Abstract — The cornerstone of a Smart Grid is the ability for multiple entities to interact via communication networks. A scalable and pervasive communication infrastructure represents a crucial issue in both structuring and operating smart networks. In addressing this problem this paper figures out the potential role of cooperative Wireless Sensor Networks (WSNs). In detail, it analyses the performance of IEEE 802.15.4 based WSNs in order to establish their suitability for a typical set of monitoring and supervision functionalities required by urban-scale Smart Grids applications. The results obtained show that the application of this technology may be very promising in several Smart Grids applications as far as automation, remote monitoring and supervision are concerned.

I. INTRODUCTION

Modern power systems are subject to a host of challenges – distributed energy resources integration, ageing, need for siting new generation and transmission infrastructures, dynamic reactive compensation, congestion management, grid ownership vs. system operation and reliability coordination, etc.

Evolving operation jurisdictions and environments, control responsibilities, rising demands and expectations for reliability call for restrictive management policies and advanced functions ensuring high performances of power systems even when more and more components are forced to operate at or near their limits and systems must endure frequently changing operating conditions [1].

In this complex scenario the wider deployment of Smart Grids paradigm (namely the convergence of information and operational technology applied to the electric grid in order to allow sustainable options to customers and improved security [2]) could play a strategic role in enhancing the efficiency of power systems and the use of cleaner energy resources, by ensuring at the same time the security of the infrastructure.

The cornerstone of a Smart Grid is the ability for multiple entities (e.g. devices, software processes) to interact via communication networks. It follows that the development of a reliable and pervasive communication infrastructure represents a crucial issue in both structuring and operating smart networks [3,4]. In this connection, a strategic requirement in supporting this process is the development of reliable communications backbone establishing robust data transport Wide Area Networks (WANs) to the distribution feeder and customer level [5].

Existing electrical utility WANs are based on a hybrid mix of technologies including fiber optics, power line carrier systems, copper-wire line, and a variety of wireless technologies (i.e. GSM/GPRS). They are designed to support a wide range of applications as far as SCADA/EMS, generating plant automation, distribution feeder automation and physical security.

These communication infrastructures should evolve toward nearly ubiquitous transport networks able to handle traditional utility power delivery applications along with vast amounts of new data from the Smart Grid [5].

These networks should be scalable, in order to support the new and the future set of functions characterising the emerging Smart Grids technological platform, and highly pervasive in order to support the deployment of last-mile communications (i.e. from a backbone node to the customers locations) [6].

To address this problem the employment of Wireless Sensor Networks (WSNs) appears to be particularly suitable since it could make possible the realization of advanced, highly valuable communication services (i.e. sophisticated metering, remote control and supervision) without requiring the construction of complex and expensive infrastructure and by assuring, at the same time, a set of intrinsic advantages such as wide area coverage, easy access to remote sites, no leasing cost and adaptability to changing network patterns.

This technology could also play an important role in supporting the deployment of distributed control architectures that move away from the traditional centralized paradigms to system distributed in the field with an increasing pervasion of intelligence devices (smart sensors) where central controllers play a smaller role. The adoption of wireless smart sensors in Smart Grids could lead to a more efficient tasks distribution amongst the computing resources and, consequently, to a sensible lightening of the centralized computing systems. This could decreases the total cost of the control system making straightforward its upgrade.

On the other hand the main factors that, in the past, have limited the application of WSNs in power systems communication have been uncertainties in quality of service and in time delays.
Nowadays the advent of the cooperative communication paradigms introduced by the IEEE 802.15.4 standard in conjunction with the continuous improving in efficiency of the modern hardware technologies are driving WSNs to become competitive with other settled communication systems.

The comprehensive application of WSNs technologies in Smart Grids communication requires a preliminary testing of their true functionalities in order to evaluate their potential integration within specific power system applications.

According to these statements the paper analyses the performance of cooperative WSN based on the IEEE 802.15.4 standard in order to establish their suitability for a typical set of monitoring and supervision functionalities required by urban-scale Smart Grids applications.

The performance evaluation has been carried out in the QualNet Developer Platform simulation environment [7]. The results obtained show that the application of WSNs based communication services exhibits a set of intrinsic advantages, particularly useful in Smart Grids communication, as reliable network services and reduced overall infrastructure support requirements.

These advantages point out that WSNs based communication services may be very promising in several Smart Grids applications as automation, remote monitoring and supervision.

The paper is organized as follows: Section II focuses on emerging needs for smart grids communication; in Section III the main features of IEEE 802.15.4 based WSNs are discussed; in Section IV simulation results are summarised and analysed; finally conclusion and open issues are presented.

II. EMERGING NEEDS IN SMART GRIDS COMMUNICATION

The design of reliable, resilient, secure, and manageable standards-based open communication systems represents a key issue in Smart Grids deployment. These infrastructures provide the fundamental backbone connecting the grid elements, the data providers and the decision-making entities in an open and interoperable framework.

They should support ubiquitous connectivity between decision-making points and dispersed and heterogeneous data sources characterised by varying degrees of transport, security, and reliability requirements [5].

They must ensure the capability of power grid automation systems to transmit data to and from distributed intelligent controllers; moreover, the prospected development of innovative energy market policies (i.e. real time pricing, ancillary services markets, multi-energy markets etc.) imposes the realization of efficient and reliable widespread bidirectional communication links between grid Operators and Customers premises.

In the light of these needs, the IEC 61850 standard provides a framework for substation automation integration that specifies the communications requirements, the functional characteristics, the structure of data in devices, how applications interact and control the devices, and how conformity to the standard should be tested [8,9].

It also defines the key success factors for an integrated smart communication network design [10]:

1. Flexibility to adjust and grow the system topology as requirements change.
2. Performance, especially Quality of Service, to enable effective prioritization among competing applications and to meet critical requirements of the most important protection and control functions.
3. Reliability, for critical protection systems, but also because so many different systems are relying on the same infrastructure.

To address this problem the use of WSNs appears to be particularly suitable as it could support advanced, highly valuable communication services without requiring the construction of complex and expensive infrastructure. It could assure, in addition, a set of intrinsic advantages such as wide area coverage, easy access to remote sites, no leasing cost and adaptability to changing network patterns.

In particular, after a comparative performances analysis of the main WSNs architectures, the one based on the IEEE 802.15.4 standard has been adopted as reference in our research activities [11].

The benefits deriving by the application of this communication architecture are [12]:

- low cost modem allowing to extend wireless networking to even the simplest of devices;
- fault tolerance and reliable transmission: if two network nodes are unable to communicate because a link fails or because the distance exceeds the device range, transmission is automatically routed to other relay systems until data reach final destination;
- open standard that allow customers to choose among different vendors;
- high level of network scalability: networks can scale from hundreds to thousands of devices, all communicating by using the best available path for reliable message delivery.

The main features of IEEE 802.15.4 based WSNs will be briefly discussed in the next section.

III. IEEE 802.15.4 BASED WSN

The IEEE 802.15.4 [11] refers to the first two layers of the ISO/OSI stack protocol, i.e. the standard defines the physical layer (PHY) and medium access control (MAC) sub-layer specifications for supporting simple devices that consume minimal power and typically operate in the wireless personal area network (WPAN) of 10 m or in general in a short communication range. IEEE 802.15.4 is a standard for PAN which is also characterized by low data rate and low cost.

In IEEE 802.15.4, all devices are divided into two categories: full function devices (FFDs) and refined function devices (RFDs) according to their capabilities. FFDs can initiate a WPAN and act as the coordinator of the WPAN, or can forward data and act as routers.

At the physical layer, wireless links under 802.15.4 can operate in three license free industrial scientific medical (ISM)
frequency bands. These accommodate over air data rates of 250 kbps in the 2.4 GHz band, 40 kbps in the 915 MHz band, and 20 kbps in the 868 MHz. A total of 27 channels are allocated in 802.15.4, including 16 channels in the 2.4 GHz band, available worldwide, 10 channels in the 915 MHz band, used in North America, and 1 channel in the 868 MHz band for Europe.

Many technologies based on the IEEE 802.15.4 standard have been deployed for WPANs. Among these, the ZigBee appears particularly suitable for the applicative domain under study.

The ZigBee has been well accepted as industrial standard for wireless sensor networks because it allows good achievements in many application domains (i.e. environment monitoring, home network, industrial automation).

ZigBee adopts IEEE 802.15.4 standard at its PHY and MAC layers and support lowrate WPANs. Its specifications add to the standard four main components: network layer, application layer, ZigBee device objects (ZDOs) and user-defined application objects which allows for customization and flexibility within the standard. At its core, ZigBee is a mesh network architecture. Its network layer natively supports as main topologies: star and tree typical networks and generic mesh networks, self-forming and self-healing networks.

In particular, the ZigBee architecture identifies three kinds of devices:

- A coordinator, which organizes the sensor network and maintains routing tables.
- Routers, which can talk to the coordinator, to other routers and to reduced-function end devices.
- End devices, which can talk to routers and the coordinator, but not to each other.

The expected benefits deriving by the application of this communication architecture are:

- Low cost: a typical ZigBee modem can be as low as $12 each in quantities as few as 100 pieces. This pricing provides an economic justification for extending wireless networking to even the simplest of devices.
- Range and obstruction issues avoidance: the routers double as input devices and repeaters, to create a form of mesh network. In this way, if two network points are unable to communicate as intended, transmission is dynamically routed from the blocked node to a router with a clear path to the data's destination. This happens automatically, so that communications continue even when a link fails unexpectedly. The use of low-cost routers can also extend the network's effective reach. When the distance between the base station and a remote node exceeds the devices' range, an intermediate node or nodes can relay transmission, eliminating the need for separate repeaters without stopping the system operation. This long-term reliability is critical for many power automation systems that are expected to last 20–30 years once installed.
- Multisource products: as an open standard, ZigBee provides customers with the ability to choose vendors as needed. A ZigBee-certified modem will interoperate with any other ZigBee-certified radio adhering to the same profile.
- High level of network scalability and reliability: networks can scale to hundreds and thousands of devices.

All these features make Zigbee based WPANs ideal candidates for supporting effective and reliable data-exchange in urban Smart Grids.

IV. SIMULATION STUDIES

This section assesses the performance of an IEEE 802.15.4 based WSN in supporting a typical set of communication services in an urban power network. The analyzed WSN is based on 30 ZigBee nodes monitoring 28 electrical substations. The WSN is characterized by a single PAN coordinator (node 1) and a data concentrator located in node 6. The data concentrator is connected to a remote control center by two wired 100 Mbps Ethernet networks as shown in fig.1.

The network performance analysis has been developed by using the QualNet Developer Platform simulation environment [7].

![Fig.1: The analysed urban network](image)

A. Urban scenario

The first case study has been focalized in assessing how the end to end data latency in an urban environment is influenced by the number of aligned nodes, the message size and the transmission period.

The obtained results are summarised in tab.1 and in fig.2-3.

| Table I  
| Maximum Data Latency vs Node Numbers |
|---|---|
| **Aligned nodes** (node distance 500 m) | **End to end delay [ms]** |
| 2 | 241 |
| 3 | 1128 |
| 4 | 1626 |
| 5 | 2123 |
| 6 | 4025 |

The expected benefits deriving by the application of this communication architecture are:
These simulations show that end-to-end delay increases when nodes number increases since if the node distance remains the same (500 m), the network area becomes larger. Moreover, we observe a little increase for delays as a function of packet sizes variation. Instead, as a function of the transmission period the end-to-end delays appear to be almost constant until 100 ms, to decrease for transmission periods between 100 ms and 800 ms and to increase for higher transmission periods.

Fig. 2: Maximum data latency vs nodes number and message size

Fig. 3: Maximum data latency vs nodes number and transmission period

Further simulation studies have been oriented in assessing the impact of weather conditions on WSNs performances. In this connection the effect of rain is known to be the most important issue to analyse, as reported in tab.II.

<table>
<thead>
<tr>
<th>Environmental condition</th>
<th>End to end delay [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td>No rain</td>
<td>67</td>
</tr>
<tr>
<td>Light rain, rain rate 6 mm/h</td>
<td>654</td>
</tr>
<tr>
<td>Hard rain, rain rate 180 mm/h</td>
<td>1833</td>
</tr>
</tbody>
</table>

On the basis of these data analysis, it is worth to observe as the measured data latencies make difficult the employment of the WSNs based data link in high performance - time critical applications.

On the other hand the employment of WSNs could be a very interesting solution in supporting the deployment of spur or last-mile communications for the Smart Grids, typically from a backbone node to the customer premises. This is mainly due to the high level of pervasion characterising WSNs that allows it to cover large residential area.

B. Intensive traffic simulation

The second case study addresses the WSNs performance in supporting power systems control and regulation functions requiring intensive data exchanges.

In particular the nodes transmit, with a time period of 1 second, the following substation information:
- 80 binary states
- 39 power measurements
- the state of 2 tap changer power transformers

According to the IEC 61850 standard, the periodic transmission of this information requires, with no data compression, a communication bandwidth of 10.5 kbps. The simulation studies have shown that the network can easily satisfy this requirement.

As far as the data latency (between the single nodes and the WSN coordinator) and the number of active connections are concerned, the corresponding results are reported in tab.III in function of the number of simultaneous transmitting nodes.

<table>
<thead>
<tr>
<th>Number of nodes transmitting at the same time</th>
<th>Mean data latency [s]</th>
<th>Active links</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3,703</td>
<td>4/4</td>
</tr>
<tr>
<td>6</td>
<td>3,202</td>
<td>6/6</td>
</tr>
<tr>
<td>10</td>
<td>3,477</td>
<td>8/10</td>
</tr>
<tr>
<td>12</td>
<td>3,877</td>
<td>9/12</td>
</tr>
<tr>
<td>16</td>
<td>3,365</td>
<td>14/16</td>
</tr>
<tr>
<td>18</td>
<td>3,601</td>
<td>15/18</td>
</tr>
<tr>
<td>23</td>
<td>2,213</td>
<td>11/23</td>
</tr>
<tr>
<td>25</td>
<td>3,612</td>
<td>12/25</td>
</tr>
<tr>
<td>28</td>
<td>6,400</td>
<td>10/28</td>
</tr>
</tbody>
</table>

These data outline that the number of active connections effectively supported by the network drastically decreases as the number of simultaneous transmitting nodes increases. This is due to network congestions observed in critical WSN sections. To address this problem the definition of ad hoc design strategies aimed at improving the network meshing represents a viable solution approach.

As far as the data latency is concerned, the obtained results make the employment of WSNs based communication services very promising for several power system communication applications: automation, remote monitoring and supervision. However, this approach does not appear to be applicable for high performance-time critical applications.

C. Cybersecurity issues

The third and last case study focuses on assessing the WSN vulnerability to external cyber attacks. To this aim, a Wormhole attack [13] has been simulated in the communication network by connecting two remote regions by a low latency connection (namely the wormhole link) as shown in fig. 4. Once the wormhole link is established, it implements a data tunnelling between region A and B (i.e. it transmits to region B all the information received from region A and vice versa). The overall effect is that all nodes located in region B erroneously identify as neighbors all the nodes.
located in region A and vice versa. This process hinders the multi-hop routing in the WSN leading to a network collapse.

This is a very critical issue that needs future researches aiming to identify external attacks and mitigate their effect on the network operation.

V. CONCLUSION

The use of WSNs technology is gaining favor within electric power industry for a multitude of applications. This paper has shown simulation results for a IEEE 802.15.4 based communication network and has outlined the potential roles of such a network for urban smart grid communication.

The obtained results have shown as the employment of WSNs based communication services is very promising for several power systems communication applications: automation, remote monitoring, supervision. Pervasive grid monitoring and last mile communications are other potential applications for which the use of WSNs technology will be beneficial. However, this approach does not appear to be applicable for high performance-time critical applications.

The future directions of this research will be oriented to define ad hoc WSNs design strategies aimed at improving the network performances in terms of data latency, number of simultaneous and active connections. Moreover, further efforts will be devoted to design suitable tools aimed at reducing WSNs cybersecurity vulnerability.

REFERENCES