Chapter 8 Overlay Networks for Smart Grids

Tim Wauters, *Ghent University – iMinds*
Filip De Turck*, Ghent University – iMinds*
Chris Develder, *Ghent University – iMinds*

8.1 Abstract

Smart Grid networks imply the extension of the power grid network with communication technologies, to enable advanced coordination mechanisms. While the main drivers for Smart Grid projects may vary from region to region (e.g., increasing penetration of distributed renewable energy production in the European Union, need for enhanced reliability in the United States, etc.), the key differentiators of the next generation power grid stem from the massive amounts of data that will be made available at distributed locations, which must be leveraged to optimally operate the grid. Thus, the basic functions that communication networks should provide can be summarized as: 1. Data acquisition from a massive amount of measurement devices. 2. Sending control signals to steer consumption/generation (e.g., demand-supply matching). The data acquisition part clearly involves gathering the "smart meter" data from the residential meters scattered across the distribution network. But it also implies collecting the information of so-called synchrophasors, generally known as Phasor Measurement Units (PMUs), which are devices typically installed in the transmission network that combine precise measurements of currents and voltages with accurate time recording. Applications that can make use of these measurements (both in distribution and transmission networks) have varying requirements for real-time communications. Clearly, there is a need for (distributed) control mechanisms, which also imply specific network architectures.

Generally speaking, an overlay network is a network that is built on top of another network and uses the basic services of the underlying network to provide a new service or optimize existing services. Smart Grid architectures can benefit from such communication overlay networks to help facilitate intelligent communication (for resource and network discovery, session establishment, routing, addressing, etc.) and data transfer between various nodes of the heterogeneous Smart Grid network. Concepts similar to overlay networks for telecommunication services can be introduced in Smart Grids to face the problems of interoperability, reduce energy consumption, decrease cost, increase reliability and create new service opportunities for all participants in the value chain. Many challenges can be met by introducing common, ubiquitous and interoperable network technologies. In this chapter, we outline the relevant overlay networking technologies that address some of the needs of Smart Grids. We will discuss two types of overlay networking: 1. Multiservice networks,

referring to multi-layer network approaches, mainly based on (G)MPLS technology to overlay (e.g., IP networks over optical networks). 2. Communication overlays (typically referring to IP-based overlays, hence mainly over the Internet). Focus will be mainly on communication overlays, since this type of overlay has the broadest applicability in practice and makes no particular assumptions on the available underlay technology.

8.2 Introduction

8.2.1 Smart Grid applications and requirements

Some utility applications, particularly those devoted to protection or "relaying," require fast interaction among devices and systems. The requirement is for "sub-cycle" response, that is, sensing and action within less than 16.67 or 20 milliseconds (for 60 Hz and 50 Hz system, respectively). Protection schemes are designed to open circuits rapidly in the event of current spikes; transmission lines carry massive amounts of energy that, if misdirected for more than these time intervals, can lead to severe damage to equipment, impact on the environment (e.g., fires), and extreme danger to utility staff and the public. Transmission protection is typically supported by low-latency communications—for example, analog or digital point-to-point microwave links, fast serial link-level connections over fiber, or special-purpose power line carrier systems. The cost of implementing these solutions, which can be quite high, is justified by the necessity of near-real-time protection schemes. For a comprehensive overview of delay and priority requirements of these protection-related (and other) Smart Grid applications, we refer to Table I of [21].

Another set of requirements arises from the need to monitor grid conditions across a power control region or market, and eventually across multiple regions. One approach to such "Wide Area Situational Awareness" involves measurement at high resolution of the phase angle between voltage and current at key points in the flow of energy. These so-called phasor measurements have revealed inter-system, sub-Hertz oscillations (with periods of 1 to 10 seconds), and can help to identify other potentially destabilizing conditions. Phasor Measurement Units capable of generating 30 or 60 samples per second, with timestamp accuracy below 10 microseconds, are being deployed in their hundreds in United States power systems. Current architectures have the data flowing to a Phasor Data Concentrator over non-specialized routed networks, but it is conceivable that high-accuracy data generated at such frequencies could be useful in fine-grained, localized control schemes that would benefit from a real-time network overlay. For an in-depth discussion of the requirements and resulting guidelines for such (PMU-based) wide-area measurement system data delivery networks, we refer to [7].

Whether driven by data from PMUs or other sensors, advanced distributed control will likely emerge as another set of applications for which real-time network overlays will be useful, or even required. Apart from, for example, PMU-based real-time control in the transmission network, possibly less stringent requirements apply in distribution network scenarios, where challenges arise to collect (and aggregate) smart meter data, as well as react upon it and perform supply-demand matching. Nevertheless, the timescales at which such balancing will be performed are likely to decrease and become more and more "real-time." Indeed, balancing authorities are already contemplating schedules based on intervals of minutes or even seconds (as opposed to today's common one-hour schedules). In this respect, it is useful to make a distinction between "hard" and "soft" real-time networks. Hard real-time networks imply the requirement for stringent low latency, where the system basically fails if the time constraints cannot be met. This would be the case for communication-based closed loop control systems. However, other applications (see Section 8.4, "Vision," for some examples) have less strict needs, but still call for clear Quality of Service (QoS)

mechanisms to provide certain guarantees; see the "**Error! Reference source not found.**" chapter in this book for more information.

Overlay networks, as explained in more detail in the following sections, are well suited to provide levels of supervised or autonomous control over the data streaming sessions, with a virtualized view of the underlying network resources and independent of technology choices. Distributed components in the overlay topology (e.g., through agent-based control [18]) can further support the necessary functionality to provide network management, monitoring, reliable transport, and security functions. More specifically for the Smart Grid, meter data collection, aggregation and processing components can be supported in the overlays through adaptive, robust and distributed signaling processes, in order to steer control mechanisms such as supply and demand matching [7].

8.2.2 Convergence to multi-service networks

For a variety of reasons—namely application isolation, performance and traffic management, security, etc.—utilities have traditionally installed and operated separate networks for operational and corporate IT (voice and data) purposes. This isolation has been achieved by implementing completely separate physical networks (i.e., discrete optical fibers or microwave links). Depending on their requirements and the location of their facilities, in order to implement redundant network topologies (closed SONET rings, etc.) some utilities may also need to supplement their own network assets by leasing network services from public telecommunication carriers [on their Frame Relay, Asynchronous Transfer Mode (ATM), or increasingly, carrier Ethernet, MultiProtocol Label Switching (MPLS), and Generalized MultiProtocol Label Switching (GMPLS)/ Dense Wavelength Division Multiplexing (DWDM) infrastructure]. This is an unwelcome cost burden, because it not only involves fees to carriers, but also multiple network management domains, which further increases the utilities' operational expenses.

These factors have led utilities to explore opportunities for supporting both corporate and operational networks on a common, managed "multi-services" platform. While multi-service networks, using MPLS as the technology of choice, aim for high-performance networking solutions (very low delay, very high bandwidth capacity), overlay networks are brought into play as low cost alternative solutions on top of existing networks with a virtualized view on the lower layer network technologies used.

8.2.3 Communication overlays

In telecommunication networks, overlay networks are introduced in order to cope with stringent QoS requirements from communication services and applications, on top of best effort Internet. These requirements cannot be met entirely by network layer solutions such as IntServ [11] and DiffServ [52], which suffer from scalability issues and cannot be realized end-to-end, spanning multiple autonomous systems. In addition to these problems, the current routing infrastructure also exhibits several shortcomings, such as suboptimal routing in terms of delay and/or packet loss ratio, slow reactions to network link failures and the absence of support for multi-domain multicasting.

Generally speaking, an overlay network can be defined as a network that is built on top of another network and that uses the basic services of the underlying network to provide a new service or optimize existing services. Using overlay network technology offers a number of advantages over providing support in the equipment in the underlying networks. Because overlay technology does not require a change in core Internet routers, an overlay network can be deployed much quicker than any change that would require a major infrastructure overhaul. Important benefits are the ability to span multiple underlay networks, possibly with different networking technologies, and to offer generic

higher-level services and support. A popular example of an overlay network is Skype Communications' Voice over IP service (VoIP) service that allows users to make voice and video calls over the internet. The Skype overlay is used to locate the IP addresses of the called parties and the QoS-aware route determination of the voice calls.

The broad domain of overlay networks can be split into two main categories: overlay networks that are formed by a set of interacting peers that are collaborating in order to profit from the use of their shared resources; and overlay networks that are formed by a third party that, for economical or other reasons, places a number of proxies to enhance the traditional network service or to offer additional services. Examples of the former include the use of peer-to-peer (P2P) networks to distribute and store files across the network and to provide VoIP and video streaming services. Examples of the latter include the usage of fixed overlay networks to provide QoS, increase resilience and offer multicasting. In [14] a similar classification and taxonomy of overlay networks is presented.

Overlay networks typically have components located in different (often hierarchical) locations of the network, to enhance the connectivity over multiple segments of the end-to-end path, from inter-domain autonomous systems to access networks. Resilient, scalable, transparent and quality-aware (inter- and intra-domain) routing services can be offered on overlay networks through dynamic overlay topology instantiation and traffic engineering. Often, monitoring components gather (cross-layer) networking information in order to steer the decision making process to adapt the overlay network characteristics on-the-fly, thus guaranteeing that service level agreements (SLAs) are respected. Smart Grids could benefit from such overlay functionality to dynamically organize the overlay network, gather meter data efficiently and optimally balance resource usage for supply and demand matching.

8.3 Technology

8.3.1 Introduction

Undeniably, the Internet Protocol (IP) is one of the most predominant underlying technologies in today's telecommunication networks. Thus, we can expect it to play a crucial role also in the context of Smart Grids. The Internet however was conceived as a best effort network, thus lacking direct support for the QoS requirements that many Smart Grid applications require, as pointed out in the Introduction. In this section, we outline the evolution of telecommunication networks—and in particular communication overlay technology—that aims to overcome the best effort limitations. Whereas this evolution originated for application scenarios beyond Smart Grids, the technological solutions that arose clearly can be applied to the current Smart Grid challenges posed on communication networks.

8.3.2 Evolution of communication overlay networks

The Internet itself started as an overlay network on top of the public switched telephone network (PSTN). Today, IP packet transport has evolved into a basic transport medium for voice, video and data. The success of the Internet was triggered by its strong interoperability and the decision to use a simple protocol to provide best-effort connectivity. This allowed other functionality to be pushed to other layers and be implemented at the edge of the network. One of the driving principles behind the original Internet was the "end-to-end argument in system design" [65], which states that functions placed at low levels of a system may be redundant and of little value when compared to the cost of providing them at that low level. An example of this concept is pushing the reliability feature to the network edge, for instance by using the TCP protocol. The Internet, while becoming very successful,

has grown to an enormous infrastructure. However, as was discussed previously, it has become very difficult to provide an answer for end-to-end support for QoS, resilience and multicasting, which essentially move away from the original simplicity behind the protocol. Furthermore, there are also problems with end-to-end routing created by the sheer Internet size, and parts of the connection, such as the last mile, still exhibit problems that result in packet loss, delay and a decrease in quality.

Overlay networks provide an abstract view of the network environment. They are often designed for specific needs that do not require precise knowledge of the underlying infrastructure [15, 33]. In overlay architectures, a set of nodes (servers, services, end-user equipment etc.) and virtual links that do not directly match those of the underlying topology, are often involved in specific applications. Data in such applications is routed according to these virtual links and an overlay network can therefore be viewed as a middle layer between them and the underlying topologies. Peer-to-peer overlays are a common implementation of overlay networks, and as such they have received a lot of attention over the past several years [5] (see also the "**Error! Reference source not found.**" chapter of this book).

8.3.2.1 Peer-to-peer networks

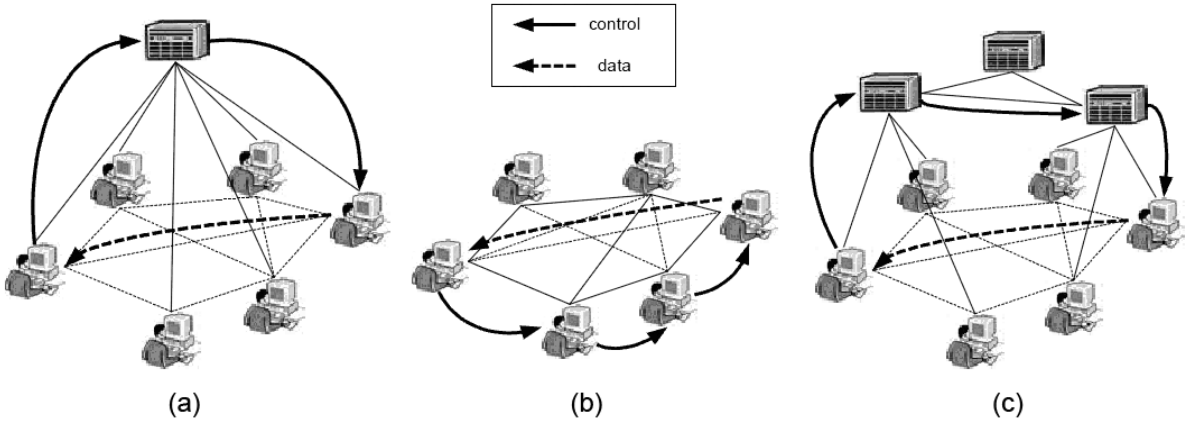

Figure 8.1 – Peer-to-peer overlays: (a) mediated, (b) pure peer-to-peer, (c) hybrid (reproduced from [6])

Peer-to-peer (P2P) overlay networks represent a special type of overlay networks and have received great attention over the last decade [5]. The proposed P2P networks comprise 1. Unstructured networks, and 2. Structured overlays. To adapt to specific application requirements, proposed solutions evolved to multiple coexisting overlays.

Originally, mainly mediated P2P architectures are introduced, where a central server is responsible for registration of and traffic control between peers. Afterwards, *unstructured networks* exploiting broadcasting as the primary means of communication are used. The popularity of P2P networks experienced rapid growth due to their usage for the sharing of content. However, using unstructured networks introduces problems in terms of communication resources, and restricts the possibility for managing differentiated policies [70].

To overcome these problems, a number of implementations have been proposed, including hybrid architectures and *structured overlay networks* based on distributed hash tables (DHT) [17]. The key feature of such structured networks is that they define specific network topologies that facilitate navigation in the overlay. They enable the deployment of components such as content or services in a flexible, scalable and decentralized way. Using distributed hash tables enables the efficient

diffusion of information among all clients and results in a system in which specific queries can be answered quickly. DHT-based architectures have a flexibility that has made it possible to successfully implement them over grid computing networks, and not only Internet-like structures. Other problems associated with P2P network are the bad mapping between the overlay and the underlying network [63]. Recent projects are addressing this problem by letting internet service providers (ISP) and P2P users cooperate [1]. Another service that can be offered with P2P overlay networks is the usage of end system multicast networks in which overlay multicast trees are set up to distribute the content to all interested receivers [60], or let participants engage in conferencing applications. Using a mesh pull approach is an alternative approach for distributing video content via P2P networks [39]. Video streaming services such as Tribler [62] are offered on P2P networks as well, and most of them use BitTorrent-like protocols for content discovery and distribution.

It is now generally accepted that different applications may require different P2P overlay structures, and currently there are several proposals on instantiation and parameterization for specific overlays, as they are needed. One way to create *multiple overlays* is by inheritance (i.e., instances are generated from a parent virtual network by inheriting signaling protocols and communication services, as proposed in Genesis [12]). Overlays based on declarative logic, defining their structure in a very compact and reusable manner, have been proposed in [57]. The proposed system, P2, is capable of directly parsing and executing specification from this language, thus constructing and maintaining overlays. However, these works only focus on the issue of defining overlays, not on instantiating and integrating different overlays, and making them dynamically parameterizable.

Frameworks have been developed that define and instantiate parameterizable overlay networks (which thus could be applied also in a Smart Grid context), such as JXTA (Juxtapose) [9, 44]. The JXTA technology is a set of open, generalized P2P protocols that allow any connected device to communicate and collaborate. Introduced by Sun Microsystems, JXTA's high-level vision is to increase interoperability among devices and networks. Overlay platforms on top of JXTA have been presented to support distributed and collaborative systems for a wide variety of industrial applications with similar requirements as smart grids.

The main trend is that the peer-to-peer paradigm has shifted in the last few years towards an approach where the peer functionality has moved from low-capacity end-user devices to more powerful and more intelligent network agents that have more information and control over the network communication.

For a more in-depth study of peer-to-peer networks and their applicability to the Smart Grid use cases, we refer to Section **Error! Reference source not found.**, "**Error! Reference source not found.**" (for a P2P architecture for smart grids), and Section **Error! Reference source not found.**, "**Error! Reference source not found.**" (for the requirements it is based on) in the "**Error! Reference source not found.**" chapter of this book.

8.3.2.2 Infrastructure overlay networks

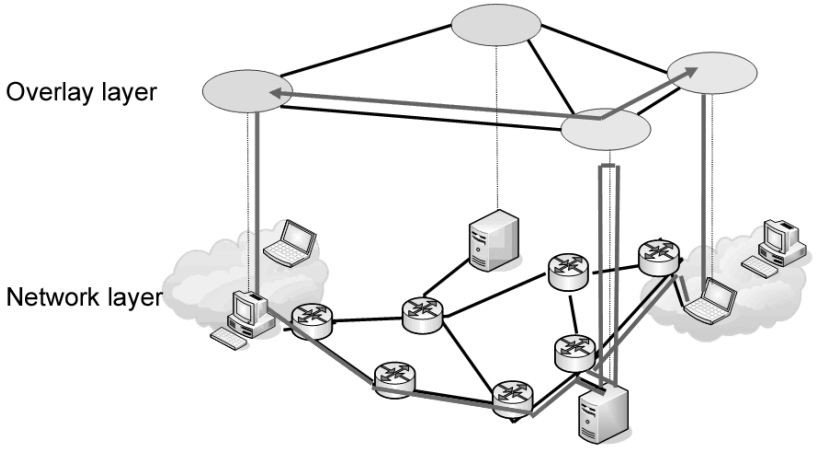

Figure 8.2 – Infrastructure overlays (reproduced from [6])

The second class of overlay networks is comprised of infrastructure overlay networks. Examples of services that can be provided with fixed overlay networks include the provisioning of end-to-end QoS, enhanced resilience, content delivery and multicasting. The fast deployment and flexibility of an extra layer offers a powerful and fast way to implement and provision new services. Content distribution networks (CDN) [74] are an example of infrastructure overlay networks. These networks consist of distributed sites that are used to enhance the delivery of content by improving speed, cost efficiency and scalability. Typically, CDNs have several replicas of content that are cached at several surrogate servers. Akamai Technologies [2] also adds support for alternative routes, in order to avoid degraded parts of the network.

The rest of this sub-section discusses the three main functionalities of infrastructure overlay networks: 1. Quality-aware routing, 2. Scalable and resilient topology construction, and 3. Multicast support. We give some representative examples below, and subsequently conclude with an overview of additional functional features such as security, NAT traversal and service discovery.

A representative example of *quality-aware routing* is the RON (Resilient Overlay Networks) project, which seeks to build an overlay network that is able to dynamically react to long path outages due to the long recovery times of Border Gateway Protocol (BGP) [4]. Servers are placed at different locations, allowing the selection of alternative routes at the overlay layer. These routes are explicitly monitored, using active probing to assess quality of routing paths (in terms of e.g., latency, loss, and throughput). The aim of the RON project is to provide extra reliability and the quick reaction to path outages. A similar idea is applied in [54], where paths via the overlay network are selected according to QoS metrics, which again are established based on active measurements. If links between overlay servers can be (dynamically) provisioned, the problem arises of appropriately sizing those overlay links. An example solution is presented in [24], where the authors look at an overlay network that is formed by a set of servers with a fixed position in the network: they determine the bandwidth that needs to be reserved to satisfy certain QoS constraints (assuming that each QoS constraint can be translated to a link utilization threshold) on the paths between the overlay proxies by using a model that is based on pipe and hose SLAs.

To improve the *scalability* of aforementioned approaches [4, 54], the authors of [75] note that the decision to route via the overlay network would be better be made at the edge in the overlay access

components, rather than by the overlay servers [75]. Deferring routing decisions to the edge provides a more scalable solution, since the overlay servers themselves are not responsible for deciding on the route via the overlay network and for changing the packets. In addition, it enables the extension of the overlay routing service to clients located anywhere in the network. Additionally, instead of the full mesh overlay networks that are often used, the use of appropriate topologies can further increase scalability. Typically, a hierarchical topology organization is proposed. An illustrative example of such a hierarchical approach is described in [54], which proposes QoS-aware routing algorithms for overlay networks with hierarchically organized brokers.

The rigid topology of structured overlay approaches hardly fits the needs of modern networks with highly dynamic usage patterns. Therefore, some recent proposals suggest the adoption of overlays with *adaptive topologies*, in which the very structure of the network is determined at run-time, and based on the patterns of activity that occur inside of it. Overlays could, for example, arrange nodes in ways that place nodes with related patterns of data close to each other [37]. Another option, suggested by [16], involves grouping reliable nodes into clusters and moving unreliable ones towards the outside bounds of the network. These techniques are very interesting due to their high adaptability, and the fact that they allow robust and extremely scalable structures. Adaptive structures, together with the possibility of adopting gossip-based [43] and probabilistic multicast methods [28], have brought research focus back to unstructured overlays based on random graphs [3]. Even though the lack of any deterministic structure is making search operations less efficient, the low diameter characteristic of such overlays could be successfully employed in the implementation of multicast/broadcast systems with low message propagation latency (as required in many Smart Grid applications, see Section 8.2, “Introduction”). Adaptive topologies can clearly also be exploited to increase overall resilience. This idea is pursued in [53], in which the authors study the influence of the overlay topology on the overall resilience. A significant impact of overlay topology on the routing performance has been found, and the conclusion was that in constructing the overlay topology, the underlying physical network information should be taken into account to construct effective overlay topologies: two topology-aware algorithms have been proposed as preferred solutions.

Overlay networks can also be used to provide *multicast* support, which could be useful in a Smart Grid context where, for example, real-time pricing or other common control signals need to be distributed to a large set of participants. The basic idea is to use so-called (unicast) tunnels, whereas the multicast forwarding logic is implemented in the overlay server. A sample of such an approach is [56], in which the authors discuss how such tunneling can give end users access to network multicasting services, even when they are in a domain without explicit multicasting support. The multicast backbone network Mbone [27] also used a tunneling approach to give access to multicasting without requiring ubiquitous deployment of IP multicasting in the network layer. It is possible to offer the multicast services with certain QoS guarantees: in [22] a dedicated overlay multicasting infrastructure also takes QoS requirements into account when setting up the overlay distribution trees; the focus is on pushing the multicasting functionality to a higher layer instead of providing ubiquitous IP layer multicast access. The difference of [22], compared to other work in the overlay multicasting domain, is that it looks at tree construction specifically aimed at providing a low cost distribution tree with a bounded delay to provide QoS. The platform they provide is focused on more long-term sessions, and is based on the exchange of information with the network provider and the ability to make reservations in the underlying network. The adaptive topology idea can also be adopted in a multicast scenario: the Yoid project [32] allows a group of hosts to dynamically auto-configure into two topologies—a shared tree topology for distribution of application content, and a mesh topology for robust broadcast distribution of control information and, where appropriate, application content. In [8], resilience is added: a probabilistic resilient multicast solution is applied

with application layer multicasting, and achieves high delivery ratios at low latency constraints (hundreds of milliseconds).

Overlay routing also allows for integration of *security* solutions and supports efficient connectivity and other higher-level functionality. One such example is the usage of intermediate peers for improving firewall and Network Address Translation (NAT) traversal when establishing end-to-end communication sessions between peers. Such a technique is often used in VoIP P2P communication networks such as Skype [9]. Proxy components at the edge of the network [75] could also take both application and network information into account to perform high-level services like data computing and bandwidth management. *Service discovery* is another problem that occurs in several domains, especially web services. While the lookup service can be provided through a central Universal Description, Discovery and Integration (UDDI) [71] server, new trends also suggest implementing it with P2P networks [31].

8.3.3 Communication overlay technology overview

While providing powerful mechanisms to handle decentralized and self-organizing networks of services, P2P networks are very often designed for specific applications, and their choice of architecture (e.g., structured vs. unstructured) strongly depends on the kinds of services that need to be supported by the overlay. In order to aim for a P2P network as a generic substrate for general-purpose Telco or Smart Grid services, a more flexible approach is required, and the possibility of instantiating a "generic overlay" by properly combining different solutions for different services is needed. (See also the discussion in Section **Error! Reference source not found.**, "**Error! Reference source not found.**," in the "**Error! Reference source not found.**" chapter of this book.)

Another promising field in the area of communication overlays involves semantic technologies—applications that query specific resources based on attributes defining the resources. The AGORA project [19] is an example of such a semantic overlay in which distance metrics based on Extensible Markup Language (XML) descriptions are evaluated for dynamic neighbor selection in small world Smart Grid overlays. Integrating search functionality into the overlay network for optimized and enriched query and information handling will provide benefits for Smart Grid applications.

Providing interoperability in communication overlays for different domains is an important research topic as well. Session management, for example, is typically organized on communication overlay networks using Session Initiation Protocol (SIP) [64] or its distributed variant P2PSIP [59]. Using such standards in Smart Grid applications could provide significant benefits to the electricity industry, an idea that is supported by the Smart Grid Special Interest Group [69]. While the current focus is on electricity, similar concepts can be applied to other utility systems such as water and gas. Such a modernization has recently become a significant focus for governments, vendor communities (utility companies and partners) as well as Industry/Standardization organizations (NIST, GridWise, IPSO Alliance, the IETF and IEEE). IEEE P2030 mainly provides a Smart Grid interoperability reference model (SGIRM) that identifies and defines generic interfaces between functional domains, focusing on transport through application layers [41].

8.4 Vision

Looking at Smart Grid applications from a high-level perspective, we see three major types of applications that can arise, using the overlay network technologies detailed above:

- **A wide-area measurement system**, targeted for transmission network control based on, for example, PMU data.

- **A meter data aggregation system**, to collect and aggregate meter data from the massive amount of smart meters positioned in the distribution network.
- **A peer-to-peer oriented network** for coordination and control for demand-supply balancing.

We will outline each of these cases in the following subsections, illustrating how the overlay networking concepts introduced before can be applied in a Smart Grid context, and pointing out some requirements and challenges. In a perfect world, a single generic, flexible software/middleware solution should be able to offer the required communication components and interfaces for control and data aggregation algorithms supporting all of the following scenarios in a scalable way.

8.4.1 Wide-area measurement system

Synchrophasors (or phasor measurement units, PMUs) generate data that is coherent and real-time; they measure characteristics of power (e.g., magnitude and phase angle of voltage) at a particular time, synchronized to a common time reference (typically a GPS clock). Thus, combining information from multiple PMUs scattered across the transmission network allows an accurate system-wide view of practically the entire transmission network. Clearly, information that can be recorded and accurately time-stamped may also include measures other than just voltage and current, such as breaker status, active/reactive power, etc. As outlined in [7], many applications can benefit from such measurements to provide increased reliability, efficient operation and stability of the power transmission system:

- **State estimation:** Fast state calculation is important mainly for reliability, and the time-synchronized measurements provided by PMUs enable quick response times for wide-area protective measures.
- **Distributed control:** The increasing contribution of renewable sources (e.g., windmills, solar panels) to power generation implies greater variability and unpredictability compared to the familiar on-demand sources. These variations can be handled more effectively with algorithms that use closed-loop feedback control exploiting real-time measurements. Given the accurate clocks, control signals themselves can be synchronized.
- **Protection:** After local protection offered by quasi-instantaneously responding relays, wide area system protection schemes can be put in place. These can be greatly facilitated by the PMU data, to deal with potential instabilities that may occur on a short timescale (50 to 250 ms range) after a failure.

Thus, there are clear drivers for a wide-area measurement system for data delivery (WAMS-DD). The authors of [7] have proposed a publish-subscribe system, illustrated in Figure 8.3(a). Publishers are the application programs or firmwares that send out a continuous stream of messages, in casu the PMU data. The applications subscribe to the relevant information (for protection, distributed control, state estimation, etc.). Functionally, publishers need to register their published variables with the data delivery system (i.e., the WAMS-DD), and subscribers need to communicate their request for subscription to a particular (set of) variable(s). The WAMS-DD can be based on middleware, which then would produce so-called proxies (one for each producer, and one for each subscriber) that packages the parameters into messages and provides the (interfaces to) delivery mechanisms. The actual delivery can be based on aforementioned overlay paradigms. As an example, a canonical peer-to-peer architecture is suggested in [7], as illustrated in Figure 8.3(b). The data delivery could be based on the multicast overlay approaches discussed earlier. Following the overlay concept, the communication network for the delivery plane can be agnostic of the P2P components at its edges:

controllable mechanisms for affecting the traffic, and all WAMS-DD specific mechanisms residing in the proxies.

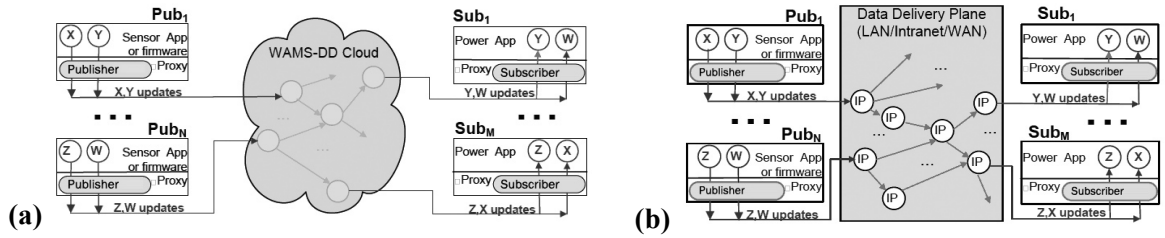

Figure 8.3 – Architecture of a WAMS-DD (reproduced from [7], with permission)

The main (non-functional) requirements for such a WAMS-DD include the following [7]:

- **Requirement 1:** End-to-end guarantees must be provided over the entire grid, given the criticality of protection and control applications that depend on the data delivery.
- **Requirement 2:** Multicast is the normal mode of operations, not point-to-point.
- **Requirement 3:** End-to-end guarantees must be provided for a wide range of QoS parameters (i.e., this may depend on the application).
- **Requirement 4:** Some applications require ultra-low latencies and one-way delivery (e.g., order of one full cycle, thus 16 to 20 ms for 60-50 Hz systems)
- **Requirement 5:** High throughput is required. Currently, PMUs measure at 30-60 Hz; future applications may cover, for example, digital fault recorders that sample at 8 kHz and output at 720 Hz.

The multicast paradigm clearly has been addressed in current state-of-the-art overlay approaches (see before), and optimization for QoS to some extent is taken into account already. Nevertheless, the stringent QoS requirements of some applications, in particular as expressed in Requirement 4 and Requirement 5, above, are major challenges using state-of-the-art approaches. To meet extreme latency and throughput requirements, it is clear that lower network layers need to step in to guarantee such performance. Isolation of the PMU traffic by setting up tunnels using (G)MPLS technology, for instance, is one possible approach. As [7] rightly points out, the stringent requirements that seem to be unique to the electric power market are achievable using state-of-the art embedded computing, and carefully design the core data delivery from an end-to-end perspective, without overloading it with unnecessary features. For particular implementation guidelines, we refer to [7].

A similar broker-based middleware framework, GridStat [38], provides flexible, robust, timely, and secure delivery of operational status information for the electric power grid. A common service platform for disseminating power grid status information within and between power utilities and marketers ensures qualitative delivery to multiple participants through a publish-subscribe architecture.

8.4.2 Meter data aggregation system

Automatic meter reader (AMR) systems allow utility companies to aggregate meter data from various sources over a communication network to the utility servers. Currently, there are four major

types of AMR communication networks: power line carrier (PLC), cellular network, telephone lines, and short-range radio frequency [46]. In PLC technology, data is transmitted over voltage transmission lines along with electrical power, and depends on parameters such as frequency, propagation speed, voltage level, distance and presence of transformers. Major challenges are high loss rates on the transmission medium, scalability issues due to limited geographical coverage, and termination of deployments in several countries due to availability of lower-cost alternatives. Sending short messages (SMS) over GSM networks allows for standardized communication over widely available cellular networks. However, scalability and reliability is questionable, and possible high latencies and failure rates reduce the usability of such technologies for low-delay applications. Reliability on bi-directional telephone lines is typically much better, and increased availability and low cost make this alternative, although known for quite a while, worth investigating. Low-power RF facilities at the costumer site (e.g., Bluetooth, Wi-Fi and Zigbee) depend on the signal power and the frequency band. Sensor network solutions are used nowadays, but often fail as connecting all nodes is difficult due to far nodes or parent nodes failures. For a more in-depth discussion of issues related to these lower layer technologies, please refer to the "**Error! Reference source not found.**" and "**Error! Reference source not found.**" chapters in this book.

The introduction of smart meters has spurred various research and demonstration projects that try to solve the problem of collecting utility meter information in real time, currently on time scales of five minutes or (usually) more. The main concern is scalability, given that a single utility can have millions of customers. Also, apart from mere gathering information (e.g., for billing purposes), it is desirable to make effective use of the meter information for coordination and control purposes. This involves synthesizing and interpreting the massive amounts of 'dumb' data to extract rich information supporting intelligent operational decisions. We discuss such control approaches in the next subsection.

On a high level, we can identify the following functional requirements (Requirements 1 and 2, below) and non-functional requirements (Requirements 3, 4 and 5, below) for a meter data aggregation system:

- **Requirement 1—Meter detection and validation:** The system should be fairly plug-and-play (i.e., configuration of the meters at install time should be minimal). Registration of the meter should be (semi-)automatic, and some basic validation should be performed. Clearly, authentication will be crucial.
- **Requirement 2—Flexibility in meter reading operation:** Both push and pull operations are likely to be required (i.e., the meter may need to actively send its data on its own initiative, or readings may be explicitly requested by other system components).
- **Requirement 3—Privacy and security:** The data captured by the meter can reveal information about the customer's behavior, and hence is quite sensitive (cf. delayed rollout of smart meters in The Netherlands); (see Section 8.5.3, "Security and privacy," for further information). If metering data will be used to, for example, enable demand side management, third parties (energy service providers) may need access to this data.
- **Requirement 4—Fault tolerance:** The system should be robust against potential failures, especially of the communication channel towards the meter. Depending on the time granularity of measurements and how detailed this needs to be communicated to the utility, a varying amount of meter data will need to be stored locally in (or near) the meter.
- **Requirement 5—Scalability in space and time domain:** Spatial scalability (i.e., in terms of number of participating meters) is of primordial importance. In addition, the time granularity of meter data may vary according to the application. For example, for billing it

will depend on the rate structure (real-time pricing versus time-of-use). Note that accurate meter clock synchronization is an important concern for the meter data aggregation system.

In terms of Requirement 5, we may observe an evolution to finer granularity measurements, if not for billing at least for (close to real-time) control mechanisms, as discussed in the next subsection. In the space domain, we may note an increasing amount of measurement components (e.g., an evolution towards deployment of wireless sensor networks). In particular, we can expect submetering of individual or a small subset of appliances. This opens up the question on the relation between the utility metering systems (recording the whole household as a single entity) and so-called home energy management systems (HEMS) deployed within the household.

The latter also implies interaction and possible integration with control mechanisms. In the case of HEMS, this is local control to optimize energy consumption within the household locally. We also envision integration of meter data aggregation with control systems of power networks (distribution and possibly beyond). Such evolution can already be observed in research projects [34] such as the European FP7 project OpenNode, taking inputs from the OPENMeter project on AMI, and ADDRESS on active demand. To support such an evolution with scalable architectures, we believe the use of communication overlay technology will be crucial.

8.4.3 P2P coordination and control

Increasingly, dispersed energy resources (DERs) such as wind turbines, solar panels and combined heat-power units (CHP) are deployed in the distribution network. Clearly, the renewable sources are highly unpredictable compared to classical bulk generation using conventional sources (e.g., coal, nuclear and hydro). Moreover, if sufficient generation (and possibly storage) facilities are present in part of the grid, such a part could be operated in so-called islanding mode, as a microgrid. Hence, control algorithms are required to deal with both the distributed and fluctuating nature of the DERs, as well as with potentially changing network configurations (cf. transitions to/from islanding mode). Apart from the power engineering aspects that need to be dealt with, questions arise as to providing appropriate communication and control infrastructure. Giving the distributed nature of DERs, and the need for a dependable solution (which is robust against defective DER units, and their associated communication components), distributed coordination is a natural choice in this scenario.

A sample solution is discussed by the authors of [20]: they propose a peer-to-peer overlay network (called Agora), because its flexible nature excellently matches the distributed microgrid control application they envisage. The dynamically varying properties (as well as the static ones) of the DER/load units in the microgrid are represented in XML. Key to their concept is to quantitatively describe semantic “similarities” between units, which indicates the probability that they will interact for a given microgrid application. A small world overlay network is constructed between the units (the nodes in network terms), such that the resulting network nodes with similar functionality (meters, manageable loads, generators, etc.) are clustered, while so-called pupil links connect them to units they will cooperate with in microgrid applications. The small world property ensures that the number of hops for a message to go from one node to another will be limited (e.g., smaller than five), even if there are hundreds of nodes in total.

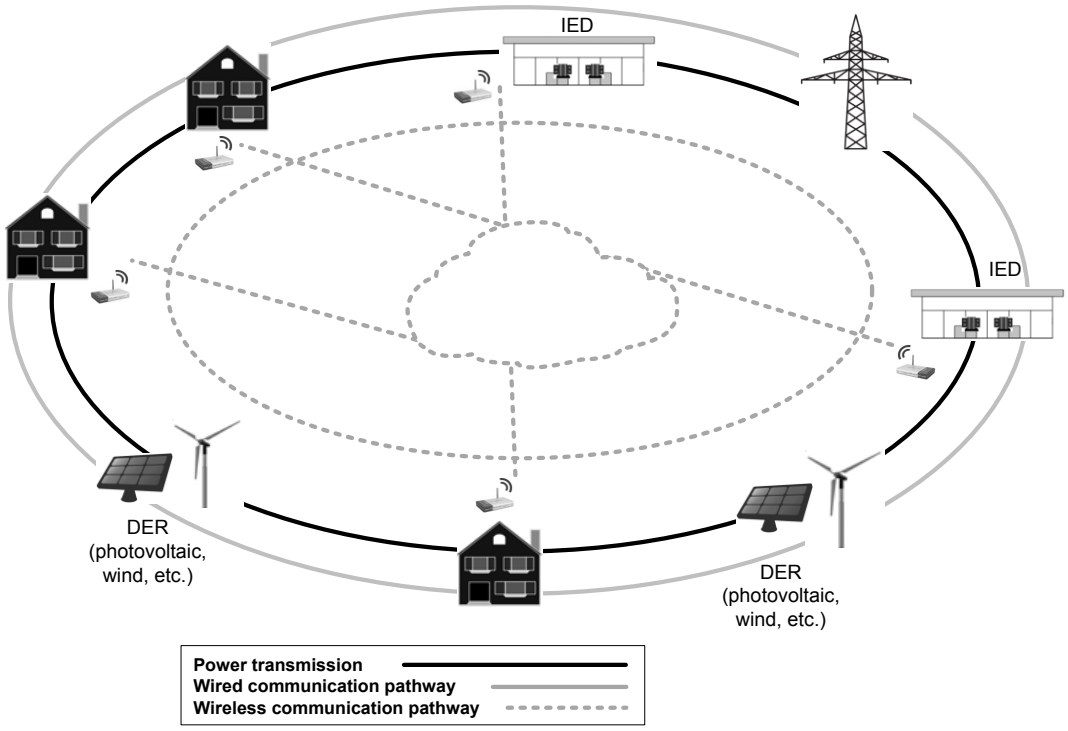

Figure 8.4 – Microgrids, consisting of DERs interconnected via the electricity grid and corresponding IEDs interconnected via the communication network

The main requirements for such a DER-control can be summarized as follows (in functional Requirements 1 and 2, and non-functional requirements 3 and 4, below):

- **Requirement 1—Dynamic participation of components:** Not all DER units and loads in the distribution grid to balance will be available all of the time. Moreover, in islanding modes it is not necessarily known beforehand
- **Requirement 2—Resource discovery:** This is closely related with the previous requirement. The dynamic properties (including presence!) of the participating DERs and loads call for a plug-and-play like setup.
- **Requirement 3—Fault tolerance:** The system should be robust against failures (both of DERs and their corresponding communication/control components).
- **Requirement 4—Scalability in space and time domain.** The control and communication network should scale well with increasing number of DER units (hundreds of nodes). Similarly, the time scales for control actions may need to be very limited (few tens of milliseconds).

Current state-of-the-art in overlay networking, and in particular P2P networks, is clearly able to cope with most of the aforementioned requirements. Nevertheless, as [20] indicates, some differences with more classical overlay networks for content sharing/distribution do arise: the audio and video files typically shared through P2P networks are static resources, which themselves do not change over time, whereas the DER units in microgrids clearly vary very much over time. From this perspective, certain P2P approaches (such as for video streaming) may be relevant areas of research that may inspire the Smart Grid community, since they deal with dynamic content as well. As

before, mainly the possibly low latencies (Requirement 4) may be a bottleneck, if the underlying communication network over which the overlay network is provided is shared with other (non-power grid) applications. For a more in-depth discussion of specific P2P solutions for smart grids, we refer to the "**Error! Reference source not found.**" chapter of this book.

8.4.4 Outlook

The aforementioned scenarios boil down to (real-time) monitoring data aggregation, and (distributed) control. Most power applications can be characterized as operations where a subset of data (spatial locality) is consumed within a certain specified time (temporal locality); this spatial and temporal locality can be leveraged as an opportunity to optimize resource usage in the communication network, and maximize reliability by adopting a decentralized data-centric information infrastructure [50]. In [50] the authors outline a generic middleware that could be used for aforementioned application scenarios, exploiting an overlay network of grid hub nodes akin to a structured P2P network, adopting the pub-sub system [as opposed to today's typical master-slave architecture of energy management systems (EMS)] to deliver time-sensitive data to appropriate entities. Spatial locality can be duly exploited by a virtually distributed storage system (thus avoiding a single point of failure and bottlenecks associated with centralized approaches). Observing current adoption of cloud-based technologies, we can expect a shift from pure P2P solutions (mainly relying on functionality in end points) to adoption of concepts borrowed from cloud services. An example use case of such cloud-inspired solutions is discussed in [48]. For more details on the architecture (e.g., security considerations), we refer to [50]. Very specific for smart grids are the stringent reliability and low latency requirements (see Table I in [21]), for which today there is no well-known protocol that meets them. Additionally, most well known protocols are not lightweight (note that [49] proposes a candidate solution).

Future Smart Grids will continue to require the previously raised functionally essential system functions, and thus the cited high-level requirements will continue to hold. It is foreseeable that the real-time aspect, and the scale of distribution of the components involved, will only grow in importance. Miniaturization and massive deployment of measurement components, as exemplified by the evolution towards (wireless) sensor networks, will call for extremely scalable approaches to manage the complexity of Smart Grid solutions. On the other hand, the power grid can be assumed to evolve to a highly dynamic environment, not just in terms of power flowing in various directions (cf. the evolution of customers to so-called prosumers), but also in terms of topology and interconnections (cf. microgrids which will operate either on or off of the main grid at different times). To deal with such large distributed environments that are characterized by a great dynamicity in both time and space domains, with possibly a large amount of constrained devices (cf. sensors), there will be a need for adaptive algorithms to efficiently operate in all conditions. To manage this complexity, the software architectures that will have to support data collection and control—and thus configure the (overlay) communication network—will need intelligent and highly flexible, modular designs. We believe that a great challenge awaits to build on ideas from the autonomic networking community to address these issues, especially incorporating components into embedded (wireless) sensor devices. This also implies pure communication network challenges at lower layers (layer 1-2 as discussed in the "**Error! Reference source not found.**" chapter, and layers 2-4, treated in the "**Error! Reference source not found.**" chapter of this book) and possibly re-thinking the communication network layers (e.g., through cross-layer optimizations). In that respect, evolutions from Future Internet [67] activities will be interesting to follow and to adopt/tweak them with respect to the aforementioned requirements for Smart Grid applications.

The adoption and adaptation of the overlay technologies discussed previously will certainly face challenges as well. In this respect, auto-configuration and auto-adaptation of the system will be one

of the more important issues (e.g., involving automatic migration of certain components to the most appropriate location to run them), thus, self-learning systems should be strived for. In addition, it is important that overlay networks are not blocked or shaped by ISPs to allow transfer of critical information in the overlay network. We strongly believe Internet Neutrality should be guaranteed, and only malicious or unfair behavior should be prevented, detected and acted upon, thus not hampering overlay-based applications (e.g., in the context of Smart Grids).

8.5 Challenges and issues

While the basic ideas and even fundamental technologies are already in place to implement the overlay approaches outlined in the previous sections, some challenges remain in applying them in the Smart Grid scenario. Apart from issues pointed out above (e.g., the dynamic content generated by PMUs and meters), we will briefly touch upon important challenges in the following areas:

- Resilience
- Quality of Service (see also Chapter 8)
- Security and privacy

8.5.1 Resilience

The power network is designed to be resilient against various failures, and has various protection mechanisms in place. Clearly, if its control in Smart Grid scenarios is delegated largely to (distributed) systems based on communication networks, the latter also should be fail-proof. In addition, in scenarios including the aforementioned islanding mode of operation of certain parts of the power grid, the grid topology may become dynamic. The overlay networks for the scenarios presented in Section 8.4, "Vision," clearly need to be made aware of both the unplanned failure scenarios and the planned (or at least expected) grid topology changes. Thus, also the overlay topologies may need to change over time, requiring adaptive approaches inspired by the proposals discussed before (see [3, 16, 28, 37, 43]). Results and proposals from the autonomous networks research community may clearly be relevant in designing network-based coordination and control of resilient power networks.

Note that even with legacy wide-area monitoring and control systems (SCADA/EMS), some disturbances require extremely rapid actions that simply cannot wait for the results of, for example, state estimation based on PMU data, to become available. Hence, special protection schemes often are in place, which are localized, hard-wired, and complementary to wide area control. In the same manner, local control mechanisms can be put in place to cater for failures in the overlay or communication network (which lead to temporary outage of distributed control). This may give rise to multi-layer recovery strategies, not unlike those in multi-layer communication networks (e.g., IP over WDM; see Chapter 6 in [73]). Note that these new (e.g., PMU-based) systems for the operation, monitoring, control and protection are generally known as WAMPAC systems: Wide Area Monitoring, Protection, and Control.

With respect to the communication network itself, certain requirements (e.g., for availability) will be greater in Smart Grid networks than for more conventional communication scenarios. Especially the channels that are involved in carrying signals (e.g., teleprotection of the power grid) are extremely critical. Similarly, information exchanged in the overlay networks may be very critical. If the telecom network incorporates packet switching technologies (e.g., Ethernet, IP etc.) rather than solely guaranteed circuits (e.g., SONET/SDH), this calls for appropriate protection strategies.

8.5.2 Quality of Service (QoS)

Given the aforementioned criticality of the messages exchanged within the overlays, especially compared to more traditional applications carried over telecommunication networks (e.g., voice, video, internet data), there is also a clear need for that underlying telecommunication network to be able to offer certain guarantees. (Note that even when the communication network is a dedicated one for the Smart Grid applications alone, multiple such applications may coexist. For example, the meter data aggregation overlay may run over the same physical network media as the control and coordination overlays, and even other less critical applications may coexist, such as video streaming of signals from surveillance cameras.)

Hence, for the connections between peers in P2P overlays as presented earlier, we may want to provide certain reservations so that the connections adhere to certain guarantees (e.g., [24] relies on reserved bandwidth between overlay proxies). Realizing this, in the GridStat project [35], a general QoS network architecture for supporting P2P communication was proposed by Bakken et al. [7].

While bandwidth requirements may be fairly reasonable (compared to, for instance, high-resolution video streaming scenarios, or massive data transfers in scientific computing), the main issue for Smart Grid networks may be latency. Various critical applications are cited to have latency requirements in the millisecond range (e.g., a few tens of milliseconds for PMU data) [40, 42].

8.5.3 Security and privacy

As will be discussed in more detail in the "**Error! Reference source not found.**" chapter of this book, privacy and security are a prime concern in a mission critical system such as the power network. First, there is need for privacy of measurement data (such as obtained from PMUs as outlined in Section 8.4.1 "Wide-area measurement system," or smart meters described in Section 8.4.2, "Meter data aggregation system"). Secondly, systems for demand response etc. that would control energy consumption (as exemplified in Section 8.4.3, "P2P coordination and control") require the control decisions to be issued by the rightful party. This calls for appropriate enforcement of authentication (to establish the identity of communicating/controlling instances), integrity (to ensure messages are not tampered with) and confidentiality (preventing unwanted access to data).

Some initial ideas are proposed in [50], where the authors propose an overlay of trusted hub nodes: they advocate for the use of secure channels (based on public-key-based credentials) between the hubs, encrypting the data exchanged, and storing the encrypted data. One remaining issue they indicate is that none of the current Internet standards (TLS and derivatives) seems a perfect candidate for Smart Grid use cases, mainly failing to meet the mission-critical requirements that call for protocol simplicity and analysis possibility. Another essential challenge is answering whether emergency overrides for gaining access and control should be possible, and if so, how to allow them (e.g., through special key escrow mechanisms). Next to such fundamental issues, there is also the sheer scale of the Smart Grid system, which introduces challenges in terms of configuration and maintenance: an illustrative example in [47] notes that a public-key infrastructure (PKI) system providing X.509 certificates is believed to require one support staff for approximately 1000 certificates (clearly implying huge challenges for a utility within the order of a few millions of meters).

Also of concern is the privacy of the end user, whose behavior (such as daily patterns in leaving his or her home) may be deduced from metering information [47], and whose individual device usage could be identified [51]. This constitutes one of the typical complaints by consumer organizations. Note that while information on consumed energy clearly is required to be unambiguously attributable to a particular customer identity, that is not really the case for instantaneous power

generation and distribution (e.g., knowledge of the substation a customer is hooked up to could suffice). One way of hiding user identities could thus be to aggregate such information at the required level of visibility (e.g., the substation). Other proposals include ways to prevent third parties from relating multiple messages sent by the same appliance or even customer [13, 25]. A more drastic way to mask actual consumption is to have an energy storage system in place, thus modulating the net power consumption as read by the meter [45].

Note that in Smart Grid scenarios, more than two parties may be interrelated; in addition to the energy supplier (which may or not be the same party as the distribution net operator) that bills the customer, a third party energy service provider (ESP) may deliver services to assist the customer in lowering their bill, while providing load shedding services to grid operators. Hence, this calls for multi-party trust relationships, with the associated complexity of correctly handling permissions, and priorities to monitor and control possibly the same devices. Such multi-party issues seem not yet to be addressed by current proposals as discussed earlier [7, 20].

8.6 Summary

Smart grids will incontestably rely on communication networks to propagate the necessary information to realize various control mechanisms. We believe that in realizing the (distributed) control algorithms, a self-organizing overlay network will play a crucial role. It is doubtful that the underlying communication network will be deployed (and optimized) for a single grid application. Hence, overlay network techniques will be crucial to ensure a flexible, cost effective and future-proof solution. Such a self-organizing network should support functions such as communications resource discovery, negotiation and collaboration between network nodes, connection establishment and maintenance, to provide the performance guarantees required by Smart Grid/metering applications.

Current state-of-the-art and lessons learned from the distributed computing community can be applied and extended to cater to the unique and challenging requirements of Smart Grids. We have outlined relevant research achievements in the domains of peer-to-peer networking and infrastructure overlay networking. Application of such ideas have been exemplified: we have illustrated the possible construction of a wide-area measurement system data delivery network to support various PMU applications, as well as a more distribution-network oriented peer-to-peer approach for microgrid control, and a content aggregation network approach to collect meter data. Future challenges will likely arise from increased dynamicity in both time and space domains, as well as a proliferation of measurement sensor devices.

From these examples, it is clear that fundamental concepts from the distributed computing and communication network communities can be applied in Smart Grid scenarios. Nevertheless, it is also obvious that Smart Grids do have their peculiar requirements, which make them substantially different from common overlay network scenarios (e.g., the time-variability of the peers in the microgrid scenario, and the high throughput and low latency requirements). Thus, we may need to revisit known concepts to cater to Smart Grid traffic (e.g., resource allocation, routing, and QoS); traffic generated by Smart Grid applications will likely differ quite a bit from today's traditional browsing/downloading/streaming applications, with a mix of both real-time and non-real-time traffic being generated and distributed across different parts of a Smart Grid. In particular, the need for low latency communication and stringent delivery guarantees for real-time applications seem the hardest to meet. Given that dedicated networks will be not cost effective, there is a need for mechanisms of isolation and bandwidth reservation for particular (Smart Grid) flows. For this, we need the overlay

approaches to be able to request guaranteed communication channels, such as the (G)MPLS-like approaches discussed in the "**Error! Reference source not found.**" chapter of this book.

8.7 Recommendations

In the current power network, it is not unusual for intelligent electronic devices (IEDs) to take local control actions in real-time. Indeed, to guarantee the safe operation of the grid, robust control that does not require any communication or interaction may be an acceptable option. Nevertheless, it is clear that a wider view of the system could allow more optimal decisions (in terms of limited waste of energy, fairness to all users of the system etc.). Thus, we envision an increase of distributed/decentralized control of power networks. Indeed, the evolution towards a Smart Grid will imply a transition to increasingly distributed generation (DG), which will be less predictable/controllable (cf. renewable energy sources) and no longer map a clear downstream power flow path from generation plants to consumers. This also will incorporate power electronics with more advanced functionality, for both control and measurement, to allow for more dynamic configuration and operation.

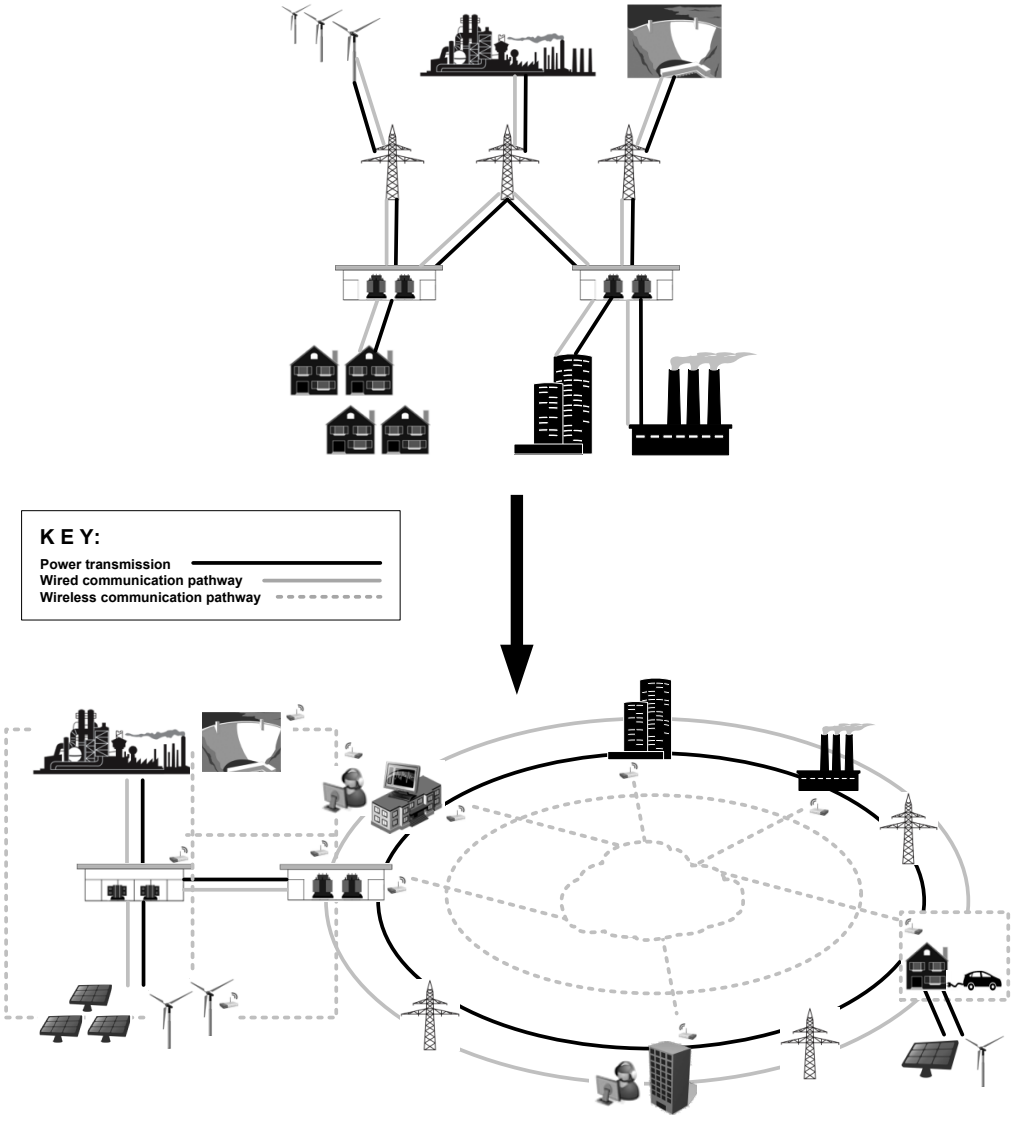

Figure 8.5 – The evolution towards a Smart Grid

Therefore, there is a clear opportunity and even need for *distributed or at least non-centralized control strategies* that coordinate the supply and demand in real time, as well as guarantee correct and safe operation of the grid. The current power system's intelligence in terms of networked infrastructure mainly resides in the power grid's "backbone"—i.e., at the transmission level, for instance based on SCADA (Supervisory Control And Data Acquisition) systems—where wide-area monitoring, protection and control actions are taken. Given evolution to DG and hence decentralized energy production, even up to the level of individual consumers (e.g., photovoltaic rooftop panels), it is clear that such advanced control networks could reach into the distribution networks, or even into consumers' homes: "the move towards the Smart Grids has to start at the bottom of the chain." [30]

First of all, the latter could imply a costly configuration/installation burden. The obvious recommendation to avoid, or at least significantly minimize, such complexity is to ensure emergence of *plug-and-play system components with embedded intelligence that could operate transparently in a variety of system integration and configuration scenarios*. Note that such configuration not only needs to occur on install-time, but also during day-to-day operation, and configuration changes may need to be implemented. In particular, operation of microgrids poses quite some challenges. A microgrid is an interconnection of supply, loads and storage that could operate on its own, disconnected from the grid in so-called islanded mode. Dis/reconnecting the microgrid to the main distribution grid clearly calls for cautious actions, from the power network's perspective.

A popular approach to provide the required autonomic networking solution that can deal with such dynamic changes effectively is using agent-based systems [18, 61]. Typically, such agent systems allow for (near-)optimal control with a minimum of data exchange and computational burden. Yet, for some applications, solutions have been devised that even operate without any inter-unit communication, such as for microgrid control [72]. Nevertheless, to achieve optimal coordination (e.g., across multiple microgrids), there is a clear opportunity for communication technologies as an enabler of closed-loop control based on information exchanged through (hard-)real-time networks.

Another area of research that can be explored more deeply is that of *multi-level control strategies*, combining local control with distributed coordination. For example, one can think of self-learning adaptive approaches that alternate the control strategy between local decisions and distributed coordination; this adaptation could be triggered by detected changes in either the power network, or the communication network (e.g., lack of bandwidth), or both. Indeed, part of the challenge in developing control strategies for Smart Grids implies their need to be extremely robust, given the high availability requirements posed to power networks. Given the structure of the power network, as well as its reliance on communication networks in Smart Grid scenarios, this gives rise to *multi-layer network architectures and related resilience challenges* (as pointed out earlier in Section 8.5.1, "Resilience"), which are largely unaddressed in the Smart Grid context to date.

Clearly, the standardization and interoperability of such architectures is another concern. Ideally, an ICT architecture should be proposed that considers all functions required to realize a Smart Grid, and hence caters to metering data collection/aggregation, power network state estimation, and intelligent control. One could dream of a unified communication network infrastructure, for reasons of cost efficiency in both deployment and maintenance, which is able to carry all associated traffic (with different requirements, such as latency and bandwidth). We believe that the development of software architectures (as exemplified in Section 8.4, "Vision,") is a crucial step in realizing that vision, and calls for further *interdisciplinary research from control, communication and power network communities*. Once research has pointed out a satisfactory direction, standardization is a prime concern and calls for definition of a framework and the interfaces that should be adhered to. Note

that current standardization efforts in the realm of Smart Grid communications mainly focus on data formats (cf. the Common Information Model, CIM, in IEC 61970 and IEC 61968) and data communication (e.g., IEC 61850 for substation automation), while main architectural ideas are also being discussed (e.g., see IEEE P2030). Discussions are ongoing in terms of communication technologies, such as for neighborhood/field area networks (NAN, FAN) communicating with smart meters. Utilities might also be very much interested in standardization of software subsystems (e.g., middleware-like packages). A first step could be the adoption of software architecture conventions and paradigms (e.g., IEEE FIPA for agent-based systems). It will be challenging to devise an integrated and flexible system that is sufficiently modular, and allows domain experts to concentrate on their specialty, calling on lower level services offered by the ICT system. Applications to be supported include both analytics (to transfer the plethora of data from meters, PMUs, etc., to useful, synthesized information) and complex real-time event processing (to enable optimized control).

To enable the development of such standards, as well as suitable control strategies (e.g., hierarchical or more flat interaction of equal peers), there is a need for testing and validating the various proposals. While limited field trials can be an option to try out (e.g., the overlay approaches suggested earlier), utilities are in critical need of a near real-world environment, with real loads, distribution gear and diverse consumption profiles, to develop, test, and validate their required Smart Grid solutions [61]. While such centers are arising (e.g., the Experimental Power Grid Centre in Singapore [29]), it remains a quite expensive test environment. To foster the development of communication-based architectures, the community would benefit immensely from adequate *simulation tools that incorporate both the power and communication networks in adequate detail*. The first such endeavors often resorted to co-simulation; [36] linked the Open Distribution System Simulator (OpenDSS) with the ns-2 Network Simulator to simulate a deployment of distributed energy resources on a model of an actual distribution circuit (feeder). Similarly, [55] uses a combination of communication network simulator ns-2 and Modelica for the power network. In [58], the authors focus on the communication network, adding abstracted models of power network elements to Omnet++ while resorting to a MatLab model for detailed power network state calculations. Laudable efforts are pursued within the Simulations Workgroup within OpenSG [68] to develop a framework and requirements for modeling and simulation tools and platforms for Smart Grid research. We strongly believe in the development of such a modular framework, allowing studies at various scales in time and space of communication-based power systems, as they evolve to more distributed and hybrid architectures, with control schemes based on increasingly integrated and pervasive information and communications technologies [68].

8.8 Acknowledgments

The authors would like to thank Craig Rodine (OpenSG Users Group, USA) for sharing his views, and in particular his assistance in setting the chapter context in the Introduction.

8.9 Sources

[1] Aggarwal, V., Feldmann, A., Scheideler, C. 2007. "Can ISPS and P2P users cooperate for improved performance?" *SIGCOMM Computer Communication Review* 37, no. 3: 29–40.

[2] Akamai Technologies. www.akamai.com.

[3] Albert, R., Barabasi, A. 2002. "Statistical Mechanics of Complex Networks." *Reviews of Modern Physics* 74: 47.

[4] Andersen, D., Balakrishnan, H., Kaashoek, F., Morris, R. 2001. "Resilient Overlay Networks." *Symposium on Operating Systems Principles*: 131–145.

[5] Androutsellis-Theotokis, S., Spinellis, D. 2004. "A survey of peer-to-peer content distribution technologies." *ACM Computing Surveys* 36, no. 4: 335–371.

[6] Backx, P., Wauters, T., Dhoedt, B., Demeester, P. 2002. "A comparison of peer-to-peer architectures." *Eurescom 2002 Powerful Networks for Profitable Services.*

[7] Bakken, D. E. , Bose, A., Hauser, C. H., Whitehead, D. E., Zweigle, G. C. 2011. "Smart Generation and Transmission With Coherent, Real-Time Data." *Proceedings of the IEEE* 99, no. 6: 928–951.

[8] Banerjee, S., Lee, S., Bhattacharjee, B., Srinivasan, A. 2003. "Resilient multicast using overlays." *SIGMETRICS '03: Proceedings of the 2003 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*: 102–113.

[9] Barolli, L., Xhafa F. 2011. "JXTA-Overlay: A P2P Platform for Distributed, Collaborative, and Ubiquitous Computing." *IEEE Transactions on Industrial Electronics* 58, no 6: 2163–2172.

[10] Baset, S., Schulzrinne, H. 2005. "An analysis of the Skype Peer-to-Peer Internet Telephony Protocol." *Technical Report CUCS-039-04*. Department of Computer Science, Columbia University.

[11] Braden, R., Clark, D., Shenker, S. 1994. "Integrated Services in the Internet Architecture: an Overview – RFC 1633. www.ietf.org/rfc/rfc1633.txt.

[12] Campbell, A. T., De Meer, H. G., Kounavis, M. E., Miki, K., Vicente, J., Villela, D. A. 1999. "The Genesis Kernel: A Virtual Network Operating System for Spawning Network Architectures." *Proceedings of IEEE Second Conference on Open Architectures and Network Programming, 1999.*

[13] Chim, T. W., Yiu, S. M., Hui, L. C., Li, V. O. 2011. "PASS: Privacy-preserving authentication scheme for Smart Grid network." *Proceedings of the 2nd IEEE International Conference on Smart Grid Communications, 2011*: 208–213.

[14] Clark, D., Lehr, B., Bauer, S., Faratin, P., Sami, R., Wroclawski, J. 2006. “Overlay Networks and the Future of the Internet.” *Communications & Strategies* 63, no. 3.

[15] Clarke, I., Sandberg, O., Wiley, B., Hong, T. W. 2000. “Freenet: A Distributed Anonymous Information Storage and Retrieval System.” *Workshop on Design Issues in Anonymity and Unobservability*: 311–320.

[16] Condie, T., Kamvar, S., Garcia-Molina, H. 2004. “Adaptive P2P Topologies.” Technical Report.

[17] Dabek, F., Kaashoek, M. F., Karger, D., Morris, R., Stoica, I. 2001. “Wide-area cooperative storage with CFS.” *Proceedings of the eighteenth ACM symposium on operating systems principles, 2001*: 202–215.

[18] Deconinck, G., Labeeuw, W., Vandael, S., Beitollahi, H., De Craemer, K., Duan, R., Qui, Z., Ramaswamy, P.C., Vande Meerssche, B., Vervenne, I., Belmans, R. 2010. “Communication overlays and agents for dependable smart power grids.” *5th International Conference on Critical Infrastructure, 2010*: 1–7.

[19] Deconinck, G., Vanthournout, K. 2009. "Agora: A semantic overlay network," *International Journal of Critical Infrastructures IJCIS (Inderscience)* 5: 175–195.

[20] Deconinck, G., Vanthournout, K., Beitollahi, H., Qiu Z., Duan, R., Nauwelaers, B., Van Lil, E., Driesen, J., Belmans, R. 2008. “A Robust Semantic Overlay Network for Microgrid Control Applications.” *Architecting Dependable Systems V*: 101–123. Springer.

[21] Deshpande, J. G. Kim, E., Thottan, M. 2011. “Differentiated Services QoS in Smart Grid Communication Networks”, *Bell Labs Technical Journal* 16, no. 3 : 61–82.

[22] De Vleeschauwer, B., De Turck, F., Dhoedt, B., Demeester, P. 2006. “Online management of QoS enabled overlay multicast services.” *IEEE GLOBECOM 2006, the Global Telecommunications Conference*.

[23] De Vleeschauwer, B., De Turck, F., Dhoedt, B., Demeester, P. 2009. “Server placement and path selection for QoS-enabled overlay networks.” *European Transactions on Telecommunications*: 247–263.

[24] Duan, Z., Zhang, Z., Hou, Y. T. 2003. “Service overlay networks: SLAs, QoS, and bandwidth provisioning.” *IEEE/ACM Transactions on Networking* 11, no. 6: 870–883.

[25] Efthymiou, C., Kalogridis, G. 2010. “Smart grid privacy via anonymization of smart metering data.” *Proceedings of the 1st IEEE International Conference on Smart Grid Communications, 2010*: 238–243.

[26] eMule. www.emule-project.net.

[27] Erikson. H. 1994. “Mbone: the multicast backbone.” *Communications of the ACM* 37: 54–60.

[28] Eugster, P. T., Guerraoui, R., Handurukande, S. B., Kouznetsov, P., Kermarrec, A.-M. 2003. "Lightweight Probabilistic Broadcast." *ACM Transanctions on Computer Systems* 21, no. 4: 341–374.

[29] "Experimental Power Grid Centre." A*Star, Singapore. http://energy.a-star.edu.sg/.

[30] Farhangi, H. 2010. "The path of the Smart Grid." *IEEE Power Energy Magazine* 8, no. 1: 18–28.

[31] Forster, F., DeMeer, H. 2004. "Discovery of Web Services with a P2P Network." *Computational Science – ICCS 2004, 4th International Conference.*

[32] Francis, P. 200. "Yoid: Extending the Internet Multicast Architecture." Unrefereed report, 38 pages. April 2, 2000. www.icir.org/yoid/docs/index.html.

[33] Gao, J., Steenkiste, P. 2004. "Design and evaluation of a distributed scalable content discovery system." *IEEE Journal on Selected Areas in Communications* 22, no. 1: 54–56.

[34] Giordano, V., Gangale, F., Fulli, G., Sanchez-Jimenez, M. 2011. "Smart Grid projects in Europe: Lessons learned and current developments." JRC-ENER Report. EU Commission.

[35] Gjermundr, H., Bakken, D., Hauser, C., Bose, A. 2009. "GridStat: A flexible QoS-managed data dissemination framework for the power grids." *IEEE Transactions on Power Delivery* 24, no. 1: 136–143.

[36] Godfrey, T., Mullen, S., Dugan, R. C. , Rodine, C., Griffith, D. W., Golmie, N. 2010. "Modeling Smart Grid applications with co-simulation." *Proceedings of the 1st IEEE International Conference on Smart Grid Communications, 2010*: 291–296.

[37] Hales, D., Arteconi. S. 2006. "SLACER: A Self-Organizing Protocol for Coordination in P2P Networks." *IEEE Intelligent Systems* 22, no. 2.

[38] Hauser, C. H., Bakken, D. E., Dionysiou, I., Karalrd Gjermudød, K., Irava, V. S., Helkey, J., Bose, A. 2008. "Security, Trust, and QoS in Next-Generation Control and Communication for Large Power Systems." *International Journal of Critical Infrastructures* 4(1/2): 3–16.

[39] Hei, X., Liu, Y., Ross, K. W. 2008. "IPTV over P2P streaming networks: the mesh-pull approach." *Communications Magazine* 46, no. 2: 86–92.

[40] *IEEE 1646 Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation*. 2004. IEEE.

[41] *IEEE P2030/D5.0. Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology and Information Technology Operation With the Electric Power System (EPS), and End-Use Applications and Loads*. 2011. IEEE SA Standards Board.

[42] IntelliGrid Project. 2004. *The Integrated Energy and Communication Systems Architecture, Vol. IV: Technical Analysis*. www.epri.com/IntelliGrid/.

[43] Jelasity, M., Montresor, A., Babaoglu, O. 2005. "Gossip-based aggregation in large dynamic networks." *ACM Transactions on Computer Systems* 23: 219–252.

[44] JXTA Community Project. http://java.net/projects/jxta.

[45] Kalogridis, G., Efthymiou, C., Denic, S. Z., Lewis, T. A., Cepeda, R. 2010. "Privacy for smart meters: Towards undetectable appliance load signatures." *Proceedings of the 1st IEEE International Conference on Smart Grid Communications, 2010)*: 232–237.

[46] Khalifa, T., Naik, K., Nayak, A. 2011. "A Survey of Communication Protocols for Automatic Meter Reading Applications." *IEEE Communications Surveys & Tutorials* 13, no. 2.

[47] Khurana, H., Hadley, M., Lu, N., Frincke, D. 2010. "Smart-grid security issues." *IEEE Security and Privacy* 8, no. 1: 81–85.

[48] Kim, H., Kim, Y.-J., Yang, K., Thottan, M. 2011. "Cloud-based Demand Response for Smart Grid: Architecture and Distributed Algorithms." *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm 2011)*: 416–421.

[49] Kim, Y.-J., Kolesnikov, V., Kim, H., Thottan, M. 2011. "SSTP: a Scalable and Secure Transport Protocol for Smart Grid Data Collection." *Proceeds of the IEEE International Conference on Smart Grid Communications (SmartGridComm 2011)*: 173-178.

[50] Kim, Y.-J., Thottan, M., Kolesnikov, V., Lee, W. 2010. "A secure decentralized data-centric information infrastructure for Smart Grid." *IEEE Communications Magazine* 48, no. 11: 58–65.

[51] Lam, H., Fung, G., Lee, W. 2007. "A novel method to construct taxonomy electrical appliances based on load signatures." *IEEE Transactions of the Consumer Electronics Society* 53, no. 2: 653–660.

[52] Li, T., Rekhter, Y. 1998. "A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) – RFC 2430." http://tools.ietf.org/html/rfc2430.

[53] Li, Z., Mohapatra, P. 2004. "Impact of Topology On Overlay Routing Service." *INFOCOM*: 418.

[54] Li, Z., Mohapatra, P. 2004. "QRON: QoS-aware routing in overlay networks." *IEEE Journal on Selected Areas in Communications* 22: 29–40.

[55] Liberatore, V., Al-Hammouri, A. 2011. "Smart grid communication and co-simulation." *Proceeds of IEEE Energytech, 2011*: 1–5.

[56] Liefooghe, P., Goossens, M., Swinnen, A., Haggdorens, B. 2004. *CastGate Technical Report* (October).

[57] Loo, B. T., Condie, T., Hellerstein, J. M., Maniatis, P., Roscoe, T., Stoica, I. 2005. "Implementing Declarative Overlays." *20th ACM Symposium on Operating Systems Principles (SOSP)*.

[58] Mets, K., Verschueren, T., Develder, C., Vandoorn, T., Vandevelde, L. 2011. "Integrated simulation of power and communication networks for Smart Grid applications." *Proceedings of the 16th IEEE International Workshop on Computer-Aided Modeling, Analysis and Design of Communication Links and Networks, 2011*: 61–65.

[59] Peer-to-peer Session Initiation Protocol (P2PSIP). www.p2psip.org.

[60] Pendarakis, D., Shi, S., Verma, D., Waldvogel, M. 2001. "ALMI: An Application Level Multicast Infrastructure." *3rd USNIX Symposium on Internet Technologies and Systems, 2001*: 49–60.

[61] Pipattanasomporn, M., Feroze, H., Rahman, S. 2009. "Multi-agent systems in a distributed Smart Grid: Design and implementation." *Proceedings of the IEEE Power Systems Conference and Exhibition, 2009*: 1–8.

[62] Pouwelse, J. A., Garbacki, P., Wang, J., Bakker, A., Yang, J., Iosup, A., Epema, D. H. J., Reinders, M., van Steen, M., Sips, H. J. 2008. "TRIBLER: a social-based peer-to-peer system." *Concurrency and Computation: Practice & Experience. Special Issue: Recent Advances in Peer-to-Peer Systems and Security* 20, no. 2.

[63] Ripeanu, M., Foster, I., Iamnitchi, A. 2002. "Mapping the Gnutella network: Properties of large-scale peer-to-peer systems and implications for system design." *IEEE Internet Computing Journal* 6.

[64] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E. 2002. "SIP: Session Initiation Protocol – RFC 3261." www.ietf.org/rfc/rfc3261.txt.

[65] Saltzer, J. H., Reed, D. P., Clark, D. D. 1984. "End-To-End Arguments in System Design." *ACM Transactions on Computer Systems* 2, no. 4: 277–288.

[66] Santacana, E., Rackliffe, G., Tang, L., Feng, X. 2010. "Getting smart." *IEEE Power Energy Magazine* 8, no. 2: 41–48.

[67] Schonwalder, J., Fouquet, M., Rodosek, G., Hochstatter, I. 2009. "Future Internet = content + services + management." *IEEE Communications Magazine* 47, no. 7: 27–33.

[68] "SG Simulations." Open Smart Grids Users Group. http://osgug.ucaiug.org/SG_Sim/default.aspx

[69] Smart Grid Special Interest Group. www.sipforum.org/content/view/351/266/.

[70] Stokes, M. 2003. *Gnutella2 specification document - first draft*.

[71] Universal Description Discovery and Integration. www.oasis-open.org/standards#uddiv3.0.2.

[72] Vandoorn, T., Meersman, B., Degroote, L., Renders, B., Vandevelde, L. “A control strategy for islanded microgrids with dc-link voltage control.” *IEEE Transactions on Power Delivery* 26, no. 2: 703–713.

[73] Vasseur, J.-P., Pickavet, M., Demeester, P. 2004. *Network recovery—Protection and Restoration of Optical, SONET- SDH, IP, and MPLS.* D. Clarck, Ed. Morgan Kaufmann Publishers.

[74] Verma, D. C. 2002. *Content Distribution Networks: An Engineering Approach*. John Wiley & Sons.

[75] Wijnants, M., Cornelissen, B., Lamotte, W., De Vleeschauwer, B. 2006. “An Overlay Network Providing Application-Aware Multimedia Services.” *2nd International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications, 2006*.