Wireless Pers Commun (2014) 76:125–147
DOI 10.1007/s11277-014-1682-6

Infrastructure for Intelligent Automation Services in the Smart Grid

Rune Hylsberg Jacobsen · Søren Aagaard Mikkelsen

Published online: 16 March 2014

Abstract The electricity grid is undergoing a radical transformation from a production-driven to a demand-driven energy delivery platform known as the smart grid. The integration of a large amount of renewable and distributed energy resources, together with new patterns of electricity production, accentuates the need for research in information and communication technologies to control bi-directional energy flows. The European FP7 project: "Energy Demand Aware Open Services for Smart Grid Intelligent Automation" is contributing to this research by providing an intelligent infrastructure for service deployment for the smart grid. The project defines a system architecture that provides interoperability between wireless sensors in home area networks connected over the Internet to a service provider function deployed in a cloud infrastructure. A key component in this infrastructure is the Home Energy Controlling Hub that, on the one hand, provides a platform for monitoring and aggregation of electricity consumption data from devices and appliances and, on the other hand, is the link between the deployed intelligent automation services and the home. To ensure openness and simplicity, the proposed infrastructure is based on the representational state transfer style architecture. This is adopted by implementing the emerging ZigBee IP and Smart Energy Profile 2.0 standards that to a wide extend conform with the Internet Protocol suite and state-of-the art web services development.

Keywords Home area network · Smart energy profile · Intelligent automation services · Smart grid

1 Introduction

The electricity industry is in a process of transformation in an effort to support the needs of a highly reliable, efficient, and sustainable society. Today's electricity industry is experiencing an increasing uptake of renewable energy, widespread deployment of smart metering and

R. H. Jacobsen (✉) · S. A. Mikkelsen
Department of Engineering, Aarhus University, Finlandsgade 22, 8200 Aarhus N, Denmark
e-mail: rhj@eng.au.dk

distribution automation, increased availability of information across the system, and new, emerging electrical devices, appliances and controllers.

The smart grid integrates the power infrastructure with an information infrastructure, thereby combining the maturity of the electric grid with the efficiency, connectivity of Information and Communication Technology (ICT). As the power system is upgraded with gradually more ICT, it enables large-scale integration of a greater diversity of technologies and end-user applications and services. As a result the smart grid is evolving towards a highly automated energy production system that uses advanced sensing and actuation technologies, control methods, and communication technologies to monitor and manage the availability and quality of electrical power, the immediate and predicted energy demands, and the status of supporting infrastructures [1].

Home Energy Management Systems (HEMS) have emerged to increase the efficiency of the integration of residential homes with the smart grid [2]. The HEMS enables energy control and monitoring, by providing benefits to both consumers and the Distribution System Operator (DSO). HEMS intelligently monitors and adjusts energy usage by interfacing, intelligent devices, appliances, and smart plugs, thereby providing effective energy and peak load management. Basically, HEMS can offer a platform for service deployment by providing functions as: (1) one-way flow of *information*, displaying energy usage data to end users; (2) an *automation* resulting from the two-way flow of information between a "hub" and home appliances, enabling consumers to set and forget the operation of home appliances and micro-generation; (3) a *control* function that enables third party control of home appliances via pricing or other remote signals made possible by the home automation; and finally (4) a mean to ensure the privacy of the consumer.

Most of today's HEMS rely on short-range, low-power wireless technology such as ZigBee to connect sensors and actuators. Figure 1 shows the integration of the HEMS with the smart grid. The HEMS uses a Home Energy Controlling Hub (HECH) to act as a bridge between the home and the smart grid. The HEMS interfaces the DSO or a third party service provider and embeds the Energy Services Interface (ESI) as well as the interface between the HECH and home appliances. The residential homes are connected to the Electricity Distribution Network (EDN) from where they exchange electricity. IAS are implemented as cloud services and deployed from the cloud over the Internet.

This paper introduces the European FP7 project: "Energy Demand Aware Open Services for Smart Grid Intelligent Automation (SmartHG)". It provides a case study for the use of intelligent infrastructures for a service-oriented deployment of intelligent automation services (IAS) in a smart grid. The paper is organized as follows: Sec. 2 introduces the SmartHG project and the Intelligent Automation Services (IAS) of the project. This section includes protocols needed for the Home Area Network (HAN) to provide connectivity between the HECH and home devices/appliances. Sec. 3 describes the SmartHG Energy Service Interface (ESI) that is needed to allow smart grid applications to interoperate. Finally, Sec. 4 discusses important security and privacy elements of the infrastructure. The paper concludes in Sec. 5.

2 The SmartHG Project

The SmartHG project captures the recent trend in ICT for smart grid and home area networking and delivers an intelligent infrastructure for service deployment based on a service-oriented architecture [3]. The project rests on a set of services that, on one side, takes into account the objectives of residential homes and on the other side meets the need of the DSO. The project will deliver six high-level services for home and grid automation control. The

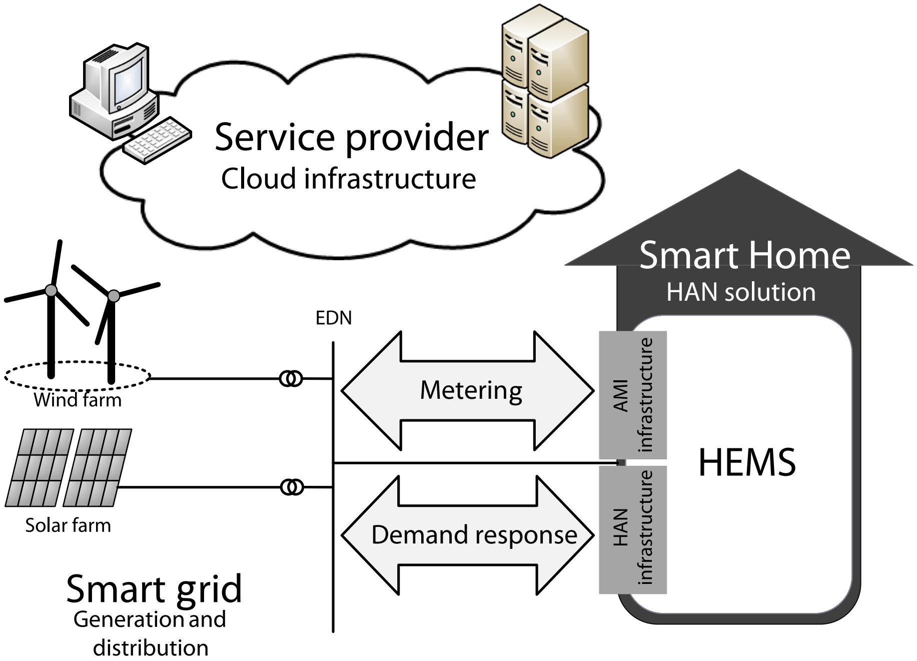


Fig. 1 Smart grid home concept. Basic metering services can be provided over the advanced metering infrastructure (AMI) and demand response is offered over a dedicated HAN

approach is for the consumer to take a *reactive* role in the actuation of a demand response by providing increased awareness of the energy consumption and information of potential benefits such as e.g., energy savings.

Today, demand and supply steering are obtained by proposing a price policy to all users in a given area. However, the two-way (from user to operator and vice versa) communication infrastructure envisioned in the SmartHG project enables the proposal of a personalized price policy to each single residential home user.

2.1 System Overview

The system architecture for the SmartHG project reflects the current ICT trends of delivering services from the cloud based on local settings and information gathered from individual homes [4]. The system must work seamlessly with local and global infrastructures and must deal with security and privacy issues. Therefore, it is necessary to develop services that integrate both systems. Besides the necessity to have services that provide interoperability, it should encourage the use of standard-based solutions that have less overhead and do not require an intermediary between services.

The high-level SmartHG architecture, shown in Fig. 2 has three logical entities: the Residential Homes, the SmartHG Management Platform, and the Intelligent Automation Services (IAS).

The Residential Home represents the demand-side entity that consumes and possible produces energy. Its main component, the HECH, interfaces the HAN and connects to the Smart Home Hardware Devices (SHHD) installed. The HECH has integration mechanisms

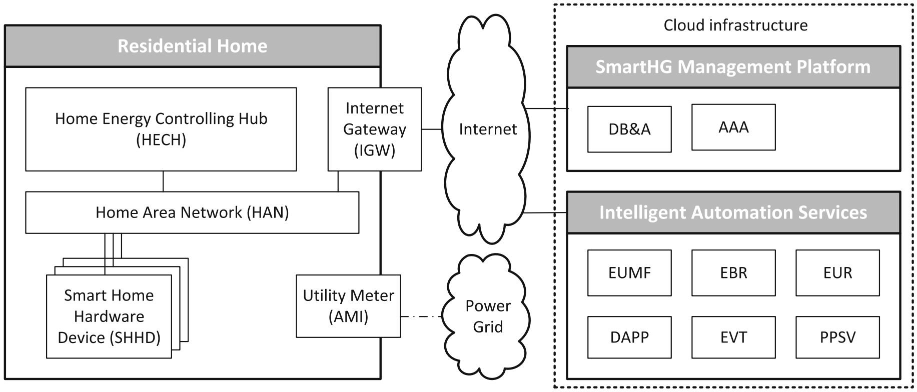


Fig. 2 The SmartHG architecture consists of two main controlling entities; the HECH and the SmartHG Management Platform. The HECH manages the residential home and supports the heterogeneity in the HAN. The SmartHG Management Platform provides consumption data of the consumers and the coordination between the consumers and the Intelligent Automation Services

that enable transparent communication to all SHHD such as sensors and actuators. The information relayed by the HECH is restricted by the privacy policy control such that the consumer is in charge of the distribution of personal data.

The Intelligent Automation Services platform contains services and applications which objectives are to optimize energy usage locally and at the same time support the optimization of EDN operation more globally. The key element in this optimization is the energy demand data from the residential home sent by the HECH over the Internet. It processes near real-time event information from the HECH and have knowledge about the status of each SHHD in the home. Furthermore, it is responsible for the creation of an interoperable communication infrastructure between itself, the residential home, and the IAS platform.

The SmartHG Management Platform is deployed as a cloud service accessible over the Internet. It offers basic services that provide support to high-level services such as installing/upgrading/removing IAS as well as providing basic services for authentication, authorization and accounting (AAA).

The SmartHG architecture is based on the representational state transfer (REST) architectural style and a service-oriented architecture. It assumes the existence of web clients and web servers. The servers are devices that host resources, and the clients are devices that obtain, extend, update, or delete representations of these resources. It is important to note that devices may be both clients and servers at the same time. Clients poll servers to obtain the current state of a resource.

2.2 Energy Demand Aware Services

The SmartHG project will develop cloud services that, by exploiting the energy usage data from residential homes, will provide intelligent automation services to residential home users, i.e., Home Intelligent Automation Services (HIAS) as well as to the DSO in the form of Grid Intelligent Automation Services (GIAS). The rationale is that HIAS will provide benefits to individual consumers by helping them to optimize their energy consumption (local optimization) whereas GIAS will support the DSO in optimizing the EDN management (global optimization).

The goal of Home Intelligent Automation Services (HIAS) is to enable residential homes in saving on their energy bill as well as reducing their overall energy consumption and optimizing their own (in-house) energy production. This will be achieved by developing three basic HIAS that can be used together or in isolation.

- The *Energy Usage Modelling and Forecasting* (EUMF) service focuses on acquiring and predicting a model of the usage and local generation of energy in a residential home. The first step towards intelligent automation of energy usage is to acquire usage patterns of each residential home. This is done by exploiting data coming from sensors, as well as those from the smart appliances deployed in the home. Similarly, patterns of the amount of energy produced by local generators e.g., photovoltaic panels, can be collected and used as the starting point to produce (and dynamically revise) an energy usage/generation model of each home. Such model may then be used to make predictions of the future energy demand/offer of the residential home.
- The *Energy Bill Reduction* (EBR) service focuses on computing energy usage strategies that would minimize the energy bill for a consumer. The EBR HIAS takes as input the energy price policy of the DSO, the energy model and usage preferences of a residential home, as computed and maintained by the HIAS and time constraints on energy tasks (e.g., the latest tolerable time for the laundry to be done). Its goal is to give advices the consumer via a suitable interface, i.e., suggesting when to start the laundry machine, or directly actuate SHHDs (e.g., starting a "smart" laundry machine) so that the overall energy cost is reduced. A key enabler for this service is the price policy offered by the DSO to the consumers.
- The *Energy Usage Reduction* (EUR) service focuses on identifying energy saving opportunities of residential homes by helping home residents to identify new opportunities to reduce the amount of energy consumed. While the EBR HIAS exploits the home energy usage/generation model and user preferences to shift energy demand when it costs less, the presence of a detailed and reliable home energy model permits the development of the EUR HIAS. For example, from the frequency of 'turn-on'/'turn-off' sequences of an air-conditioning device, the EUR HIAS may infer data about the current thermal properties of the house. By comparing this information with the insulation values of typical construction materials the EUR HIAS can identify margins of improvement in the home's thermal insulation and thus, reduction of energy consumption.

Knowledge of the energy usage/generation model of each single home, as learned and collected by the EUMF HIAS, enables a new level of smartness in the smart grid. To bring forward this opportunity, SmartHG develops Grid Intelligent Automation Services (GIAS) that will exploit the data gathered from residential homes to improve EDN management. Such an improvement will translate into lower EDN operations cost for the DSO and better services for the consumer. GIAS is essential in making HIAS e.g., the acquisition of a model of the energy usage/generation of each single home, interesting also for the DSO. Closing such a loop is crucial in order to make residential home energy data acquisition economically feasible. The SmartHG project plans to develop the following GIAS:

- The *Demand-Aware Price Policies* (DAPP) service aims at proposing to consumers individual, yet fair price policies in order to steer the overall energy demand on the EDN e.g., by better load balances. The EDN is subject to various kinds of constraints such as voltage quality and frequency stabilization which need to be kept always satisfied during operation. The key approach to keep the EDN constraints under control is to dynamically steer and shape the electricity demand. In particular, the profile of the electrictiy demand

and supply in particular areas of the EDN can be steered on the basis of the available data. The proposed policy will be close enough to the typical energy usage/generation pattern of the recipient (thus convenient for the user, who is interested in buying and selling energy from/to the DSO at the best prices), still yielding a saving in the EDN operation.

- The *EDN Virtual Tomography* (EVT) service exploits the detailed data about energy consumption and in-house generation collected by the EUMF HIAS to virtually sense the state of nodes of the EDN where no sensors are available. In fact, the lack of a fixed and hierarchical structure for monitoring in most EDNs combined with the high presence of bidirectional flows may lead to a degradation of the reliability of the overall EDN, with higher risk of brownouts. The EVT GIAS will explicitly support the DSO in keeping a close control over the overall state of the EDN, as it will permit to infer voltage, current, and other measures in points of the EDN not directly accessible by sensors.
- The *Price Policy Safety Verification* (PPSV) service is devoted at verifying the safety, with respect to EDN constraints of the demand steering entailed by a given price policy. The price policies proposed by the DSO are the major mechanism to control the demand and offer of energy in the various parts of the EDN. They steer the energy usage profiles of the consumer and allow the DSO to directly actuate smart devices such as local generators, electric vehicles chargers, heat pumps etc. The presence of this control mechanism makes the overall system safety critical. As a consequence, the price policies proposed by the DSO must be designed as to guarantee that the EDN remains in a safe state. The PPSV GIAS is dedicated to such a safety verification.

To make it convenient for a consumer to accept and actually follow an energy usage/generation profile consistent with the proposed price policy and to avoid peaks due to consumers (accidental) synchronization of globally-defined price policies, the SmartHG project will develop a service that computes such policies taking into account both DSO and suitable fairness constraints.

The *Database and Analytics* (DB&A) service is very central in the service hierarchy. DB&A is a support service which stores measurements used to monitor the status of the EDN at various points in the grid. It is collecting and storing data needed by the DSO and by the other GIAS including data about energy consumption and generation profiles at the different end-points of the EDN, also enabling their aggregation. DB&A is also very central in the architecture because it provides the communication path between the HIAS and GIAS. The intelligent automation services communicate by writing entries into the database; in this way the RESTful architecture style is followed.

Another support service is *Authentication, Authorization and Accounting* (AAA). This service is the basis for securing IAS delivery and to support the need for privacy. In addition, the AAA service will offer a platform for registration and maintenance of services of consumers by maintaining a set of consumer accounts.

3 Open Standard Protocols for Intelligent Automation

To foster sustainability of the envisaged approach, it is guaranteed that the software services developed in the SmartHG project can be used as building blocks on which future services can then be made. For this reason, one of the fundamental objectives, that the SmartHG project will pursue, is the usage of open protocols for the foreseen services as well as for the data gathering hubs deployed in residential homes.

3.1 Open Protocols for Home Devices

Protocols for ICT service infrastructures for the energy grid may be grouped into families ranging from supervisory control and data acquisition (SCADA) protocols and its associated IEC standards; protocols emerging from industry forums like the ZigBee and HomePlug® Alliance; to protocols driven by the Internet Engineering Task Force (IETF). A key success factor for the future is the proper selection of a suitable set of protocols to ensure a seamless, secure, and interoperable system for ICT service deployment for the smart grid.

Interoperability issues for the HAN is one of the mechanisms that inhibit the horizontal integration of home automation services across different application domains such as e.g., home entertainment, home security, smart grid services etc. No “one size fits all” technology seems to dominate the energy management solutions for the home networks. The following section identifies and discuss the protocols that need to be defined and deployed to ensure the open and secure communication between home devices and the IAS.

In recent years, it has become clear that inter-networking of smart objects e.g., sensors or actuators in appliances is possible due to advances in low-power electronics and light-weighted communication protocol implementations. These devices and sensors may be used intelligently to provide a basis for IAS. As a consequence, communication technologies for smart buildings and smart home infrastructures can be based on commonly available low-power wireless radios e.g., ZigBee and Z-Wave [5].

Standardization organizations have made high-level specifications for the architecture and the communication, where there is consensus about using IP-based communication. One of the main reasons for adapting the IP-based network is the maturity of the IP standards and the number of applications that already use the technology today [6]. The flexibility IP provides by implementing a layered architecture of open protocol standards, makes it highly suitable for the smart grid.

HEMS deployed today are mostly IPv4-based. These are implemented by either using private IPv4 addresses for sensors and actuators or by relying on MAC layer addressing. While this approach works fine with existing systems, it breaks with the end-to-end design principle of internet engineering, complicates infrastructure and implementation, and opposes an overall goal of achieving seamless interoperability of heterogeneous networks. Because of the lack of globally available IPv4 addresses, a wide-spread deployment of IP-enabled home sensors and smart appliances need to be based on IPv6 with its vast address space.

The SmartHG project will implement and deploy IPv6-compliant inter-networking technologies such as IPv6 over Low-Power Personal Area Networks (6LoWPAN). The IPv6 network layer can cope with heterogeneous networks and provide seamless connectivity between smart meters, smart appliances, as well as other smart objects in the building. It offers a sufficiently large address space for scaling the ICT infrastructure. Subsequently, it is specified to use this infrastructure to collect data coming from smart appliances and meters in near real-time. Given that home gateways may be embedded into the devices, having limited computational resources, it is important for the communication protocols to be light-weight. This poses constraints on the security measures that can be taken. The HAN data and traffic must be kept private and secure with respect to attacks and tampering attempts. The application of proper light-weighted types of encryption must be deployed.

3.1.1 Protocol Specifications

Recent trends in protocol definitions for the smart grid seem to converge towards the use of open protocols defined by the Internet Society. To position these protocols, the IETF has published RFC 6272 that describes a suitable set of internet protocols to be used with the smart grid [7]. This specification may be considered as a super set of suggested protocols without providing configuration details for specific applications for the smart grid.

The "classical" ZigBee, i.e., ZigBee specification version 1 and version 2, provides a network layer to run on top of the IEEE 802.15.4 radio MAC. The protocol stack is an open standard and it is free for vendors to download and implement. The ZigBee network layer (NWK) is not compatible with IP and does not provide support for interconnecting heterogeneous networks. Due to the lack of support for heterogeneous networks the NWK protocol is considered to be less attractive for the SmartHG HAN.

A recent specification from the ZigBee and HomePlug® Alliance provides a selection of protocols for the HAN. The selection has resulted in the ZigBee IP standard [8]. The ZigBee IP standard defines an interoperable stack of IETF-established protocols for use in IEEE 802.15.4 wireless mesh networks [9]. In contrast to RFC 6272, the ZigBee IP standard offers details on the configuration of the open protocols to be used. A key difference between classical ZigBee and ZigBee IP is that the NWK layer has been substituted by IPv6 over low power wireless personal area networks (6LoWPAN).

3.1.2 Low Power Wireless Networks with IEEE 802.15.4 Radios

Many of today's HEMS are typically based on Wireless Personal Area Network (WPAN) technology such as the IEEE 802.15.4-2006 wireless standards [9]. The IEEE 802.15.4 standard specification defines the protocol and interconnection of devices via radio communication in a Personal Area Network (PAN). The standard uses carrier sense multiple access with collision avoidance (CSMA-CA) to access the medium. It supports star as well as peer-to-peer topologies. Typically, these networks are deployed with a PAN coordinator, that implements a general model of communication, which allows it to talk to any other device. The PAN coordinator relays messages between nodes in the PAN. The media access is contention-based which means that devices are allowed to access the radio channel in a distributed fashion using CSMA-CA with a back-off algorithm. However, by using the optional super frame structure, time slots can be allocated by the PAN coordinator to devices with time critical data. Connectivity to higher performance networks is provided through the PAN coordinator. Hence, there is often coincidence between the PAN coordinator and the gateway providing access to the Internet.

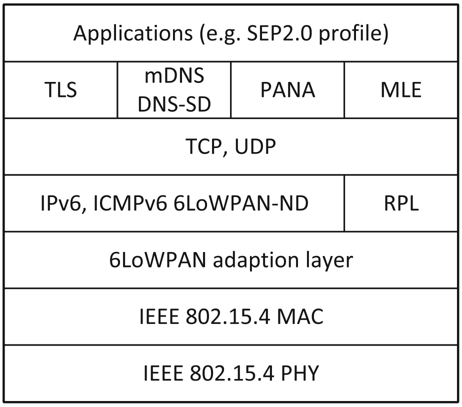
The IEEE 802.15.4 standard was designed specifically for long-lived applications that require the deployment of numerous low-cost nodes. The throughput is limited to a maximum of 250 Kbps and the physical layer packet size length is limited to 127 bytes to ensure reasonably low packet error rates and to adapt to buffering capabilities of constrained devices. The communication range is kept short (tens of meters). IEEE 802.15.4 radios typically operate in the 2.4 GHz frequency band.

The IEEE 802.15.4 standard has been selected by the ZigBee specification to form layer 1 and layer 2 of a ZigBee network [10]. This design choice has been kept in the ZigBee IP specification [8].

3.1.3 ZigBee IP

The MAC layer of IEEE 802.15.4 supports discovery of PAN nodes within radio range and a frame transmissions with a maximum frame size of 127 bytes including MAC header and frame security overhead. ZigBee IP nodes shall be able to support the 64-bit (also called EUI-64 MAC address or extended address) and 16-bit MAC level addressing schemes. Moreover,

Fig. 3 ZigBee IP protocol stack



the MAC supports transmission of frames to sleeping devices using frame buffering and a polling scheme.

Figure 3 shows the protocol stack overview of ZigBee IP. It is intended for use with Smart Energy Profile version 2.0 (SEP 2) described below in Sect. 3.2.2. The key IETF networking standards included in ZigBee IP are: 6LoWPAN adaption layer [11], 6LoWPAN neighbor discovery (6LoWPAN-ND) [12]; IPv6 [13]; TCP [14]; UDP [15], ICMPv6 [16]; and RPL [17]. Higher layer protocols count TLS [18] and PANA [19] for security, multicast DNS (mDNS) [20] and DNS service discovery (DNS-SD) [21] for service discovery and MLE [22] for mesh network maintenance.

3.1.4 Internet Protocol

The success of the Internet can be attributed to the design and wide-spread deployment of the Internet Protocol (IP). The introduction of a global addressing scheme combined with a connectionless datagram delivery service have made IP a superior technology for interconnecting computers across heterogeneous networks. In today's deployment, IP exists in two versions: IPv4 and IPv6. IPv4 has the most wide-spread deployment.

A number of key differences between IPv4 and IPv6 are especially relevant for an efficient transport of IPv6 datagrams over WPANs. IPv6 requires the minimum transmission unit to increase from 576 bytes to 1280 bytes in the recognition of the growth in link bandwidth. To simplify routers and to enhance performance, IPv6 implements fragmentation at the source rather than in intermediate routers. Moreover, IPv6 assumes multicast support as an integral part of the architecture. This increases protocol efficiency and eliminate the need for ad hoc link-layer services for network bootstrapping. The IPv6 neighbor discovery (ND) protocol supports a stateless address autoconfiguration method. It simplifies configuration and management of IPv6 devices by enabling nodes to construct unique addresses and to discover routers and neighbor devices. The implementation of IPv6 ND greatly reduces the management and configuration effort for the HAN.

The SmartHG project will use IPv6 as the open protocol layer for interconnecting devices in the HAN and will provide connectivity to IAS deployed over the Internet. In some part of the HAN, IPv6 must be adapted to the WPAN, whereas in other parts IPv6 can run on top of Ethernet or WiFi.

3.1.5 IPv6/IPv4 Translation

Special support is required to allow IPv4 and IPv6 to interwork in the Internet. Whereas a transition from IPv4 to IPv6 was believed to be necessary a decade ago, it is a growing belief that this transition will occur at such slow pace that IPv4 and IPv6 will need to coexist in the Internet for a very long future [23]. The basic IPv4/IPv6 transition principles and mechanisms are described in [24]. Basically, the mechanisms fall into two categories: *tunneling* and protocol *translation*.

In the *tunneling* approach, IPv6 traffic is encapsulated into IPv4 packets and sent over the Internet. Encapsulation takes place at tunnel endpoints. These endpoints need to be IP hosts or routers that implement a dual IPv4/IPv6 protocol stack. The key drawbacks of this approach are added protocol overhead and the forming of overlay networks.

Alternatively, protocol *translation* between IPv4 and IPv6 can take place in special dual-stack devices. Several different protocol translation mechanisms have been suggested [25]. Basically, a mapping between IPv4 and IPv6 addresses is made in a protocol translation. The approach is somewhat fragile because a sloppy made software application can choose to embed IP addresses as opposed to domain names, and may no longer function through the translation mechanism. In this case, special care is taken to also cope with application data. Another, drawback of protocol translation is the need for assigning additional IP addresses which further enlarge the problem of the lack of global IPv4 addresses.

The SmartHG project will use both the tunneling and the translation method. The tunneling approach shall be used to connect to the IPv6 Internet by using an IPv6 tunnel broker service. IPv4/IPv6 translation will be used in proxy gateways to interconnect proprietary gateways that only support IPv4.

3.1.6 Transmission of IPv6 Packets over IEEE 802.15.4 Networks

With the attachment of IP-enabled low power WPANs, i.e., the so-called LoWPANs, to the Internet, a number of radically different network characteristics come into play as compared to the current Internet [26]. First of all, LoWPANs typically do not have a fixed network infrastructure. Given the size of the network, this demands a self-configuring behavior. Furthermore, the LoWPAN must be able to handle hosts that join/leave the network unexpectedly and frequently. The nodes must be able to relay, switch or route packets received from neighbors in a multi-hop infrastructure to maintain a good connectivity of the network. When the Internet is extended with LoWPANs, islands of wireless embedded devices form stub networks. A stub network is a network where IP packets are sent from (or destined to), but does not act as a transit to other networks. IP packets destined for the stub networks have to transverse a border router [27]. Subsequently, the border routers may act as gateways for the access to devices in the stub network. The border routers share the same network prefix and they are attached to a common backbone link. Figure 4 shows an example of a 6LoWPAN network. In the SmartHG HAN, the HECH will act as border router to a LoWPAN in the home.

Mesh topologies are common for LoWPAN extensions of the Internet. These topologies extend the network coverage, and reduce the cost of infrastructure. In order to achieve a mesh topology, forwarding between nodes is required. This can be done in two distinct ways: by forming a link layer mesh or by IP routing. This negates the assumption that the link is a single broadcast domain on which a core of IP architectural components, such as neighbor discovery and stateless address autoconfiguration, relies upon [28].

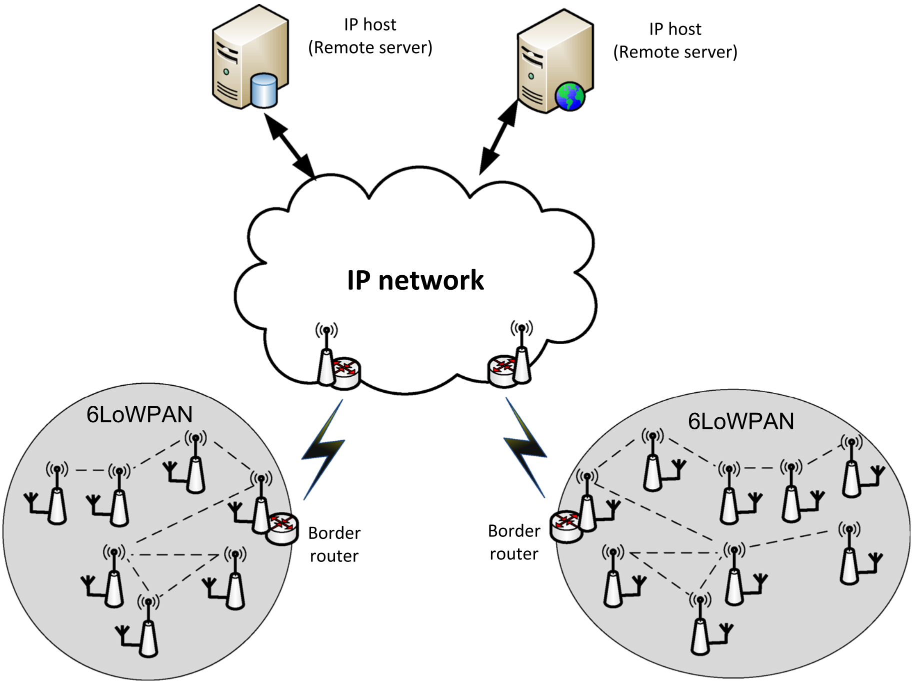


Fig. 4 Example of an IP network with 6LoWPAN stub networks. The border routers act as gateways for the 6LoWPANs. End-to-end connectivity is established between remote servers and the end-devices of the 6LoWPAN

Due to resource constraints and the multi-hop nature of LoWPANs, the support of IPv6 over these networks presents several design challenges [26]. Essentially, IPv6 datagrams are poorly fit for LoWPANs. Low throughput, limited buffering capabilities, and small frame sizes make datagram fragmentation and compression a necessity for efficient operation. By introducing the 6LoWPAN adaption between the networking and the link layer, many design challenges can be circumvented [11]. The main elements in the 6LoWPAN adaptation are *link layer forwarding*, *fragmentation*, and *header compression*.

To support *link layer forwarding* of IPv6 datagrams, the adaptation layer may use link-level addresses for destination end-points of IP hops. Alternatively, the IP stack might realize intra-PAN routing via IP layer forwarding by constructing the IP address of the LoWPAN nodes, in which case each LoWPAN node becomes a single IP hop.

Fragmentation of IPv6 packets into multiple link-level frames is used to accommodate the IPv6 minimum transmission unit size requirement. The fragmentation and assembly is performed in the 6LoWPAN adaptation layer and is transparent for the IP layer.

IPv6 *header compression* is performed by making use of common values in the protocol header redundant. Header fields are omitted from a packet whenever the 6LoWPAN adaptation layer can derive these from assumptions of a shared context such as link-level information carried in the IEEE 802.15.4 frame. In the best case, a UDP/IPv6 header can be compressed from 8+40 bytes down to 7 bytes.

IEEE 802.15.4 devices may construct their unique IPv6 addresses by using either EUI-64 extended addresses or, after an association event, 16-bit addresses that are unique within a

PAN. In the latter case, a PAN ID for a group of physically collocated IEEE 802.15.4 devices is defined.

3.1.7 Multihop Networking

The Mesh Link Establishment (MLE) protocol defines a mechanism for establishing and configuring secure radio links in IEEE 802.15.4 multi-hop networks [22]. MLE operates below the routing layer and allows the dynamic configuration and security protection of radio links. Furthermore, MLE supports the network-wide exchange of radio parameters and the discovery of neighbor devices. In particular, MLE can be used to make the Expected Transmission count (ETX) metric to be operational and provided for the routing layer [29]. This is accomplished by using periodic multicasting over the radio links to estimate the quality of the links.

MLE messages are carried over UDP. The protocol can be used to initialize link-layer security. Consequently, MLE cannot rely on link-layer security itself and have adopted the AES-128-CCM security mechanism from the IEEE 802.15.4 standard [9].

The routing protocol for low power and lossy networks (RPL) is a reactive, distance-vector routing protocol designed for use in resource-constrained networks [27]. The aim of the protocol is to construct routing paths from embedded devices such as sensors to a network sink. RPL constructs a destination-oriented directed acyclic graph (DAG) rooted at the sink of a hierarchical network. The DAG is the central topology upon which routing is performed. Downward routes support point-to-multipoint flows, from the DAG root towards the leaves. Downward routes also support point-to-point flows where point-to-point messages can flow towards a DAG root through an upward route, then away from the DAG root to a destination through a downward route. In the converged state, each router in the WPAN has identified a stable set of parents on a path towards the root of the DAG, as well as a preferred parent. A DAG allows the routing protocol to minimize resource requirements. The state complexity of the protocol is small because nodes only need to maintain routes to upwards nodes, i.e., to its DAG parents.

The DAG optimizes routes from any node to the sink in the network according to an Objective Function (OF). The OF defines how nodes translate one or more metrics and constraints into a value called Rank. The Rank is basically the distance of the node to the backbone network. Furthermore, the OF defines how nodes select their parents. By using the construct of the OF, the RPL protocol itself becomes agnostics to routing metrics and parent decision making criteria.

3.1.8 ZigBee IP Security Support

The security protocol stack of ZigBee IP [8] is illustrated in Fig. 5. In addition to link-layer security supported in the IEEE 802.15.4 standard, it provides security services support for the application layer and will be introduced in the following sections.

The Protocol for Carrying Authentication for Network Access (PANA) [19] is a network-layer transport for Extensible Authentication Protocol (EAP) [30] to enable network access. Essentially, the PANA protocol defines an EAP encapsulation that runs between two IP-enabled nodes. Other EAP transport protocols include Point-to-Point Protocol (PPP) and IEEE 802.1X. The protocol uses the concept of a PANA Client (PaC) and a PANA Authentication Agent (PAA). PANA messages are carried over UDP and the protocol has its own retransmission mechanism for reliable message delivery. A fixed session identifier is maintained throughout a session that is confined to a single network interface.

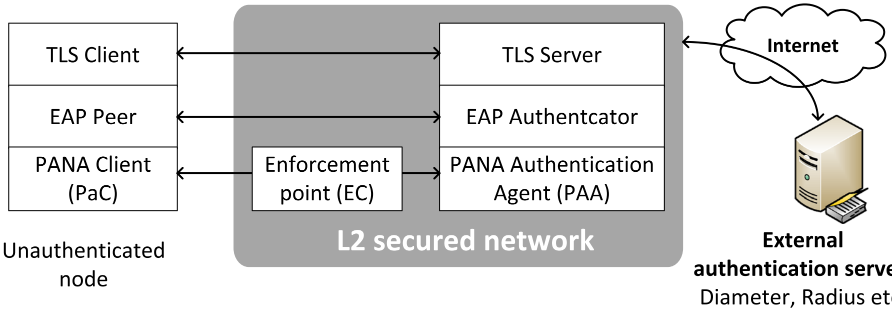


Fig. 5 ZigBee IP security model

EAP is an authentication framework which supports multiple authentication methods [31]. EAP is used to select a specific authentication mechanism, typically after the authenticator requests more information, in order to determine the specific authentication method to be used. Rather than requiring the authenticator to be updated to support each new authentication method, EAP permits the use of a back-end authentication server, which may implement the necessary authentication methods. In this setup, the authenticator is acting as a pass-through for some or all methods and peers. By using PANA, the EAP can be transported over UDP/IP instead of over a layer 2 protocol which is the most typical scenario in today's network.

Securing transactions between clients and servers in a ZigBee IP/SEP 2 network is based on using HTTP over TLS [32] by using TLS version 1.2 [18]. TLS provides a mechanism for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints. The protocol allows client and server applications to communicate securely such that it prevents eavesdropping, tampering, or message forgery. TLS runs on top of TCP. The TLS handshake mechanism provides mutual authentication based on device certificates or self-signed certificates and TLS Records provide encryption and message authentication using the AES-CCM mode of operation. The keys for this symmetric encryption are generated uniquely for each connection and they are based on secrets negotiated by another protocol such as e.g., the TLS Handshake Protocol. Furthermore, the TLS Record Protocol ensures that the connection is reliable by providing message integrity checks that use keyed message authentication codes.

The use of TLS requires that all hosts implementing the server functionality shall use a device certificate whereby the server presents its certificate as part of the TLS handshake. Access control lists allow or deny use of resources based on authentication level and address information. If a client does not have a certificate and the security policy allows, client authentication may be omitted or secondary client authentication may take place after the TLS handshake. Pre-authorization for resources is normally set when the client registers with the host. If the security policy allows, authorization may occur immediately after authentication based on implicit rules to allow a request to complete. This is to allow unregistered access to resources based on security policy.

There are different versions of the TLS communcation for constraind devices. The DTLS is a light-weight implementation that differs from the TLS by using the UDP instead of TCP [33]. The EAP Transport Layer Security (EAP-TLS) encapsulates the EAP concept into the TLS protocol by a simple extension to EAP-TLS authentication [31]. EAP-TLS includes support for certificate-based mutual authentication and key derivation, utilizing the protected cipher-suite negotiation, mutual authentication and key management capabilities of the TLS protocol. The EAP-TLS protocol requires that both user and authentication server have certificates for mutual authentication. While the mechanism is very strong, it requires that the organization, that deploys it, maintain a certificate infrastructure for all of its users. The specification defines a certificate-based mutual authentication and key distribution mechanism.

3.1.9 Restful Application Layer Protocols

RESTful protocols such as HyperText Transfer Protocol (HTTP) and Constrained Application Protocol (CoAP) are application layer protocols that carry application data in accordance with the basic architectural characteristics of the SmartHG project. These protocols may be accompanied with application protocols for providing network services such as e.g., timing, address lookup, and autoconfiguration.

HTTP is a key invention and prime responsible for the popularity of the world wide web. The protocol is defined in "Hypertext Transfer Protocol—HTTP/1.1" specification and it conforms to the REST architectural style. HTTP is a request/response protocol that runs on top of TCP. The protocol uses a set of simple methods such as: GET, POST, PUT, and DELETE to manipulate resources on a web server. Furthermore, HTTP allows the transport of meta-data e.g., content coding and media types that provide the application layer with information useful for rendering of data.

HTTP relies on the concept of Uniform Resource Indicators (URIs) to uniquely identify resources on a web server. When used with TLS the protocol is abbreviated HTTPS.

All resources are self-describing to recognize that URIs, schemas, and resources might change in the future. The generic syntax used for URIs is specified in [34]. A resource-oriented service exposes a URI for every piece of information the client might want to operate on [35]. URIs are transferred in ASCII format between clients and servers and transfers occur with every transaction.

CoAP is a specialized web transfer protocol for use with constrained devices and constrained networks [36]. The protocol targets machine-to-machine interactions and typical implementations result in CoAP devices acting in both client and server roles. A CoAP request is somewhat equivalent to that of HTTP, and is sent by a client to request an action (using a method code) on a resource on a server. The server responds with a response code that may include a resource representation. Unlike HTTP, CoAP deals with these messages interchanges asynchronously over a datagram-oriented transport such as UDP. In addition, the CoAP specification describes how an HTTP/CoAP proxy should be implemented [36].

3.2 The SmartHG Energy Service Interface

In SmartHG, web services will be used to establish interoperable communication between machines, applications and software services. At a higher level, the web is a loosely coupled application-layer architecture, where a key role is played by resources, i.e., server-controlled abstractions made available by software application processes. The state of a resource is kept by the server, which provides caching, proxying, and redirection of requests and responses.

To ensure interoperable applications in the SmartHG, a common data model is needed. One of the main functions of a common data model is that it offers is the ability to define the associations between components in the architecture. Fortunately, much effort has been put into defining a Common Information Model (CIM) for the electricity domain and from this model the Smart Energy Profile version 2.0 (SEP 2) has been derived. The following sections introduces the data models used in SmartHG.

3.2.1 Common Information Model

The Common Information Model (CIM) is an open standard for representing power system components and networks. The model has been developed by the Electric Power Research Institute (EPRI) and documented in the IEC 61970 series and the IEC 61968 series. It is officially adapted by International Electrotechnical Commission (IEC). This standard, which can be used by energy management systems (EMS), mainly specify the interfaces between components, thereby allowing software modules from different vendors, to communicate with each other. IEC 61970 and IEC 61968 specify a CIM for utility data exchange. Together with IEC 62325 and IEC 62351, these standards constitute the core of a secure smart grid. Each of these standards has its own characteristics and supports different tasks within the grid.

IEC 61970 describes information of energy management system and provides a set of instructions to simplify the integration of multi-vendor applications and to simplify exchange of information to systems outside the control centre including transmission, distribution and generation systems that need to exchange real-time data with the control centre. Moreover, the standard series provide adequate interfaces for data exchange across legacy and new systems. The standard series include the generation and transmission parts of the CIM. It represents a power system model exchange as well as other information exchanges, and specifies XML file format standards for information exchange. The CIM base model is given in IEC 61970-301 [37] and its architecture is described by the Unified Modeling Language (UML) standardized by the Object Management Group (www.uml.org). It defines the components of a power system as UML classes and the relationships between them. This gives the base for a common model to describe situations of a power system, independently of any specific proprietary data standard or format, and hence facilitates the interoperability among software applications.

IEC 61968 is a series of standards that have been derived from IEC 61970 with the aim of simplifying inter-application integration and to support distribution management systems. It is intended to support the integration of a utility enterprise that requires connecting different applications that are either legacy or new. IEC 61968 supports applications that require exchange of data on an event-driven basis and is intended to be built with middleware services that broke messages between applications. The interfaces addressed by the standard include message exchange for network operations, operational planning and optimization, records and asset management, network extension planning, customer support, maintenance and construction, and meter reading and control.

IEC 62325 is a series of standards that define energy market models and communications based on CIM. The objective is to evolve standards for electricity market communications. It describes the communication formations of e-business in energy markets and system operations as well as the communication between market operators. Business operation encompasses system applications with interfaces between different market participants in trading, consumption, market services and billing.

The IEC 62351 standard addresses the information security for power system control operations. The goal of this standard is to handle the security of the communication protocols including the IEC 61968 series and others. It specifies the security requirements for power system management and data exchange.

3.2.2 The Smart Energy Profile 2.0

The Smart Energy Profile version 2.0 specification [38] is the result of a joint effort of the ZigBee Alliance and the HomePlug® Alliance. Essentially, SEP 2 is an application layer protocol that conforms with the CIM standard. The SEP 2 application protocol is built on top of the IP stack. It is intended to run on ZigBee IP [8]. SEP 2 is aimed for use with smart grid applications and supports devices including gateways, metering devices, load control devices, etc.

SEP 2 uses the multicast Domain Name System (mDNS) and DNS-Service Discovery (DNS-SD) to discover SEP 2 compliant devices on a local network [21]. Security is ensured by the use of TLS for communications between devices [18]. This ensures that the protocol meets the security needed to protect sensitive consumer information, at the same time ensuring the integrity of smart grid transactions.

SEP 2 is based on a Public Key Infrastructure (PKI) for its certificate management system. A SEP 2 device manufacturer issues RFC 5280 compliant PKI certificates to devices at the time of application installation, i.e., at manufacturing time [39]. These certificates are intended for use during deployment (or redeployment) and on-going operation to authenticate the device to other SEP 2 devices. While native SEP 2 devices are required to understand and process manufacturer PKI certificates, support of the additional certificates is optional and generally targeted at specific classes of devices such as ESI, web portals etc.

The functionality provided by SEP 2 is divided in function sets [38] and summarized in Table 1. In addition, SEP 2 provides a set of common functionality such as for timing, scheduling of events as well as resources and function sets that provide operational information to the end devices of SEP 2 networks.

The SEP 2 specification comes with SEP 2 Application Protocol Specification [38] and all SEP 2 devices will be required to maintain compliance with the SEP 2 XML Schema Definition (XSD) (sep.xsd in [40]), and the SEP 2 WADL specification (sep_wadl.xml in [40]).

3.2.3 RESTful Web Services

The SEP 2 protocol follows a RESTful architecture design style [35]. The RESTful style lists a number of general design principles to be used in an implementation. A few specific ones are important for the application protocol [38]:

- While devices may maintain state, interfaces should be stateless.
- URI structure should be clear but as efficient as possible.
- The number of transactions required to achieve a given function should be minimized.

SEP 2 mandates the use of HTTP [41] and it is built around the core methods: GET, HEAD, PUT, POST, and DELETE [35], with the addition of a light-weight subscription mechanism. Any application protocol that can implement a RESTful command set could likely be used with SEP 2, but HTTP is a required baseline for interoperable SEP 2 implementations. SEP 2 is supporting the Extensible Markup Language (XML) [42] and the Efficient XML Exchange (EXI) [43] message formats. Consequently, content shall be transferred with either one of the content types: “application/sep+xml” or “application/sep-exi” in the HTTP header.

XML describes a class of data objects called XML documents and partially describes the behavior of the computer programs which process them [42]. XML is an application profile that has been designed as a subset of the Standard Generalized Markup Language (SGML) with the purpose of easing implementations and for the interoperability with both SGML and HTML.

EXI is a compact representation of the XML information set that is intended to optimize performance as well as the utilization of computational resources [43]. It is a binary XML format that is not easily read by humans. Compared to XML, EXI reduces bandwidth requirements without jeopardizing the use of other resources such as battery life, code size, processing power, or memory. A number of options for encoding EXI documents have be

Table 1 SEP 2 function set

Function set	Decription
Demand response and load control (DRLC)	The *DLRC function set* provides an interface for Demand Response and Load Control, where client devices are usually simple sensors and actuators or any other devices that support load control. Server devices include devices that implement ESI and HEMS that may be acting as a proxy for upstream DRLC management systems. Servers expose load control events called End Device Controls (EDC) to client devices. All EDC instances expose attributes that allow devices to respond to events that are explicitly targeted at their device type
Metering	The *Metering function set* provides interfaces to exchange metering information such as reading type and meter reading between devices
Pricing	The *Pricing function set* supports application-specific tariffs for devices (e.g., plug-in electrical vehicles, distributed energy resources), and special event-based prices like critical peak price. It has been designed to stand on its own but can be paired with a billing function to provide additional benefit to users
Messaging	The *Metering function set* provides an interface for a text messaging service
Billing	The *Billing function set* consists of several resources that are used to support billing related functions. This relates to accumulating cost of consumption on an end-device and providing estimates of future consumption, or holding historical consumption information. Furthermore, billing offers a mechanism to allow the service provider to push down targets or challenges to encourage curtailment of energy consumption
Prepayment	The *Prepayment function set* defines a mechanism for the conditional delivery of services based upon outstanding credit or debt
Distributed energy resources control	The *Distributed Energy Resources Control function set* is used in specific cases where energy must be provided to and be managed by the grid. In these cases, energy load, area capabilities, costs and transfer of energy timing impact the management of accepting power. Management of the necessary energy is achieved according to the scheduling of energy via requested and accepted energy transfer transactions. This function set provides an interface to control distributed energy resources, e.g., solar inverters, fuel cells, generation units, and battery storage systems. It is supported by the same type of servers as for the DRLC function set
Energy flow reservation	The *Energy Flow Reservation function set* provides an interface for the exchange of energy flow reservation events. Client devices of this function set include plug-in electric vehicles, distributed energy storage devices, and other managed loads that draw large amounts of power. Server devices of this function set include devices supporting the ESI, electric vehicle support equipment, and EMS

defined in the SEP 2 specification and transactions will likely fail if not addressed appropriately by the EXI option header.

Although not supported by the SEP 2 specification, the JavaScript Object Notation (JSON) needs an introduction. JSON is a serialization format for general data structures [44]. It is a more light-weight, but still readable, equivalent to the XML document. JSON is well-suited for transporting serialized data structures rather than hypermedia documents. Like EXI, JSON has a low bandwidth requirement and is suitable for use with constrained devices. Furthermore, binary formats of JSON exists such as BSON (bsonspec.org), BJSON (bjson.org), UBJSON (ubjson.org) and Smile (wiki.fasterxml.com/SmileFormat).

3.2.4 Web Application Description Language

The Web Application Description Language (WADL) is an XML vocabulary used to describe RESTful web services [45]. A WADL file describes the HTTP request one can legitimately make from a service, i.e., which URIs you can visit, what data to those URIs can expect, and what data they may return. A generic client implementation can read a WADL file and can be immediately equipped to utilize the full functionality of the corresponding web services.

The SEP 2 WADL contains the recommended URI structures and use of HTTP methods associated with these objects. The SEP 2 RESTful interface is defined using WADL and SEP 2 devices shall conform to the interface specifications contained in WADL. By implication, all resource representations shall validate the schema [40] within the standardized SEP XML namespace (http://zigbee.org/sep).

3.2.5 SEP 2 XML Schema Definition

The SEP 2 XSD contains the definitions of the SEP 2 resources, attributes, and elements as well as their textual descriptions. A SEP 2 UML model has been utilized in the creation of the SEP 2 XSD.

An XML Schema is a language for expressing constraints about XML documents [46]. The purpose of an XML Schema is to define the legal building blocks of an XML document. Technically, a schema is an abstract collection of metadata, consisting of a set of schema components: chiefly element and attribute declarations and complex and simple type definitions.

The primary reason for defining an XML schema is to formally describe an XML document. However, the resulting schema has a number of other uses that go beyond simple validation such as code generation and the generation of XML file structure documentation. This code allows content of XML documents to be treated as objects within the programming environment.

Figure 6 shows an excerpt of sep_wadl.xml. From an application point of view, the most interesting parts are the definitions of ComplexTypes and related Elements. In the example, the ComplexType $<$ `resource` $>$ is shown with its elements $<$ `doc` $>$ and $<$ `method` $>$. The SEP 2 XML schema defines a number of ComplexTypes including: DeviceCapability, AbstractDevice, DeviceStatus, EndDevice, EndDeviceList, Registration, SelfDevice, Temperature, FunctionSetAssignment, etc. These ComplexTypes and elements are specified in [40].

3.2.6 Service Discovery

SEP 2 specifies a domain name service-based methods for service discovery, resource discovery, and hostname to IP address resolution. In SEP 2, services are defined as application instances uniquely identified by host, port, and a protocol, where protocol in this case is SEP 2 including its underlying transport bindings. DNS-based service discovery (DNS-SD) [21] is a conventional use of existing DNS to discover instances of a given service within a given domain. In SEP 2, DNS-SD is used to describe the location of function sets and resource groups.

A service with a path forms a URI that can be used to locate a resource. A client discovers instances of a given service or resource type by sending a query for a record with the name "$<$ `service` $>$. $<$ `domain` $>$", which returns a set of zero or more service instance names: "$<$ `instance` $>$.$<$ `service` $>$.$<$ `domain` $>$" for the requested service or resource type.

Multicast DNS (mDNS) [20] provides the ability to perform DNS-like queries on the local link in the absence of any conventional unicast DNS server. mDNS uses link-local multicast

```
<application xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:wx="http://zigbee.org/wadlExt" xmlns:sep="http://zigbee.org/sep"
  xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd">
    <doc title="SEP 2.0 Application">SEP 2.0.0</doc>
    <grammars>
      <include href="sep.xsd"/>
    </grammars>
    <resources wx:sampleBase="http://localhost/sep/">
      ...
      <resource id="DemandResponseProgramList" wx:samplePath="/dr">
        <doc title="DemandResponseProgramList">
           List of DemandResponseProgram instances. Devices implementing
           the DemandResponseProgramList resource MAY support multiple
           instances of DemandResponsePrograms.
        </doc>
        <method id="GETDemandResponseProgramList" name="GET" wx:mode="M">
          <request>
            <param name="s" style="query" type="xsd:int">
              <doc>start</doc>
            </param>
            <param name="l" style="query" type="xsd:int">
              <doc>limit</doc>
            </param>
          </request>
          <response>
            <representation mediaType="application/sep+xml"
            element="sep:DemandResponseProgramList"/>
            <representation mediaType="application/sep-exi"
            element="sep:DemandResponseProgramList"/>
          </response>
        </method>
        ...
      </resource>
    </resources>
</application>
```

Fig. 6 Excerpt of sep_wadl.xml. The example shows the schema definitions for the function to retrieve a demand response program list from a server

addressing for requests and either multicast or unicast addressing for responses in support of service discovery. Finally, the Extended Multicast DNS (xmDNS) extends the scope of mDNS beyond the local link through the use of site-local multicast requests and responses. The reachability of this site-local multicast addresses is administratively defined and may span multiple sub-networks.

4 Security and Privacy Considerations

Security and privacy are key challenges for the smart grid and the security architecture needs to be discussed. It seems that there are two schools that meet in the home. On the one side, we have the energy utility companies that come with their standardized security schemes defined in IEC 62351 and wish to protect their assets by enforcing cumbersome security measures. On the other side, the HAN will be equipped with constrained devices such as sensors and actuators that have limited memory and processing power and that even may run on batteries. Currently, it does not seems realistic that these devices run with large protocol overheads and strong cryptographic keys which require advanced computational processing.

When third party businesses enter a rather sensible market as the residential homes, privacy is a critical topic to address. Access to personal data and personal habits are worth money and this should be controlled by the involved persons. On the other hand, the HEMS should also be flexible enough to deliver useful information when third parties require this and when the consumers consent. The control of each device should also be addressed by a service so that there is a seamless access and control without any prior knowledge of communication infrastructure or location of the device. With this capability the consumer will be able to control every device locally or remotely given that the privacy policy allows it. Although the access and control to the home devices are autonomous from the grid perspective, it is important for the grid system to be aware of the state of the system on a global level. It is therefore necessary for the system to comprise a diagnostic service that provides the current status of each residential home without exposing private information.

In the SmartHG project, the storage of consumer-specific data such as the energy consumption and generation profiles of single homes is handled by the DB&A service. Although it provides substantial benefits for the consumer and is crucial for the GIAS, it raises important privacy concerns as well as data access issues.

The SmartHG project will provide consumers with a flexible level of privacy and security, by employing suitable data access policies, where consumers may, for example, autonomously decide which of their data can be accessed by which GIAS, for which purposes, and at which level of granularity. As an example, a consumer might allow access to his/her detailed energy usage profile to some GIAS, but only aggregate/accumulated data to others. Consumers might also decide whether to give the various GIAS full information about their identity, e.g., for direct billing, or to exploit various forms of anonymization. For example, consumers might give to a GIAS only an identity-masking ID and/or limited details about the geographical region with the DSO being the only entity able to derive their true identity.

The overall approach envisioned to handle privacy and security is, in a sense, similar to that employed in current social networks such as e.g., Facebook, where the users can keep under control which applications have access to their private data, to which extent, and for how long.

5 Conclusions

The SmartHG project takes a service-oriented approach to the deployment of intelligent automation services. These services are used to support the smart grid by enabling functions such as status monitoring and peak load shifting driven by DSO price policies as well as energy usage and energy bill reductions. It relies on an Home Energy Management System (HEMS) where energy awareness is created from data collected from sensor installed in residential homes. The HEMS of individual consumers report data to a centralized, but scalable database and analytics (DB&A) service upon which Intelligent Automation Services (IAS) on a higher level can be deployed. These services are implemented as cloud services accessible over the Internet.

The Home Energy Controlling Hub (HECH) is central to bridge the residential HEMS with the IAS deployed in the cloud. The HECH implements open protocols to ensure seamless connectivity to Home Area Network (HAN) devices while providing security and privacy for the consumers. The SmartHG project is based on the RESTful design style leaning towards the SEP 2 specification. To ensure interoperability, the SmartHG project rests on a set of open protocols with the majority coming from the IETF and the ZigBee Alliance.

The work described in this paper represents parts of the specification of SmartHG. The project was started in the fall 2012 and is scheduled to run for 3 years.

Acknowledgments The research leading to these results has received funding from the European Union Seventh Framework programme (FP7/2007-2013) under *Grant Agreement* N° 317761.

References

1. Moslehi, K., & Kumar, R. (2010). A reliability perspective of the smart grid. *IEEE Transactions on Smart Grid*, *1*(1), 57–64.
2. Kailas, A., Cecchi, V., & Mukherjee, A. (2013). *Chapter 2—A survey of contemporary technologies for smart home energy management. Handbook of green information and communication systems* (pp. 35–56). New York: Academic Press.
3. Papazoglou, M. P. (2003). Service-oriented computing: Concepts, characteristics and directions. In *2003 Proceedings of the fourth international conference on Web information, systems engineering* (pp. 3–12).
4. Rusitschka, S., Eger, K., & Gerdes, C. (2010). Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain. In *2010 first IEEE international conference on smart grid, communications* (pp. 483–488).
5. Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, *48*(6), 92–101.
6. Sauter, T., & Lobashov, M. (2011). End-to-end communication architecture for smart grids. *IEEE Transactions on Industrial Electronics*, *58*(4), 1218–1228.
7. Baker, F., & Meyer, D. (June 2011). *Internet protocols for the smart grid*. Internet Society, RFC 6272.
8. *Zigbee ip specification*. Technical report, ZigBee Alliance, 2013.
9. Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans), 2006. IEEE Std 802.15.4-2006.
10. *Zigbee specification (version 2)*. Technical Report Document 053474r17, ZigBee Alliance, January 17 2008.
11. Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (Sept. 2007). *Transmission of ipv6 packets over ieee 802.15.4 networks*. Internet Society, RFC 4944.
12. Shelby, Z., Chakrabarti, S., Nordmark, E., & Bormann, C. (Nov. 2012). *Neighbor discovery optimization for ipv6 over low-power wireless personal area networks (6lowpans)*. Internet Society, RFC 6775.
13. Islam, S., & Grégoire, J.-C. (2010). Network edge intelligence for the emerging next-generation internet. *Future Internet*, *2*(4), 603–623.
14. Postel, J. (Aug. 1980). *User datagram protocol*. Internet Society, RFC 768.
15. Postel, J. (Sept. 1981). *Transmission control protocol*. Internet Society, RFC 793.
16. Conta, A., Deering, S., & Gupta, M. (March 2006). *Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification*. Internet Society, RFC 4443.
17. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., et al. (2012). *Rpl: Ipv6 routing protocol for low-power and lossy networks*. Internet Society, RFC 6550.
18. Dierks, T., & Rescorla, E. (Aug. 2008). *The transport layer security (tls) protocol version 1.2*. Internet Society, RFC 5246.
19. Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., & Yegin, A. (May 2008). *Protocol for carrying authentication for network access (pana)*. Internet Society, RFC 5191.
20. Cheshire, S., & Krochmal, M. (Feb. 2013). *Multicast dns*. Internet Society, RFC 6762.
21. Cheshire, S., & Krochmal, M. (Feb. 2013). *Dns-based service discovery*. Internet Society, RFC 6763.
22. Kelsey, R. K. (2013). *Mesh link establishment*. Internet Society, draft-kelsey-interea-mesh-link-establishment-05.
23. Huston, G., & Michaelson, G. (May 2008). Measuring ipv6 deployment. In *RIPE 56 meeting May 2008*, Retrieved 2013-06-10.
24. Nordmark, E., & Gilligan, R. (Oct. 2005). *Basic transition mechanisms for ipv6 hosts and routers*. Internet Society, RFC 4213.
25. Mackay, M., Edwards, C., Dunmore, M., Chown, T., & Carvalho, G. (2003). A scenario-based review of ipv6 transition tools. *IEEE Internet Computing*, *7*(3), 27.
26. Jacobsen, R., Toftegaard, T. S., & Kjærgaard, J. K. (2011). *IP connected low power wireless personal area networks in the future internet* (pp. 191–213). Technologies and protocols for future internet design: Reinventing the Web. IGI Global.
27. Hui, J., & Vasseur, J. P. (March 2012). *The routing protocol for low-power and lossy networks (rpl) option for carrying rpl information in data-plane datagrams*. Internet Society, RFC 6553.

28. Hui, J. W., & Culler, D. E. (2010). Ipv6 in low-power wireless networks. *Proceedings of the IEEE*, *98*(11), 1865–1878.
29. Vasseur, J. P., Kim, M., Pister, K., Dejean, N., & Barthel, D. (March 2012). *Routing metrics used for path calculation in low-power and lossy networks*. Internet Society, RFC 6551.
30. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (June 2004). *Extensible authentication protocol (eap)*. Internet Society, RFC 3748.
31. Simon, D., Aboba, B., & Hurst, R. (March 2008). *The eap-tls authentication protocol*. Internet Society, RFC 5216.
32. Rescorla, E. (May 2000). *Http over tls*. Internet Society, RFC 2818.
33. Rescorla, E., & Modadugu, N. (Jan. 2012). *Datagram transport layer security version 1.2*. Internet Society, RFC 6347.
34. Berners-Lee, T., Fielding, R., & Masinter, L. (Jan. 2005). *Uniform resource identifier (uri): Generic syntax*. Internet Society, RFC 3986.
35. Richardson, L., & Ruby, S. (2007). *Restful web services* (1st ed). Sebastopol: O'Reilly.
36. Shelby, Z., Hartke, K., Bormann, C., & Frank, B. (April 2013). *Constrained application protocol (coap)*. Internet Society, draft-ietf-core-coap-15.
37. *Energy management system application program interface (ems-api)—part 301: Common information model (cim) base*. Standard IEC61970-301:2013, International Electrotechnical Commission (IEC), 2013.
38. *Smart energy profile 2 application protocol standard*. Technical Report Document 13-0200-00, ZigBee Alliance, 2013.
39. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (May 2008). *Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile*. Internet Society, RFC 5280.
40. *Smart energy profile 2.0 uml model*, November 2008. ZigBee Alliance, Document 13-0201.
41. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., et al. (June 1999). *Hypertext transfer protocol—http/1.1*, Internet Society, RFC 2616.
42. *Extensible markup language (xml) 1.0* (5th ed.). Technical report, World Wide Web Consortium (W3C), November 2008.
43. *Efficient xml interchange (exi) format 1.0*. Technical report, World Wide Web Consortium (W3C), March 2011.
44. Crockford, D. (July 2006). *The application/json media type for javascript object notation (json)*. Internet Society, RFC 4627.
45. *Web application description language*. Technical report, World Wide Web Consortium (W3C), August 2009.
46. *W3c xml schema definition language*. Technical report, World Wide Web Consortium (W3C), April 5 2012.

Rune Hylsberg Jacobsen received his M.Sc. degree (1995) and Ph.D. degree (1997) from Aarhus University in Denmark based on research in ultrafast optoelectronics and laser physics. He is currently Associate Professor and Group Leader of the Communications Systems Group in the Electronics and Computer Engineering Section at the Department of Engineering, Aarhus University. His main research interests include communication for the smart energy grid, Internet of Things, wireless IP networking, and embedded systems development. His professional career includes several years of professional experience in the telecommunication and IT industry where he has assumed responsibilities in R & D systems engineering and international leadership and management from companies as Tieto, L.M. Ericsson and the Danish telecommunication operator TDC. In addition, he is actively involved in European Research and Technology Development (RTD) projects under the 7th framework programme.

Søren Aagaard Mikkelsen received his B.Eng. (2010) degree in Electrical Engineering and his M.Sc. degree (2012) in Information and Communication Technology from Aarhus University, Denmark. He is currently a Ph.D. student within Communication Technology at Aarhus University. His research explores the communication aspects of the future Smart Grid services, especially concerning the privacy and security sides of the communication. Other interests includes digital signal processing and embedded systems.