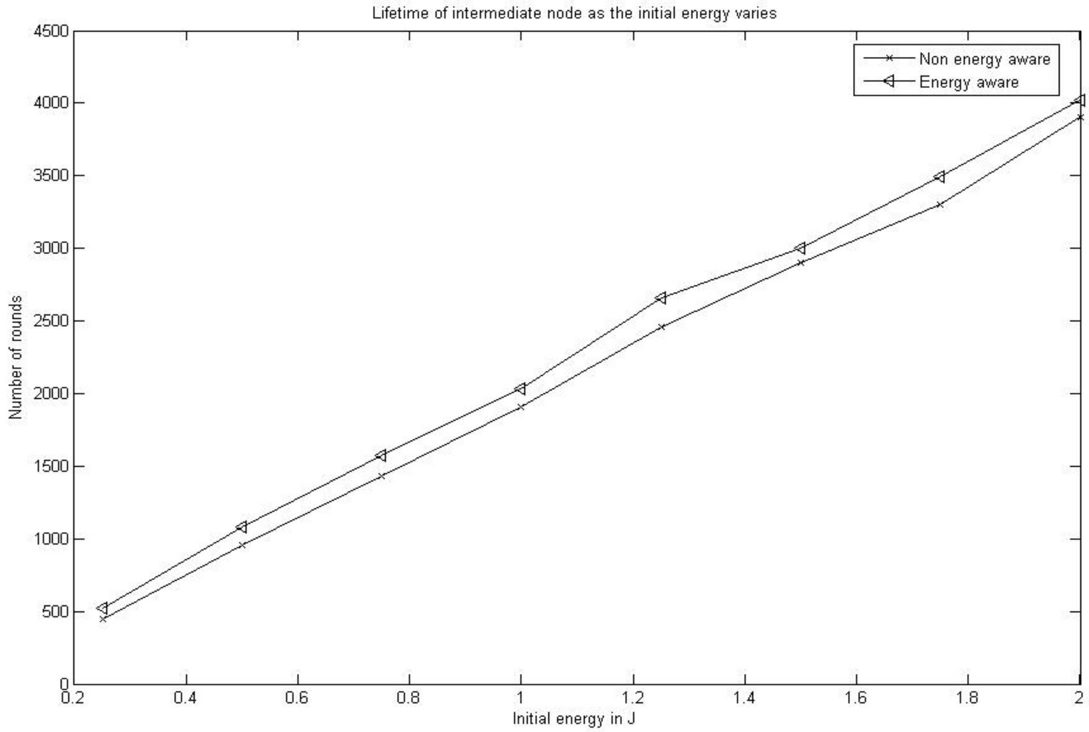

Figure 3: Initial Energy vs. Lifetime of Intermediate Node in the Case of Energy Aware and Non-energy Aware Routing

Theft Detection

The theft of electrical power can be detected by placing the sensor nodes strategically along the transmission paths. Any undue changes in the electrical parameters can be immediately reported to the appropriate destination so that necessary action pursues.

Figure 3 shows the placement of sensor clusters along the transmission path. The sensors continuously monitor the voltage, current, and power levels. The values of these parameters during normal conditions are already maintained in the databases of these sensors. Whenever there is a change in the measured parameters, these sensors immediately communicate to the nearest reporting station either progressively through the clusters of sensors or directly. 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 unnecessary redundancy. At the same time, if the distance between clusters is too far, that would lead to decreased potential of theft detection.

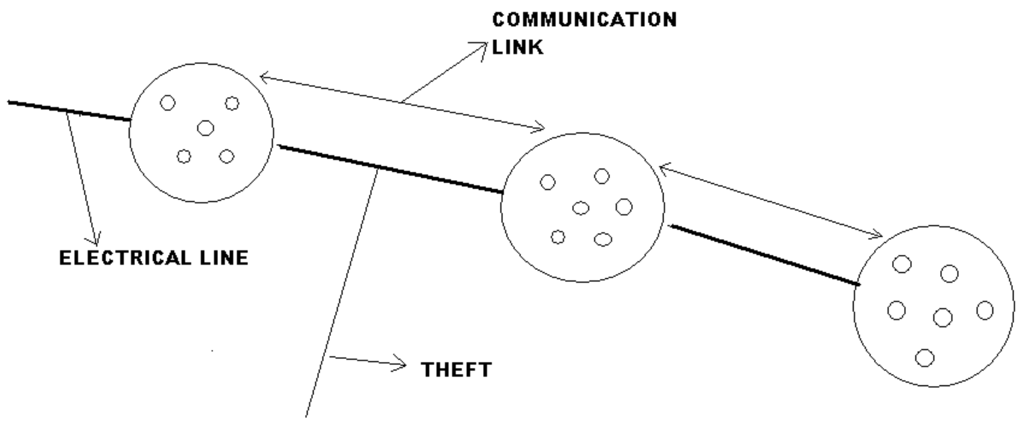

Figure 3: Electricity Theft Detection Using Sensor Networks

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. A TDMA-based approach may be preferable.

Conclusion

Today, an alternative paradigm for maintaining system security is developed, where a fast tracking tool is used to predict the short-term trajectory of the system state and attempt to navigate the state back into the secure normal operating region via system wide coordinated real-time controls. While this is easier said than done, one of the prerequisites for its success is faster and more detailed monitoring of both the dynamic system state and system topology. An integrated data and information exchange system must be implemented. This can be implemented by the application of sensor networks in the automation of power distribution.

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 serious damage to equipment, and it tends to destabilize the whole system. The conventional polling process delays the decision-making process, which may lead to irreversible damage. Further, the proposed communication model has the following advantages:

- Decentralized decision-making allows the SCADA system to be more flexible.
- Virtual MIMO-based cooperative processing eliminates the possibility of error prone decisions.
- The proposed communication model is extremely energy efficient and increases the lifetime of the nodes.
- The application of sensor networks avoids complex wiring, as compared to high speed LANs and Ethernet.
- The distributed processing of information speeds up the control operations and prevents fatal 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*, ISI-TR-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.
[11] Nirupama Bulsu and Sanjay Jha, ed., *Wireless Sensor Networks: A Systems Perspective*, Artech House, Inc.: Norwood, MA.
[12] Ivan Stojmenovic, ed., *Handbook of Sensor Networks-algorithms and Architectures*, John Wiley and Sons, Inc.: Hoboken, NJ.
[13] Sunil S Rao, ed., *EHV AC and HV DC Transmission Engineering and Practice*, Khanna Publishers: Nai Sarak, New Delhi.
[14] *IEC 61850-5 Communication Requirements for Functions and Device Models 2003*, 1st Edition, pp. 43–48.

Biography

M. MUTHUKUMAR, N. SURESHKUMAR, and MA. BHADRINARAYAN received their BEs in Electronics and Communication Engineering from the College of Engineering, Anna University Guindy, Chennai, India, in April 2008.

M. MUTHUKUMAR is completing his MS in Electrical Engineering at the University of Minnesota, Twin Cities.

N. SURESHKUMAR is working as an Associate Engineer at Force10 Networks in Chennai, India.

MA. BHADRINARAYAN is working as an Applications Developer at iNAUTIX Technologies India Pvt. Ltd. in Chennai, India.