EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
Research Article EAI.EU

Towards a Security Enabled and SOA-based QoS (for the Smart Grid) Architecture

C. Chrysoulas[1,*] and N. Pitropakis[1]

[1] Computer Science and Informatics Department, School of Engineering, London South Bank University

Abstract

QoS and Security features are playing an important role in modern network architecures. Dynamic selection of services and by extension of service providers are vital in today's liberalized market of energy. On the other hand it is equally important for Service Providers to spot the one QoS Module that offers the best QoS level in a given cost. Type of service, response time, availability and cost, consist a basic set of attributes that should be taken into consideration when building a concrete Grid network. In the proposed QoS architecture Prosumers request services based on the aforementioned set of attributes. The Prosumer requests the service through the QoS Module. It is then the QoS Module that seeks the Service Provider that best fits the needs of the client. The aforementioned approach is well supplemented with an in depth analysis on existing authentication and authorization protocols. The authors believe that QoS and security can work in parallel without adding extra burden in the Smart Grid infrastructure. This is feasible by building an in advance system for placing, scheduling, and assigning of the requests for energy consumption or production, thus decongesting the traffic in the whole network.

Keywords: Authentication, Authorization, QoS, Security, Service Oriented Architecture, Smart Grid.

Received on 3 September 2017, accepted on 6 December 2017, published on 10 January 2018

doi: 10.4108/_____

1. Introduction

In a constantly growing and demanding market of energy environment, there arises the need for a Quality of Service (QoS) mechanism to properly support the constraints that are imposed by the consumers of energy, without neglecting the importance of keeping the balance of energy flow in the network in an as stable as possible level.

In order to properly achieve this goal, an in advance way of placing, scheduling, and assigning the requests for energy consumption (or even for energy production) should be considered. A mechanism with respect to attributes like: type of service to be served, response time, availability, cost and probably throughput should be developed and adopted in order to smoothly pass from the classic energy grid to this new more intelligently build Smart Grid era.

In the proposed approach, we try to enforce the Service Oriented Architecture Approach (SOA) to the Smart Grid field. The idea was born by noticing that in the Smart Grid field the whole action is initiated by two main actors, namely the Consumer (in our case the Prosumer/User) and the Provider (in our case the Aggregator) of energy (the service). We tried to get the best of what the promising SOA field has to offer in order that different Providers to be able to independently create their services and seamlessly "feed" the Consumers. This approach is worth adapting to the Smart Grid environment.

To efficiently deliver energy resources in the smart grid, an energy resource management strategy needs to be developed to balance the energy demand and supply. Developing effective energy resource management schemes is challenging due to numerous fluctuations the entities on both the demand and supply sides experiencing. For example, on the supply side, fluctuations could come from distributed renewable energy resources due to solar irradiance, wind speed, etc. On the demand side, numerous effects, including natural disasters, plug-in vehicles, personal habits of using

*Corresponding author. Email: chrysouc@lsbu.ac.uk

energy, weather and temperature, etc., could make it difficult to predict energy usage. In this paper, we develop techniques to effectively manage energy resources and usage in order to provide the needed stability to the grid. Particularly, to balance energy demand and supply, we develop a SOA-based QoS architecture to effectively tackle with the needed amount of energy generation, based on the demand over time.

Security and privacy are two of the most important challenges faced by the future smart grid. These issues include: (i) lack of mutual authentication between communicated entities; (ii) risk of various cyber-attacks; (iii) unauthorized access to the resources; and (iv) revealing of device's and network's private information to the communicating entity. The requirements of the Smart Grid network are different from that of the traditional information network, since the specific network deals mostly with confidential information. That is the reason, confidentiality has been prioritized as first, the integrity comes as second, and the availability of information is last. On the other hand, the Smart Grid is primarily responsible for the availability of information, as well as the integrity protection of the message, and then the data confidentiality and privacy [37].

Before allowing any entity to have an access over a network and its associated resources, it is required to authenticate the entity, which may be a device or a user, and then verify the authorization and control policy based on the entity's identity. Authentication verifies the user's identity while the authorization verifies whether the user has valid permissions to access the requested resource. The modern power grid makes use of supervisory control and data acquisition (SCADA) systems with communication protocols. Unfortunately, protocols used in these systems are often vulnerable to a variety of possible attacks (man-in-the-middle attacks, replay attacks, etc) due to the diversity of the attack surface. In the aforementioned, the cryptographic keys used in various devices of the system can be compromised [38]. When connecting a SCADA system to other communication networks (e.g., Internet) what is significantly increased are security and privacy threats [39]. This is one of the major challenges in many countries around the globe [40]. A lot of researchers, actively work building secure and efficient authentication protocols in order to resolve the various communication and security/privacy issues that (co)-exist in the SCADA [41, 42], home Smart Grid environment [43], security management and the Smart Grid operation [44], and message delivery in the Smart Grid [45].

Since various modules and entities receive data input from different other modules and send data output to several modules and entities, secure integration in the Smart Grid network is strongly required. Thus, maintaining data integrity and secure integrated communication among various entities and control modules are necessary. By data integrity we are referring to actions needed for maintaining accuracy and consistency of the data in the database or when transmitted over the network, while secure integrated communication refers to a reliable real-time information exchange within the system. Data integrity can be maintained by using either hash functions, such as SHA1, SHA256, etc., in which variable length input is converted into a fixed length hash code, or by the message authentication code (MAC) functions, such as cipher-based message authentication code (CMAC), hash-based message authentication code (HMAC), one-time MAC, etc., where variable length input with a secret key is mapped to a fixed length MAC code. MAC functions provide data integrity as well as authenticity of the message.

The security and performance objectives for developing a secure and efficient authentication protocol with secure network environment in the Smart Grid network end-to-end at power distribution among various entities, such as users, devices, control centre, utility provider, etc., are listed as follows: (i) Low execution and protocol delay; (ii) Low computational and storage cost; (iii) Low communication and computation overhead; (iv) Resistance to attacks and failures; (v) Trust among Smart Grid entities; (vi) Buffer management; and (vii) Confidentiality and privacy.

The rest of the paper is structured as follows: Section II provides a related literature review on QoS and Security, while Section III gives a detailed presentation of the proposed architecture. Finally, Section IV draws the conclusions, and outlines future work.

2. Related work on QoS and Security

2.1. Related work in QoS

SOA is a way of developing software in the form of interoperable services. The promise that the service-oriented development brings to the IT world stems from providing a common programming interface, through which any application can be accessed [1]. A service can be defined as a discrete unit of functionality that is made available through a service contract [2]. The service contract specifies all interactions between the service consumer and service provider and includes: i) Service interface; ii) Interface documents; iii) Service policies; iv) Quality of service (QoS); and v) Performance.

One of the main differences between a service and other software constructs (such as components or objects) is that a service is explicitly managed. The QoS and performance are managed through a service level agreement (SLA). In addition, the entire service life cycle is managed — from design, to deployment, to enhancements, to maintenance. SOAs can easily support QoS features and behavior by putting their characteristics in the WSDL description of a requested or provided service. Since SOAs message exchange is based on XML, we only need to flourish a bit the description in order to make it possible.

Normally the need for code and systems re-use is the driving force for adopting SOAs [3] instead of using highly specialized building blocks, focusing on a certain application. A service must hide its internal logic. A service should be loosely coupled, with no predefined connections, but with clearly defined inputs and outputs.

QoS in Grid computing was studied in GARA [5]. In GARA approach, the separation of resource reservation and

actual allocation is proposed for supporting critical requests. Studies of Ran [6] and Tian [7] concentrated on extending the first one the UDDI registry and the second one extended the WSDL files in order to bridge the gap between the Web Service layer and the network layer. To our knowledge both approaches lack implementation and validation reports.

Numerous approaches for providing QoS support in middleware based models, and specifically message oriented middleware models can be found in the bibliography. The Quartz [8] approach needs a large dataset (meaning large number of attributes) in order to provide adequate QoS support amongst different application areas. In [9] the QoS negotiation is in advance takes place by communicating a QoS contract amongst the involved parties. Our approach is in position to also send alternative offers to the Prosumers.

Cucinota et al. [10] presented a SOA approach that allows negotiation of the individuals QoS characteristics. In this way any unwanted interference amongst different services can be avoided. In [11], a negotiation architecture was developed where a QoS Manager detects any possible QoS violations, communicates with the resource manager and starts a new negotiation among the interested parts. Our model is proposing the most fitted to the Prosumer's needs QoS offer based on mining techniques and by processing the outcome with the help of machine learning algorithms.

Current research in service oriented systems is aiming to the efficient and automated provision of managed services which particularly during runtime are subject to dynamic and adaptive change processes, as described in the overview article of Papazoglou et al. [15]. The service management not only has to cover the installation, first configuration and monitoring of services but also adaptation, re-configuration and life-cycle management in order to support self-configuration, self-adaptation, and self-healing, in order to properly establish the need for service versioning and dependence management.

When the focus comes to the actual implementation, managing dynamically adaptive service systems implies that the various elements of the service implementations can suitably and efficiently be managed at runtime. Based on this perspective, many authors propose combinations of service oriented architectures with software component based implementation approaches. Chrysoulas et al. [16] reports on the FlexiNET project which applies a special Grid-oriented component model in order to master dynamic service deployment by means of component management. The efficiency and the changeability of software component based service system implementations can rise substantially, if the software component structure is a real refinement of the service structure supporting additional opportunities for component reuse. As a consequence, however, more rich dependency relations arise since each software component may depend on certain versions of other ones. Kon et al. [17] report on the relevant dependence problems and their implications for the reliability of complex distributed software systems. They propose the utilization of component configurators which maintain and manage lists of dependency hooks and client dependency references. Chen [18] directly addresses the dynamic reconfiguration by component replacement, identifies the relevant static and dynamic dependencies and proposes procedures for the monitoring, analysis and reconfiguration of component structures.

Another aspect that should be taken into consideration is the messages exchanging is smart grids. The dominant standards are the (i) Data Distribution Service framework (DDS) [19]; (ii) Extensible Messaging and Presence Protocol (XMPP) [20]; and (iii) RabbitMQ [21]. After carefully analyzed the aforementioned frame-works we reached to the conclusion that the QoS capabilities of XMPP are limited and are mostly supported by extensions to the protocol. DDS targets distributed real-time systems and therefore it is capable of addressing very complex distributed applications, where QoS requirements have to be guaranteed. RabbitMQ is used for high performance distributed system applications, and it is an open cloud messaging platform for real-time on a global scale and is mostly focused on high performance and not on predictability. It is therefore evident to conclude that DDS is the most suitable candidate for smart grid applications which come with high QoS requirements.

The challenges associated with the forecasting and demand response associated with energy usage were also discussed in [23]. Energy usage forecasting can be categorized into short-term, medium-term, and long-term forecasting. Hong et al. [24] adopted a multiple linear regression mechanism for conducting short-term forecasting, which provides an interpretability of the behavior of the electricity usage in the service territory. A semi-parametric additive model proposed by Fan et al. in [25] used a regression mechanism and investigated the nonlinear relationships between energy usage data and variables in the short-term time period. In addition, a human-machine construct intelligence framework was proposed in [26] to determine the horizon year load for a long term load forecasting. Machine learning methods such as SVM and neural networks have been used in carrying out forecasting [27-34]. For example, Shi et al. [28] developed a SVM-based model for one-day-ahead power output forecasting using the characteristics of weather classification. Research has been conducted in predicting energy consumption for smart homes. In [35], a method for predicting energy usage using data collected from CASAS Smart Environment System is introduced. People's activities, overall movement in the home, and frequency of sensor data events are used to predict energy usage.

2.2. Related work on Security

Authentication and authorization are mandatory to create an access control mechanism, by which users are granted access and certain privileges to systems, resources or information. It is strongly required in the Smart Grid system as various users with different roles access billions of devices in the network. Generally speaking, there are several types of

access control mechanisms: (i) Discretionary Access Control (DAC); (ii) Mandatory Access Control (MAC); (iii) Identity Based Access Control (iBAC); (iv) Role-Based Access Control (RBAC); and (v) attribute-based access control (ABAC). Authentication is the process of proving an identity to a given system, including users, applications, and devices [40]. For information exchange in the Smart Grid network, involved entities must be bi-directionally authenticated. Mutual authentications in the distributed Smart Grid network can be categorized as follows: (i) Device-to-device [46]; (ii) Device-to-network [47]; and (iii) User-to-network/device [48].

Authentication protocols

In this subsection, we discuss the challenges and desired objectives of authentication protocols regarding the Smart Grid network, and the existing solutions with their strong and weak points towards meeting these objectives.

There are some standardized protocols that exist in the literature for the Smart Grid, which support the authentication process, such as the Device Language Message Specification/COmpanion Specification for Energy Metering (DLMS/COSEM) for the advanced metering infrastructure network and OpenADR for the demand response program. DLMS is an application layer communication protocol, while COSEM is a data model. The above combined provide an interface model for metering applications belonging to IEC 62056 standards, such as electricity [48]. Three authentication procedures are used by DLMS/COSEM: (i) no security (public access with no identity verification); (ii) low level security authentication (server identifies client by password); and (iii) high level security authentication (mutual identification) with exchange challenges. DLMS/COSEM specifies its own security services (authentication and confidentiality), based on symmetric key encryption, which is not necessarily an advantage. For example, if smart meters combine their measured data with digital signatures, the meters would then need asymmetric keys that can be used in secure sockets layer/transport layer security (SSL/TLS). TLS/SSL is something that DLMS/COSEM does not allow.

In order to provide support for asymmetric encryption, the European committee for electro-technical standardization relays in CENELEC TC-13 [49]. Similarly in demand response, OpenADR, a standard development effort supports authentication based on public key cryptography with exchange of certificates [50]. OpenADR maintains a hierarchy of certified authorities, thus requiring a Public Key Infrastructure (PKI) in order to use a three-tier PKI technology, which eventually leads in a high cost.

Other authentication protocols also exist, such as remote authentication dial-in user service (RADIUS) and diameter protocols for the 2G, 3G, and 4G cellular networks. RADIUS is used to provide remote user authentication and accounting in 2G, 3G, and 4G networks, and WLAN interworking and Wi-Fi offload situations [51]. RADIUS comes with centralized services and maintains a central database. The smart grid requires decentralized solutions since a single-point failure can massively affect the centralized system. Another drawback is that RADIUS has poor scalability and uses the User Datagram Protocol (UDP), which does not provide reliable data transfer, thus making it not suitable for the smart grid where the availability of information is crucial. On the other hand, the diameter protocol is an authentication, authorization, and accounting protocol used in networking, which supports Transmission Control Protocol (TCP) instead of UDP. Its drawback is that does not provide transition support and application level congestion control [52]. Diameter implementation supports peer authentication between communication endpoints using a pre-shared key. Consequently, this brings up key management issues and is not suitable for large systems, such as the smart grid. Another important aspect is that RADIUS and diameter protocols do not directly protect against Denial-of-Service (DoS) attacks carried out by flooding the target equipment.

A secure and efficient buffer management may be required at the aggregators in the Smart Grid network, which are responsible for receiving a large volume of information from the various smart meters, and at the memory stack of controlling devices in the SCADA system to prevent buffer overflow-based DoS attacks. Confidentiality is strongly required along with the privacy preservation of the information. In the Smart Grids network, there is the need to adequately hide the identity and other relevant information of the devices from the other entities. For example, a compromised aggregator may breach the privacy of the Smart Grid and can harm the user by tracing its pattern and energy consumption details. Similarly, some personal information, such as consumed units in every time slot, need to be encrypted over the network when providing it to an untrusted entity, such as an Aggregator.

Moreover, the performance of the system is important for satisfying the system requirements as well as supporting a huge number of devices. The evaluation metrics comprise of communication and computation overheads generated by the protocol, execution time of the protocol, delay at intermediate entities, and message transmission time. A solution is scalable, if it can support the authentication for a huge number of devices and can be further extended if required, with reasonable execution time and low overheads. Timing accuracy in the Smart Grid varies from few microseconds to few seconds depending upon different communication scenarios among various entities. In power communication networks, such as Smart Grid, reliability, security, and real-time message delivery have higher priorities than providing high throughput. Therefore, latency requirement is much more important in smart grid system [53]. The communication latency needed for the transmission system protection is in the order of a few milliseconds [54] and authentication time varies up to few seconds [55]. Furthermore, the computation complexity of various functions used in the protocol should be as low as possible to be scalable.

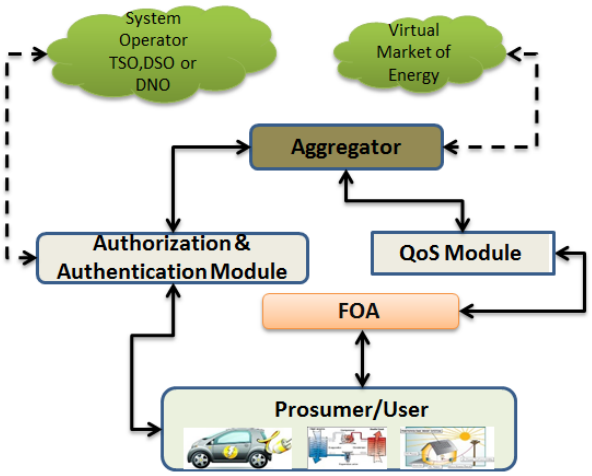

Figure 1. Proposed QoS and Security Enabled Smart Grid Architecture

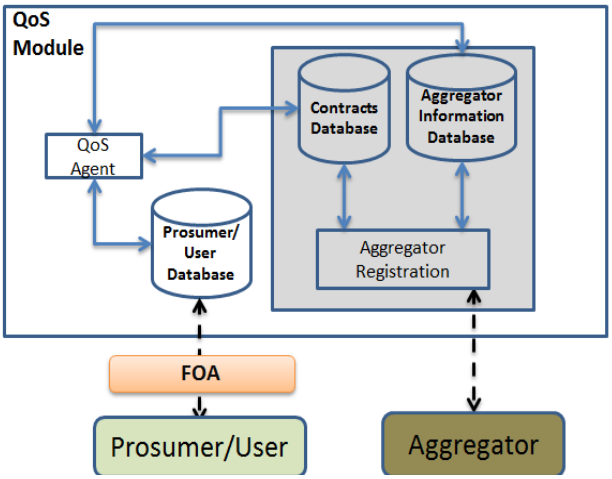

Figure 2. Proposed QoS Smart Grid Architecture

Authorization protocols

There are many access control mechanisms. Jung et al. [56] proposed a SOA based mechanism as a way to provide data infrastructure capabilities on the exchanged information such as customer energy feedback, billing and invoicing of variable tariffs, demand side management, and efficient charging of Electrical Vehicles in the Smart Grid. What is not discussed is possible system overheads. Ryba et al. [57] proposed an authorization as a service architecture for the Smart Grid, while Zhang and Chen in [58] proposed a data-centric access control for the Smart Grid services. Various challenges in defining and enforcing consistent authorization policies are described by Lakshminarayanan [59], but the work fails to describe the implementation part and other important aspects (overheads, execution time, etc.). Cheung et al. [60] presented a new model that extends the network access control from a single security domain to multiple domains for interconnected micro grids. What is unclear is how the policy would be effective for a large network like the Smart Grid. A RBAC model-based access control mechanism is extended for the Smart Grids by Rosic et al. [61] considering the regional division and a concept of areas of responsibility for providing an efficient and consistent policy with a greater level of granularity. However, the RBAC based model may significantly increase complexity. A multi-authority access control with efficient attribute revocation (MAAC-AR) scheme for the Smart Grid by Liu et al. [62] achieves fine-grained access control, collusion resistance, privacy preservation, and secure attribute revocation. However, this scheme generates a large storage overhead. Vaidya et al. [63] present a lightweight and efficient security solution for substation automation system in order to provide a multi-factor authentication and attribute-based authorization by deploying public key certificates, and zero-knowledge protocol-based server-aided verification.

As in detail discussed in this section, authorization is important for supporting secure communication among various entities of the Smart Grid. National Institute of Standards and Technology (NIST) also suggested a distinct need for a lightweight, secure, and efficient AA protocol to mitigate intrusion and Distributed DoS (DDoS) attacks targeting resource-intense AA mechanisms [40]. In the view of large network systems, such as smart grid, a decentralized access control scheme is recommended in order to reduce the overall cost of adding and deleting entities in the system. ABAC is preferred over the user-based and the RBAC when the system is defined with large attributes or the user role is computed dynamically. There are researchers [64, 65] that presented attribute-based decentralized access control scheme, but they do not justify resistance against security attacks or generate large overhead.

3. Proposed Architecture

Security is a critical and complex part of a system like the one proposed. The Authentication and Authorization (AA) Module is responsible for the Authentication and Authorization of the Prosumers/Users and the Aggregators in the system (Fig. 1). The AA module receives the Prosumer Authentication and Authorization request. This module authenticates, and authorizes the Prosumer by obtaining the Prosumer's and Aggregator's profile from the System Operator. The System Operator can be a Transmission System Operator (TSO), a Distribution System Operator (DSO), or a Network System Operator (DNO), i.e. an entity with whom the Prosumer or the Aggregator has a contract with. The possible candidates to serve that need were in depth analyzed in Section II.

The QoS part architecture presented in the [36] consists of the following components: The Aggregator [4], the

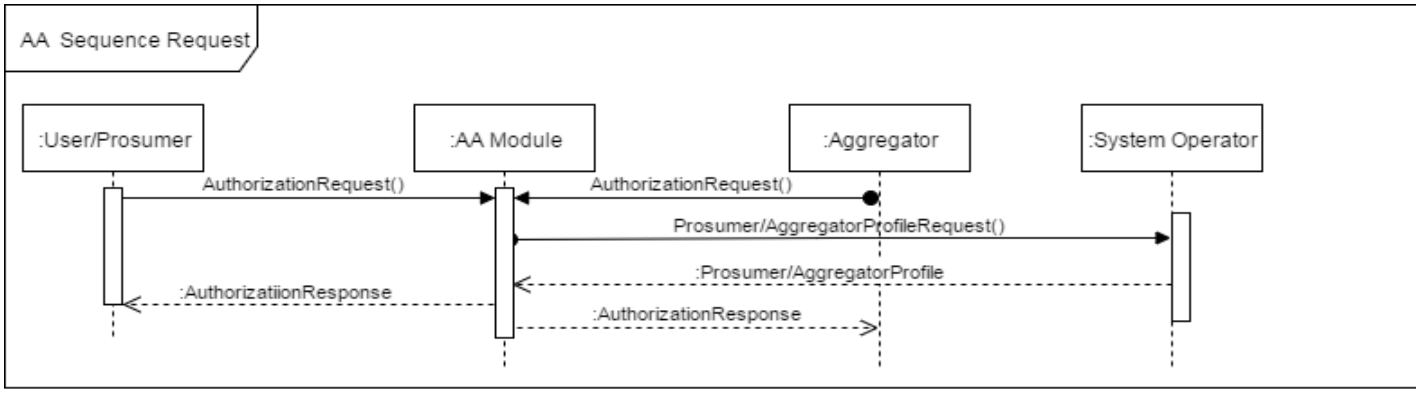

Figure 3. AA Module Interactions

Aggregator Agent (AggA), the Prosumer/User [4], the Flex-Offer Agent (FOA) [4], the QoS Agent, the Aggregator Registration, and databases: to store information regarding the Prosumers/Users, the Contracts (closed, served, etc.), and information regarding the available Aggregators and their characteristics. See Fig. 2.

The Prosumers/Users send their micro flex-offers to the Aggregator, through the FOA and QoS Module. A micro flex-offer states the possibility of a Prosumer/User to consume a certain amount of energy and the time interval during which it has the flexibility to schedule that consumption. There is also the possibility the flex-offer to be generated by the Flex-Offer Agent or by a Flex-Offer Agent that resides on the Aggregator's side, but we will not consider these two options in the present work.

The Aggregators are capable of joining several micro flex-offers into larger macro flex-offers, which are then placed on the electricity market. The energy market will answer with bids to buy and sell energy at given times. Aggregators receive and respond to the bids which allocate energy consumption periods to the macro flex-offers. After, they disaggregate macro flex-offer responses and send an answer to the Prosumers/Users which specify the periods of time to consume the required energy amount from the grid at a lower cost. It is the QoS Module that has the responsibility to find the best matching between the Prosumer's request for a service and the Aggregator that best covers its needs, in terms of response time, availability, and cost. More information can be found in [36].

3.1. Sub-components' interactions

Fig. 3 presents the interactions between the Prosumers/Users and Aggregators with the AA Module, the Systems Operators and the Virtual Market of Energy. After the AA phase the available Aggregators register themselves to the QoS Module, specifically to the Aggregators Information Database, providing information like type of provided services, response time and cost models. The Prosumer asks for a service, which in our case is a need for energy consumption. This type of information is named micro flex-offer. It is then the responsibility of the QoS Module to perform all the needed steps in order to spot the Aggregator that best serves the needs of the Prosumer. Fig. 4 presents the interactions between the Prosumer, the QoS Module and the Aggregator. The list of interactions for the whole systems is the one that follows:

1. Aggregators and Users/Prosumers initiate their AA request through the AA Module.
2. The AA Module contacts the System Operator asking for the Aggregators profile.
3. The System Operator replies with the profile (if exists) and the AA Module comparing the profile from the System Operator with the one from the User/Prosumer – Aggregator authenticates and authorizes it or not.
4. Aggregators register themselves (with their id), and their services (type of services, response time, cost models, and number of Prosumers/Users each can serve) with the QoS Module.
5. A Prosumer/User initiates the sequence of steps, by sending to the QoS Module a QoS request (pointing out the requested service type, amount of needed energy, cost constraints, time flexibility).
6. The QoS Module identifies the Aggregator that best fits the needs of the Prosumer/User. The QoS Module creates a token that includes information like the id of the Aggregator, a session id, the service id, expiration date and time for the offer.
7. If the Prosumer accepts the offer, the QoS Module saves it in the Contract database. The Prosumer only needs the created token to request the service in the given time.
8. The Prosumer makes a service request to the Aggregator using the created token.
9. The Aggregator creates the macro flex-offer and places a bid to the Virtual Market of Energy. The market answers back with a schedule.
10. The Aggregator sends the Schedule to the Prosumer/User, through the Flex-Offer Agent.

11. The Prosumer consumes the service and reports back to the Aggregator the power consumption.

4. Conclusion

In this paper we presented an outline for a Quality of Service architecture targeting the Smart Grid world. All the involving parts were in detail described and documented. QoS attributes like: type of service to be served, response time, availability, and cost where taken into consideration while forming the proposed architecture. Another equally important step is handling the different ways that a flex-offer can be generated and come up with an as common as possible approach. In this paper we considered the flex-offer to be created by the Flex-Offer Agent that is connected to the Prosumer/User. Other identified formal cases are the generation of the flex-offer on the Aggregator, by using power measurement data available on the cloud, and the flex-offer to be initiated by the Prosumer/User, through a User Interface provided by the Flex-Offer Agent. We also presented an in-depth literature review/analysis on the work done till now on the authentication and authorization field and presented how an AA approach can be applied to demand/supply Smart grid architecture.

Future work should include a full implementation of the proposed approach which should also be supplemented by a machine learning part. The machine learning part should be in position to extract useful information, like identifying common patterns amongst multiple users/prosumers. Common patterns for instance in electricity usage in terms of time and amount. In this way the market of energy will be in position to better regulate its production thus leading to a more stable and economically sustainable power grid. In the case of Smart Grids there is no real battle between Security and QoS since the authors argue that the QoS constrains can be satisfied by enforcing an in advance provisioning for the energy consumption and/or production, thus allowing the security part to have more real-time characteristics. This part is also now a reality and will be also presented in a future update.

References

[1] E. Newcomer, G. Lomow, Understanding SOA with Web Services, ISBN-10: 0321180860, ISBN-13: 9780321180865, Publisher: Addison-Wesley Professional, Copyright: 2005.

[2] M. Rosen, B. Lublinsky, T.K. Smith, J.M. Balcer, Applied SOA: Service-Oriented Artchitecture and Design Strategies. John Wiley & Sons; Pub. Date: June 16, 2008 , Print ISBN: 978-0-470-22365-9; Web ISBN: 0-470223-65-0, 2008.

[3] E. Thomas, SOA Design Patterns. Prentice Hall PTR, ISBN: 0136135161, 2009.

[4] L.L. Ferreira, L. Siksnys, P. Pedersen, P. Stluka, C. Chrysoulas, T. Guilly, M. Albano, A. Skou, C. Teixeira, T. Pedersen, "Arrowhead compliant virtual market of energy," in Emerging Technology and Factory Automation (ETFA), 2014 IEEE, Sept 2014, pp. 1–8, 2014.

[5] I. Foster, C. Kesselman, C. Lee, R. Lindell, K. Nahrstedt, A. Roy, "A distributed resource management architecture that supports advance reservations and coallocation," in: Proc. Intl. Workshop Quality of Service 1999, UCL, 1–4 June, London, 1999, pp. 27–36, 1999.

[6] S. Ran, "A model for web services discovery with QoS," ACM SIGEcom Exchanges 4 (1) 1–10, 2003.

[7] M. Tian, A. Gramm, T. Naumowicz, H. Ritter, J. Schiller, "A concept for QoS integration in web services," in: Fourth Intl. Conf.Web Information Systems Engineering Workshops, WISEW'03, Roma, Italy, December 2003, pp. 149–155, 2003.

[8] F. Siqueira, V. Cahill, "Quartz: A QoS architecture for open systems," in: The 20th Intl. Conf. Distributed Computing Systems, ICDCS 2000, 10–13 April, Taipei, Taiwan, 2000, pp. 197–204, 2000.

[9] D.L. Tien, O. Villin, C. Bac, "Resource managers for QoS in CORBA," in: Second IEEE International Symp. Object-Oriented Real-Time Distributed Computing, 2–5 May, Saint-Malo, France, 1999, pp. 213–222, 1999.

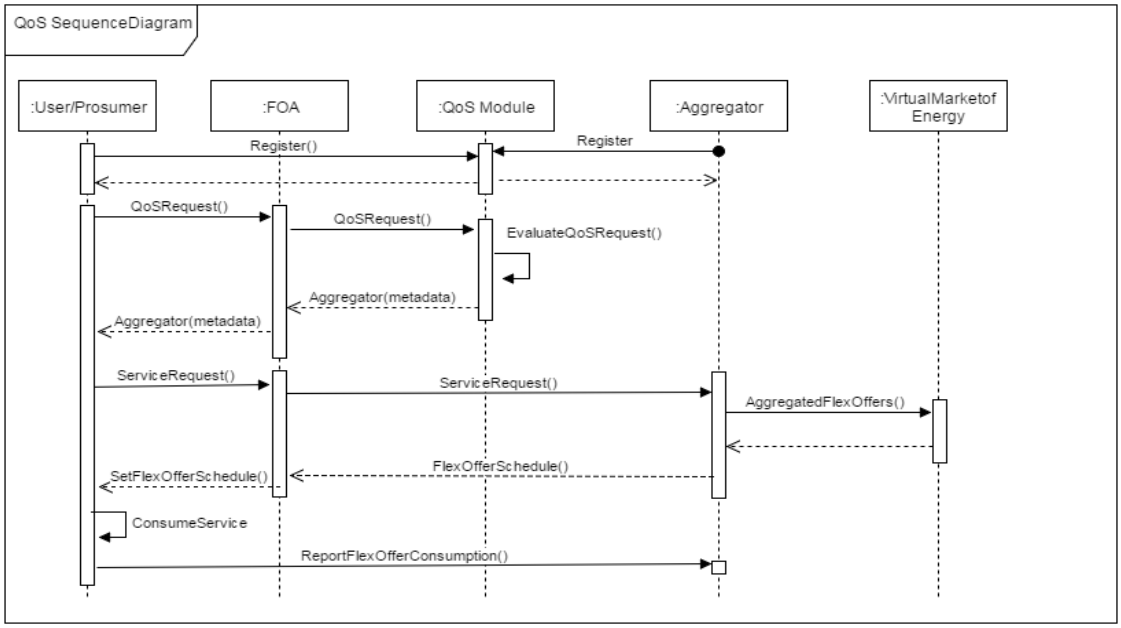

Figure 4. QoS Module Interactions

[10] T. Cucinotta, A. Mancina, G. Anastasi, G. Lipari, L. Mangeruca, R. Checcozzo, F. Rusinà, A real-time service-oriented architecture for industrial automation, IEEE Trans. Ind. Informat., vol. 5, no. 3, pp. 267-277, 2009.
[11] C. Cavanaugh, L.R. Welch, B. Shirazi, E. Huh, S. Anwar, "Quality of service negotiation for distributed, dynamic real-time systems," in: IPDPS Workshop on Bio-Inspired Solutions to Parallel Processing Problems, BioSP3, 15 April, Fort Lauderdale, FL, 2002, pp. 757–765, 2002.
[12] R. Agrawal, R. Srikant, "Fast algorithms for mining association rules," in: Proc. 20th Int. Conf. Very Large Data Bases, VLDB, 1994, pp. 487–499, 1994.
[13] The Arrowhead project: http://www.arrowhead.eu/ [accessed April 2017]
[14] H. Li, Y. Wang, D. Zhang, M. Zhang, and E. Chang, "PFP: Parallel FP-Growth for Query Recommendation," RecSys 2008, Proceedings of the 2008 ACM Conference on Recommender Systems, pp. 107-114, 2008.
[15] M. P. Papazoglou, P. Traverso, S. Dustdar, F. Leymann, "Service oriented computing: State of the art and research challenges", Computer, no. 11, pp. 38–45, 2007.
[16] C. Chrysoulas, G. Kostopoulos, E. Haleplidis, R. Haas, S. Denazis, O. Koufopavlou, "A decision making framework for dynamic service deployment", in Proc. 15th IST Mobile & Wireless Communications Summit, Mykonos, Greece, volume 3, 2006.
[17] F. Kon, R. H. Campbell, Dependence management in component-based distributed systems, IEEE concurrency, no. 1, pp. 26–36, 2000.
[18] X. Chen, "Dependence management for dynamic reconfiguration of component-based distributed systems", in IEEE International Conference on Automated Software Engineering. Proceedings. ASE 2002. 17th, pp. 279–284, 2002.
[19] Object Management Group, Inc. (OMG): Data Distribution Service for Real-Time Systems Specification, Version 1.1, formal/05-12-04, December 2005.
[20] P. Saint-Andre, K. Smith, R. Tronc, "XMPP: The Definitive Guide", O'Reilly, 2009.
[21] J. Videla, J.W. Williams, "RabbitMQ in Action: Distributed Messaging for Everyone", MEAP Edition, Manning Early Access Program, 2011.
[22] Fuseki: serving RDF data over HTTP. https://jena.apache.org/documentation/serving_data/, 2016.
[23] P. Luh, L. Michel, P. Frieland, C. Guan, and Y. Wang, "Load forecasting and demand response". In Proceedings of IEEE Power and Energy Society General Meeting, pages 1–3, 2010.
[24] T. Hong, M. Gui, M. Baran, and H. Willis, "Modeling and forecasting hourly electric load by multiple linear regression with interactions". In Proceedings of IEEE Power and Energy Society General Meeting, pages 1–8, 2010.
[25] S. Fan and R. J. Hyndman, Short-term load forecasting based on a semi-parametric additive model. IEEE Transactions on Power Systems, 27(1):134–141, 2012.
[26] T. Hong, S. Hisiang, and L. Xu, "Human-machine co-construct intelligence on horizon year load in long term spatial load forecasting". In Proceedings of IEEE Power and Energy Society General Meeting, pages 1–6, 2009.
[27] Z. A. Bashir and M. E. El-Hawary, Applying wavelets to short-term load forecasting using pso-based neural networks. IEEE Transactions on Power Systems, 24(1):20–27, 2009.
[28] J. Shi, W.-J. Lee, Y. Liu, and Y. Yang, Forecasting power output of photovoltaic systems based on weather classification and support vector machines. IEEE Transactions on Industry Applications, 48(3):1064–1069, 2012.
[29] Z. Yun, Z. Quan, and S. Caixin, Rbf neural network and anfis-based short-term load forecasting approach in real-time price environment. IEEE Transactions on Power Systems, 23(3):853–858, 2008.
[30] Y. Wang, Q. Xia, and C. Kang, Secondary forecasting based on deviation analysis for short-term load forecasting. IEEE Transcation On Power Systems, 26(2):500–507, 2011.
[31] M. Afshin, A. Sadeghian, and K. Raahemifar, "On efficient tuning of ls-svm hyper-parameters in short-term load forecasting: A comparative study". In Proceedings of IEEE Power Engineering Society General Meeting, pages 1–6, 2007.
[32] W. Li and P. Choudhury, Probabilistic planning of transmission systems: Why, how and an actual example. In Proceedings of IEEE Power and Energy Society General Meeting Conversion and Delivery of Electrical Energy in the 21st Century, pages 1–8, 2008.
[33] T. Hong, P. Wang, A. Pahwa, M. Gui, and S. M. Hsiang, "Cost of temperature history data uncertainties in short term electric load forecasting". In Proceedings of International Conference on Probabilistic Methods Applied to Power Systems, pages 212–217, 2010.
[34] P. Pinson, C. Chevallier, and G. N. Kariniotakis, Trading wind generation from short-term probabilistic forecasts of wind power. IEEE Transactions on Power Systems, 22(3):1148–1156, 2007.
[35] C. Chen, B. Das, and D. J. Cook,"Energy prediction based on resident's activity," in Proceedings of the International workshop on Knowledge Discovery from Sensor Data, 2010.
[36] C. Chrysoulas, and M. Fasli, "A service oriented QoS architecture targeting the smart grid world & machine learning aspects". IEEE International Multidisciplinary Conference on Computer and Energy Science (SpliTech), pp. 1-6, 2016.
[37] Guidelines for Smart Grid Cyber Security. Available online: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628 [accessed April 2017].
[38] Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. Available online: http://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf [accessed April 2017].
[39] G.N. Ericsson, Cyber security and power system communication—Essential parts of a smart grid Infrastructure. IEEE Trans. Power Deliv., 25, 1501–1507, 2010.
[40] Forging a Path toward a Digital Grid Global Perspectives on Smart Grid Opportunities. Available online: https://www.accenture.com/se-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Forging-a-Path-toward-a-Digital-Grid_Global-Perspectives-on-Smart-Grid-Opportunities.pdf [accessed December 2017].
[41] R.E. Mahan, J.R. Burnette, J.D. Fluckiger, C.A. Goranson, S.L. Clements, H. Kirkham, C. Tews, Secure Data Transfer Guidance for Industrial Control and SCADA Systems; Technical Report for Pacific Northwest National Laboratory: Richland, WA, USA, 2011.
[42] C.R. Taylor, C.A. Shue, N.R. Paul, "A Deployable SCADA Authentication Technique for Modern Power Grids". In Proceedings of the IEEE International Energy Conference, Dubrovnik, Croatia, 13–16 May 2014; pp. 696–702, 2014.
[43] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, "Network Security Management and Authentication of Actions for Smart Grids Operations". In Proceedings of the IEEE Canada Electrical Power Conference, Montreal, QC, Canada, 25–26 October 2007, pp. 31–36, 2007.
[44] A. Hamlyn, H. Cheung, T. Mander, W. Lin, Y. Cungang, R. Cheung, "Computer Network Security Management and Authentication of Smart Grids Operations". In Proceedings of the IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008, pp. 1–7, 2008.
[45] X. Lu, W. Wang, Z. Lu, and J. Mat, "From Security to Vulnerability: Data Authentication Undermines Message Delivery in Smart Grid". In Proceedings of the Military Communications Conference, Baltimore, MD, USA, 7–10 November 2011; pp. 1183–1188, 2011.
[46] S. Lee, J. Bong, S. Shin, Y. Shin, "A Security Mechanism of Smart Grid AMI Network through Smart Device Mutual Authentication". In Proceedings of the International Conference on Information Networking (ICOIN), Phuket, Thailand, 10–12 February 2014; pp. 592–595, 2014.
[47] A.J. Paverd, A.P. Martin, Hardware Security for Device Authentication in the Smart Grid. In Smart Grid Security Cuellar, J., Ed.; Springer: Berlin/Heidelberg, Germany, pp. 72–84, 2012.
[48] IEC 62056-6-2:2017 Electricity metering data exchange—The DLMS/COSEM suite—Part 6-2: COSEM interface classes. Available online: https://webstore.iec.ch/publication/34317 [accessed December 2017].
[49] S. Feuerhahn, M. Zillgith, C. Wittwer, C. Wietfeld, "Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850

for smart metering applications". In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 410–415.
[50] OpenADR and Cyber Security. Available online: http://www.openadr.org/cyber-security [accessed April 2017].
[51] Remote Authentication Dial in User Service—RADIUS, Developing Solutions. Available online: https://www.developingsolutions.com/ products/radius [accessed December 2017].
[52] A. Hosia, Comparison between RADIUS and Diameter, 2003. Available online: http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/11.pdf [accessed December 2017].
[53] W. Wang, Z. Lu, Cyber Security in the Smart Grid: Survey and Challenges. Comput. Netw. 2013, 57, 1344–1371.
[54] A. Aggarwal, S. Kunta, P.K. Verma, "A Proposed Communications Infrastructure for the Smart Grid". In Proceedings of the IEEE Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–5.
[55] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Available online: http://www.nist.gov/ public_affairs/releases/upload/smartgrid_interoperability_final.pdf [accessed December 2017].
[56] M. Jung, T. Hofer, S. Dobelt, G. Kienesberger, F. Judex, W. Kastner, "Access Control for a Smart Grid SOA". In Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 10–12 December 2012; pp. 281–287.
[57] G. Ryba, M. Jung, W. Kastner, "Authorization as a Service in Smart Grids: Evaluating the PaaS Paradigm for XACML Policy Decision Points". In Proceedings of the 18th IEEE Conference on Emerging Technologies & Factory Automation (ETFA), Cagliari, Italy, 10–13 September 2013; pp. 1–4.
[58] Y. Zhang, J.L. Chen, "Data-Centric Access Control with Confidentiality for Collaborating Smart Grid Services Based on Publish/Subscribe Paradigm". In Proceedings of the 33rd IEEE International Conference on Distributed Computing Systems Workshops, Philadelphia, PA, USA, 8–11 July 2013; pp. 45–50.
[59] S. Lakshminarayanan, "Authentication and Authorization for Smart Grid Application Interfaces". In Proceedings of the IEEE/PES Power Systems Conference and Exposition (PSCE), Phoenix, AZ, USA, 20–23 March 2011; pp. 1–5.
[60] H. Cheung, A. Hamlyn, T. Mander, C. Yang, R. Cheung, "Strategy and Role-Based Model of Security Access Control for Smart Grids Computer Networks". In Proceedings of the IEEE Canada Electrical Power Conference, Montreal, QC, Canada, 25–26 October 2007; pp. 423–428.
[61] D. Rosic, U. Novak, S. Vukmirovic, "Role-Based Access Control Model Supporting Regional Division in Smart Grid System". In Proceedings of the 5th International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, Spain, 5–7 June 2013; pp. 197–201, 2013.
[62] D. Liu, H. Li, Y. Yang, H. Yang, "Achieving Multi-Authority Access Control with Efficient Attribute Revocation in Smart Grid". In Proceedings of the IEEE ICC-Communication and Information Systems Security Symposium, Sydney, Australia, 10–14 June 2014; pp. 634–639.
[63] B. Vaidya, D. Makrakis, H.T. Mouftah, Authentication and authorization mechanisms for substation automation in smart grid network. IEEE Netw. 2013, 27, 5–11.
[64] S. Ruj, A. Nayak, A decentralized security framework for data aggregation and access control in smart grids. IEEE Trans. Smart Grid 2013, 4, 196–205.
[65] S.S. Yeo, S.J. Kim, D.E. Cho, Dynamic access control model for security client services in smart grid. Int. J. Distrib. Sensor Netw. 2014, 2014, doi:10.1155/2014/181760.
[66] N. Saxena, and B. J. Cho, State of the Art Authentication, Access Control, and Secure Integration in Smart Grid. Energies, 8, 11883-11915; doi:10.3390/en81011883, 2015.