Fault Location in an Electrical Energy Distribution Infrastructure with a Wireless Sensor Network

This article presents a detailed analysis of the applicability of wireless systems in the localization of faults in the energy distribution network. The hardware and software architectures of the envisaged sensor solution will also be described and finally, the integration of this system into Smart Grids will be discussed in terms of automatic fault analysis. A pilot system has been tested in a subset of the Portuguese energy distribution infrastructure operated by EDP Energias de Portugal. It presents a new approach to a fault locator system for the power network. The purpose is to obtain faster and more reliable information about the disruptions in the power distribution network and their location. Furthermore, the wireless sensors allow remote detection of medium and low voltage (MV/LV) power transformer hotspots in order to identify emerging malfunction as well as detection of intrusion in the MV/LV power transformers.

Nowadays, the electrical energy distribution is considered a critical infrastructure in industrially developed societies and its protection regarding safety and security threats is being more and more used.

The fact that this infrastructure is geographically spread across huge areas brings difficult technological challenges for the real-time prevention, detection and precise localization of anomalies.

The protection and localization of faults in the electrical energy distribution is a key task for any operator of such an infrastructure. Securing the main infrastructure components through the deployment of secure wireless sensor networks (WSN) providing remote monitoring and alarm capabilities.
The proposed approach in the case of the Medium Voltage (MV) overhead lines is based on the analysis of the increased current. Vision Control And Data Acquisition (SCADA) systems By using analytic methods we can detect faults, through wave transmission, the high frequency components of the currents and tensions and the fundamental frequency of the currents and tensions, measured in the line terminals (also called impedance Based Methods).

2 The prototype of the MV current sensor

3 Concept of the fault detection and identification system
The video streaming scenario is the most demanding for sensor network resources.

The Impedance Based Methods, consisting in the lines' impedance calculation in their terminations and in the estimation of the distance to the defects are, due to the easiness of implementation, the most adopted ones by the Electrical Companies. These methods can use the measurements of one of the lines' terminations, or the measurements of the two lines' terminations.

The impedance based methods have a precision of 2 to 3% of the total length of the line.

The precision of this method is influenced by several factors, including the combined effect of the charge current and the resistance of the defect (reactance effect), the imprecision in the identification of the type of defect (phases in fault) and the uncertainty about the parameters of the lines, particularly the homopolar impedance.

Nowadays, MV protection units usually have the function of fault locator incorporated, which is a well established function for transmission networks.

However, distribution networks have some differences that must be taken into consideration.

The main factor is that distribution networks are radial and constituted by many branches, which may have different impedances. In that way, it is not possible to use this information as it is commonly used in higher voltage levels.

In High Voltage (HV) networks each line has a protection unit capable of comparing impedances of the line and fault and transmitting the fault's location data. However, in MV networks that is not possible because, despite being radial, there are many ramifications with different electrical characteristics.

An option is to use the wireless sensors to communicate from the local network to the SCADA system, which processes the signals sent by the sensors, allowing the operator to know the location of the fault. For example, a sudden variation of current measurements is usually considered a fault indication.

If, for a pair of sensor nodes that are adjacent in the same branch of the electricity distribution network, only one of them is able to measure that sudden variation, then there is a high probability that the fault is located precisely between those sensor nodes.

This solution can be easily implemented with reduced costs.

Case Study

The proposed approach was tested through a case study of a distribution line and MV/LV Power Transformer. This case study was made within the FP7 European project WSAN4CIP, which uses a WSN technology.

Here, the faults can be located quickly, reducing the time of a power outage. A more complete view of the whole system deployed for fault location can be generically observed in Figure 1.

A picture of the MV Current Sensor prototype developed by INOV with the contribution of EDP can be seen in Figure 2.

Basically there are sensors at the substation to monitor the status of the trip coils, the temperature of the transformers and the neutral resistor and at the power lines to monitor the current and detect and locate the faults. In the MV/LV power transformers placed in the secondary substation, there are also video sensors to detect intrusions and hotspots. The WSN interacts with the SCADA system to allow a centralized monitoring and control of the protection system. A gateway node acts as a sink node to receive
Nowadays, the electrical energy distribution is considered a critical infrastructure in industrially developed societies and its protection regarding safety and security is being used more and more.

Considering the network in Figure 3, if a fault occurred between the S6 and S7, as an example, it would be detected by S7 and S6 and the information transmitted through Wi-Fi to S6, S2 and finally to S1 and from there to the gateway to the SCADA system. After collected by the rear-end processing system, the fault location can be identified and displayed in the Human Machine Interface of SCADA system (Figure 4).

A gateway node acts as a sink node to receive data from sensors and provides the interface Supervision Station.

The video streaming scenario is the most demanding in terms of sensor network resources. Video is streamed multipath from MV/LV power transformer to the SCADA supervision station when a passive infrared motion detector detects an intrusion.

The human machine interface of the system is shown in Figure 4. With those outputs it is possible to see the status of the network of the sensors, the alarms, the currents and the images of intrusion and hotspots.

A database of all faults is created in the SCADA system. This way it is possible to:

- Analyze the location and type of faults over time,
- Provide valuable information for intervention in the network’s maintenance.

In the WSAN4CIP project we focused on improving the dependability of the substation components, MV and LV power lines, and MV/LV power transformers in the secondary substations. We defined solutions for the remote active monitoring of:

- Substation circuit breaker trip coil status
- Temperature of the substation power transformer oil, substation neutral reactance oil and substation neutral resistor coil box
- MV and LV power line current activity
- MV/LV power transformer hotspot detection
- Human activity in the secondary substation through the use of movement detectors and video cameras

All the monitored parameters and images are visualized at the SCADA system, through a special-purpose graphical user interface. The communication between the sensors is done through the IEEE 802.11 g protocol (Wi-Fi).

The generic configuration of the system is shown in Figure 5. The WSAN is integrated with the SCADA system by means of a SCADA/
WSAN Gateway, in order to provide a unified power distribution infrastructure interface to the human operators.

The power-line sensor nodes were developed based on a Silix SX-560 core. The PCB designed at INOV includes a common voltage converter able to generate 3.3V DC to feed the Silix and 5V DC to feed the USB interface (considered a part of the Sensor Interface Unit) based on an input of 6-20 V DC. The Energy Unit in the board is able to harvest energy from the MV power-line, assuring the autonomy of the sensor nodes for a long time period, without the need for maintenance.

The software modules of the WSAN node are depicted in Figure 6. The selected Operating System is Linux.

The main software modules of a generic WSAN4CIP node are the following:

- **WSAN Sensor/Actuator Application Logic**: Application logic of the WSAN node, that manages sensors, actuators and communications.

- **Dependable Protocol Stack**: The Routing and Transport protocols. The transport layer consists of a secured version of the Distributed Transport for Sensor Networks (DTSN) while routing consists of a secure version of the Routing Protocol for Low power and Lossy Networks (RPL).

- **Sensor/Actuator Device Drivers**: Software that provides access to each type of sensor/actuator.

- **Management Information Base (MIB)**: Configuration parameters of the WSAN nodes.

**Experimental results**

Tests were conducted in the WSAN4CIP trial network in order to assess the performance of the supported services and the compliance with the requirements provided by EDP.

For the current measurement tests, extra current was externally injected into the power lines by the EDP technicians.
Table 3: Delay Evaluation

<table>
<thead>
<tr>
<th>Application</th>
<th>Average Delay</th>
<th>Standard Deviation</th>
<th>Delay Bound Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Line Current Measurement (1 hop)</td>
<td>21.10 ms</td>
<td>5.10 ms</td>
<td>&lt; 10 s</td>
</tr>
<tr>
<td>Power Line Current Measurement (5 hops)</td>
<td>338.20 ms</td>
<td>18.0 ms</td>
<td>&lt; 10 s</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>2.10 s</td>
<td>1.10 s</td>
<td>&lt; 10 s</td>
</tr>
<tr>
<td>Hotspot Detection</td>
<td>2.20 s</td>
<td>0.40 s</td>
<td>&lt; 10 s</td>
</tr>
</tbody>
</table>

As can be seen, both UDP and DTNS current sensors present similar delay and jitter performance, being able to comply with the requirements defined by EDP. DTNS achieves lower frame losses due to its error recovery mechanism, while achieving slightly less delay. Although neither of the tested transport protocols is able to provide the required channel capacity of 768 Kbit/s, both are able to support the required resolution at a frame rate that is even higher than the one defined therein. The difference towards the required channel capacity is also not too significant, being respectively 11.5% and 12.5% for UDP and DTNS.

Conclusions

The analysis and application of the Fault Location method for distribution lines and MV/LV power transformers has been presented. In the proposed approach, the acquired current signals, hotspots, images, signals, and intrusion detection images are transmitted to the SCADA System. The signals acquired from the electrical grid are processed in the server to identify the kind and location of fault. To identify the faulty operation, it will be used as a program to detect the towers in which the faults exist. In order to confirm the proposed approach, several test results for different situations have been presented.

This article has presented the planned architecture and high-level implementation solutions for the WSN system, including a description of the protected equipment, the hardware, and software architecture. We can conclude that it is possible to pre-fault detection, which will prevent some damages in major equipment, minimizing the impact on clients; the faults can be located quickly, reducing the time of a power outage.

The WSAN4CIP project fits in the Smart Grid EDP project and it is a proof of concept and a step forward in fault and pre-fault detection.

Acknowledgment:

This research received funding from the European Community’s 7th Framework Program under grant agreement no. 225186.

Consortium: Eurescom, IHP Microelectronics, NEC Europe, INOV, EDP Energias de Portugal, Budapest University of Technology and Economics, INRIA, Lulea University of Technology, Sirix, Tecnatom, University of Malaga and FWA.

Table 4: Video Streaming Evaluation

<table>
<thead>
<tr>
<th>Transport Protocol</th>
<th>Parameter</th>
<th>Average</th>
<th>Standard Deviation</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Delay</td>
<td>385.00 ms</td>
<td>55.00 ms</td>
<td>&lt; 50.00 s</td>
</tr>
<tr>
<td></td>
<td>Jitter</td>
<td>50.00 ms</td>
<td>40.00 ms</td>
<td>&lt; 200.00 ms</td>
</tr>
<tr>
<td></td>
<td>Throughput</td>
<td>233.00 Kbit/s</td>
<td>20.00 ms</td>
<td>230.00 Kbit/s</td>
</tr>
<tr>
<td></td>
<td>Video frames lost</td>
<td>69.0 %</td>
<td>20.0 %</td>
<td>&lt; 200.00 ms</td>
</tr>
<tr>
<td></td>
<td>Channel capacity</td>
<td>680.00 Kbit/s</td>
<td>391.00 Kbit/s</td>
<td>768.00 Kbit/s</td>
</tr>
</tbody>
</table>

DTNS

<table>
<thead>
<tr>
<th>Delay</th>
<th>176.00 ms</th>
<th>37.00 ms</th>
<th>&lt; 10.00 s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jitter</td>
<td>11.00 ms</td>
<td>5.00 ms</td>
<td>&lt; 200.00 ms</td>
</tr>
<tr>
<td>Throughput</td>
<td>243.00 Kbit/s</td>
<td>&lt; 200.00 ms</td>
<td></td>
</tr>
<tr>
<td>Video frames lost</td>
<td>0.00 %</td>
<td>0.00 %</td>
<td>&lt; 0.00 %</td>
</tr>
<tr>
<td>Channel capacity</td>
<td>672.00 Kbit/s</td>
<td>186.00 Kbit/s</td>
<td>768.00 Kbit/s</td>
</tr>
</tbody>
</table>