An Approach for Cyber Security Experimentation Supporting Sensei/IoT for Smart Grid

B. Genge, P. Haller, A. Gligor, and A. Beres

Petru Maior University of Tg. Mures, Mures, Romania
bela.genge@ing.upm.ro, phaller@upm.ro, agligor@upm.ro, adela.beres@gmail.com

***Abstract*—We propose SCYAMIX, a middleware aimed at facilitating cyber-physical security experimentation with Sensei/IoT* standard proposal and physical processes for Smart Grid. Sensei/IoT* represents the first joint effort involving ISO, IEC, and IEEE to provide a Semantic Web 3.0 standard for Sensor Networks, M2M and IoT. The proposed middleware fuses together distributed Sensei/IoT*-compliant communication architectures and protocols with real-time software simulators to enable disruptive cyber security experiments. A case study is presented to demonstrate SCYAMIX's ability to recreate Smart Grid architectures involving complex physical processes and cyber security scenarios.**

***Keywords*—Smart Grid, security, middleware, Sensei/IoT*.**

I. Introduction

NOWADAYS, Smart Grid is commonly recognized as the next generation power grid. Through the pervasive adoption of modern Information and Communication Technologies (ICT), Smart Grid improves operational benefits of control, reliability and safety, and provides advanced two-way communication, more flexible integration of heterogeneous measurement and sensor-actuator networks.

Although the adoption of generic off-the-shelf ICT in Smart Grid provisions indisputable advantages and benefits, it raises several issues concerning the reliability and security of communications and control systems – the core infrastructure of Smart Grid. The impact of generic malware on the normal functioning of Industrial Control Systems (ICS – part of Smart Grid core) can be devastating if we simply consider the published attack reports on ICS. Of course, the construction of a comprehensive list of events and attacks is difficult to achieve in the industrial setting, mainly because of non-disclosure policies adopted by different stakeholders. Therefore, most reported events cannot be chronologically ordered, since the actual discovery date of malware does not coincide with the actual infection time of the system.

Nevertheless, the year 2010 can be seen as a turning point in the perception of security in the industrial setting. This is mainly attributed to the discovery of Stuxnet [1], the first malware specifically designed to attack ICS. Stuxnet is also the world's first (discovered) malware capable to rewrite the control logic of ICS hardware and to actually hide its presence by exploiting several zero-day vulnerabilities. Unfortunately, the discovery of systems infected with Stuxnet malware is not limited to the year 2010 and other Stuxnet targets have been discovered at different power plants and installations from southern Iran in 2012 [2]. The potential impact of cyber attacks in the power sector has been highlighted by the Tempe, AZ incident [3] from 2007. In this particular case an improper configuration of load shedding programs caused the opening of 141 breakers and a loss of significant load, which subsequently led to a 46 min power outage affecting almost 100 000 customers.

In this context, the deployment of effective protective mechanisms for future infrastructures such as Smart Grid requires novel testing facilities with complex features embodying the cyber and physical dimension of these critical infrastructures. To address this issue, a substantial number of approaches have been documented in research publications. As such, we find a wide range of testbeds and middleware aimed at facilitating cyber-physical security experimentation with Smart Grid and other industrial infrastructures [7-12]. In the particular case of Smart Grid, a commonly addressed problem is the actual architecture and protocols which will enable the deployment of large-scale infrastructures consisting of a wide variety of devices and systems such as Customer Energy Management Systems (CEMS), Distributed Energy Resources (DER), Advanced Metering Infrastructures (AMI), and so on.

To alleviate the aforementioned issues, this paper proposes *SCYAMIX*, a middleware combining the distributed communication features of HERMIX platform [4] with the real-time simulation capabilities of AMICI [5]. In a nutshell, SCYAMIX enables real-time cyber-physical security experimentation with the recently proposed Sensei/IoT* standard [6]. It implements basic communication and architectural features defined within Sensei/IoT*, and it enables the execution of disruptive experiments against physical infrastructures through the adoption of distributed simulation software.

Although, as shown in the following section, in the literature we find several approaches and middleware for Smart Grid, to the best of our knowledge, the approach presented in this paper is the first attempt aiming at providing experimentation features combining a Sensei/IoT* standard-compliant architecture and protocols with simulated physical processes.

The remaining of this paper is organized as follows. Section II provides an overview of related work. The proposed approach is presented in Section III and experimental results concerning a specific cyber security case study is presented in Section IV. The paper concludes in Section V.

II. RELATED WORK

In this section we provide an overview of the state-of-the-art for Smart Grid architectures. AMI (Advanced Metering Infrastructure) is an important part of the Smart Grid system and several researches have been carried out for making it scalable and operational during outages.

In the work of Zaballos, *et al.* [7], an architecture based on wireless networks and communication power lines for Smart Grids is proposed. The authors concentrate on the communication infrastructure and on the importance of integration of different communication protocols and standards. The paper also documents the successful adoption and application of International Telecommunication Union (ITU) USN/NGN to Smart Grid architecture.

SeDAX (Secure Data-centric Application eXtensible platform) is the platform proposed by Young-Jin Kim, *et al.* [8, 9]. SeDAX uses Delaunay Triangulation (DT) graphs to provide and information-centric communication in the grid. Its architecture focuses on data availability and communication resilience by using a geographic hash forwarding algorithm and a DT-based data replication scheme. The algorithm is evaluated and compared with other geometric-based alternatives based on route tables size, message overhead, delivery performance and replication cost.

Zhou, *et al.* [10] introduced a new performance metric – Accumulated Bandwidth Distance Product (ABDP) to evaluate communication architectures for AMI in Smart Grid. The metric, based on greedy algorithm, was tested on Distributed MDMS (Meter Data Management System) architecture, a fully distributed architecture and centralized communication architecture. Results proved that distributed architectures have more benefits compared to centralized ones.

Athreya and Tague [11] proposed a self-organizing mesh hierarchy to assure the operability of AMI during outages based on a distributed Time Division Multiple Access (TDMA). The model's performance was evaluated using a wireless TDMA modeler, which proved to assure consistent performance during outages.

Finally, we mention the work of Siaterlis, *et al.* [12], where a generic testbed was proposed to enable security studies with cyber-physical systems. The approach employed emulation testbeds to recreate ICT hardware and software and the AMICI simulation software to recreate the behavior of physical processes.

Compared to the previously mentioned approaches, the novelty of the middleware proposed in this paper is that it enables cyber security experiments with an emerging standard, i.e., Sensei/IoT*, ensuring at the same time an accurate recreation of cyber and physical dimension of Smart Grid.

III. ARCHITECTURE AND DESCRIPTION OF THE PROPOSED MIDDLEWARE

In this section we provide a description of the proposed middleware. We start with an overview of the emerging Sensei/IoT* standard and we continue with a brief presentation of the two main components of the proposed middleware: HERMIX and AMICI. Finally, we present the proposed architecture which fuses several technologies and software to enable a wide range of features for cyber security experimentation with Smart Grid.

A. Sensei/IoT: from XMPP to Smart Grid*

The eXtensible Messaging and Presence Protocol (XMPP) protocol, developed in 1999 by the Jabber open-source community was intended for near real-time instant messaging, presence information, and contact list maintenance.

The XMPP is an open eXtensible Markup Language (XML) protocol which defines the way of XML content streaming. It has been used in many applications, most importantly the Smart Grid in the case of the Internet of Things applications.

Since 2002 the XMPP working group established by Internet Engineering Task Force (IETF) has made efforts for standardization. Initially, four specifications (RFC 3920, RFC 3921, RFC 3922, RFC 3923) were created that lead in 2004 to a Proposed Standard. In 2011, first specifications were replaced by RFC 6120 and RFC 6121, and new ones were added such as RFC 6122.

Besides the mentioned core protocols, the XMPP Standard Foundation takes part at the new open XMPP extensions development also known as XEP stanzas. These are not singular and therefore joint attempts for global, open standards among global players are noticed. We mention here the ISO/IEC/IEEE P21451-1-4 XMPP standard, outlined in the following sub-sections.

1) ISO/IEC/IEEE P21451-1-4 XMPP Overview

ISO/IEC/IEEE P21451-1-4 XMPP Interface Standard is also known as *Sensei/IoT** and represents the first joint effort amongst ISO, IEC, and IEEE to design a Semantic Web 3.0 Sensor Standard for Sensor Networks, M2M and IoT.

The main goal of the Sensei/IoT* standard is to demonstrate the assured interoperability, scalability, and security using the XMPP protocol. The scope of the standard concerning Smart Grid can be summarized in the following main points: (i) electric power generation by offering access to data sharing on energy usage, primary energy cost or greenhouse gas emission; (ii) renewable energy based generation and storage systems by offering access to data concerning the primary energy and stored energy availability; (iii) transmission system on lines and busses fault detection; (iv) distribution system on microgrid integration and substation controls; (v) consumer side on using smart metering, the management of the local generation and storage capabilities.

2) Sensei/IoT Main Features*

Smart grid implementation based on Sensei/IoT* standard must answer a series of key challenges concerning: effectiveness of Internet usage, interoperability, scalability, session persistency, cyber vulnerability, cyber exposure, presence detection, security, etc. Many of these challenges are covered by the new proposed standard. We mention some of these features:

- technology agnostic and protocol independent;
- the use of the Transport Layer Security (TLS) for data traffic encryption built into the protocol;
- Meta Data Isolation (MDI) and intrusion protection against cyber-attacks;
- usage of the Semantic Web 3.0 based on XML metadata for providing semantic conversation between devices;
- usage of a Service Broker as a trusted intermediary to establish a trust relationship between users, applications, and devices;
- possibility to use an Identity Provider (IdP) in order to provide Single Sign On (SSO);
- support end-to-end digital signing and encryption based on RFC 3923 Efficient XML Interchange (EXI).

3) Remarks on Using Sensei/IoT standard*

Adopting in the existing or newly emerging Smart Grid the Sensei/IoT* standard can provide a series of benefits such as interoperability, scalability and security. It can be used at any level of a Smart Grid allowing the harmonization of protocols by enabling operation between new and legacy protocols.

Many advantages are given by the characteristics of the XMPP protocol: the technology and protocol independence allows decreasing costs and complexity; XMPP can facilitate a transition to new IEC standards; XMPP offers trusted messages transmission solutions and an easy usage in case of dynamic addressing issues; it has built-in cyber security protection mechanisms.

B. HERMIX Platform

The HERMIX platform [4] developed by Vitheia consortium was designed to collect, store and analyze large amount of data coming from a diversity of nodes, ranging from sensors to high resolution cameras.

The platform can be viewed as a set of interconnected nodes (physical resources, users, automation scripts, services) with a layered architecture. Every node represents an information provider or a consumer. The logical management layer has a service oriented architecture and it is responsible for formatting and extracting the data, for automatic analysis and processing. This layer also manages the proper authentication, authorization and access control mechanisms and assures the interconnection with other systems. The lower communication layer uses the event-driven architecture that follows a publish-subscribe pattern for small and structured data exchanges between nodes. The data storage layer hides the used underlying database system and at the same time it provides storage support for this hybrid communication model.

The features embedded within XMPP, including federation across domains, authentication, end-to-end signing, object encryption and its security support even for mobile endpoints make it a good candidate for industrial applications. The platform uses XMPP for meta-data exchange (like session initiation, device managing requests, etc.) and small structured data generated by endpoints (e.g., events: a switch changes its state, an alarm sensor detects movement). For high quantity, binary data, e.g., video and audio streams, an out-of-band protocol is used depending on the type of stream. At the highest level there is a set of interconnected XMPP servers running over the Internet. The distribution of the XMPP servers ensures proper load distribution, interconnection between resources managed by different authorities.

On the XMPP server level the proposed platform features are implemented in a server side component which exposes basic and common functionalities to be used by the other modules. Those functionalities include:

- communication with the XMPP server and message routing between the connected nodes;
- node management;
- interconnection with the physical bus;
- authorization management;
- persistent storage.

To assure the interoperability between different vendors' specific devices a dedicated module needs to be created for every type of industrial bus (e.g., LON, CAN, EIB, Modbus, etc.). The module communicates with the specific bus and transforms the physical devices information into node representation. The node is not necessarily hosted on the resource itself, it acts as a host for a set of resources connected to the same bus. The module and the delegate nodes assure the protection of the low capability resources, e.g., low power sensor nodes, from external attacks implementing proper authorization and encryption mechanism.

A node identified in XMPP world by a unique *JID* (Jabber ID) is defined by a set of features, status information, received commands, and generated events. Taking into account the heterogeneity of existing protocols, new types can be described, but the main goal of this resource model is to provide homogeneity at the description level. A node can be dynamically created by the Node Manager based on an XML description or based on the image saved in the database. The Node Manager collects and saves automatically every modification in the registered node data in the Object Archive. When a saved data is required, it is loaded into memory and transformed into its runtime C++ representation.

The discovery mechanism is used to obtain information about devices, their features or events, using the standard Service Discovery protocol defined in the XMPP extension XEP-0030 [13]. The state is divided into several parts to assign different privilege levels to the state variables. The events are also organized hierarchically and different events require different privileges to subscribe to them. A user subscribing to a collection node (an event node tree) will receive events generated by all the descendants of the collection node.

The transport of the binary data from a source to multiple destinations is handled by the Controller nodes. The access to the binary archives is also done indirectly, through the controllers. The Controller poses two types of communication channels: one for controlling the way data is distributed based on XMPP protocol; other for actual large data transport. The controller is exposed in middleware as a delegated node attached to a component.

The Object Manager also enforces permission policies managed by an Authorization Manager. Permission attached to an object is represented as a set of tuples (object id, list of permission types, a set of bare JIDs, set of groups). When the Object Manager needs to authorize access to an object, it will request the object's access control list (if not already cached) from the Authorization Manager. The maximum caching interval is imposed by the Authorization Manager and must be invalidated if it is changed. Separation between permission validation and permission management assures the third-party integration.

C. AMICI Platform

The *Assessment platform for Multiple Interdependent Critical Infrastructures* (AMICI) [5] provides software simulators to recreate the physical dimension of critical infrastructures such as Smart Grid. AMICI was developed from the need to provide real-time multi-model experimentation capabilities supporting cyber security studies concerning critical infrastructures. Its architecture, depicted in Figure 1, includes two main components: a simulation unit denoted as *Sim*; and a proxy unit, denoted as *Proxy*.

The main role of the simulation unit (Sim) is to run the physical process model in real-time. This is achieved by coupling the model time to the system in such a way to minimize the difference between the two. Models are constructed in Matlab Simulink from where the corresponding 'C' code is generated using Simulink Coder. These are then integrated using an XML configuration file that provides the required flexibility so that researchers do not need to modify AMICI's source code.

From the *Sim* unit's point of view each model is seen as a set of inputs and outputs. These are mapped to an internal memory region (I/O MEM) that is read/written by other software modules as well. The Sim unit allows an open access to its I/O MEM by implementing OS level shared memory operations. This way, AMICI enables interaction with ad-hoc software that can write specific model inputs, i.e., OPEN/CLOSE a valve, and can read the status of the model, i.e., measured voltage. Interaction with other Sim units is enabled by implementing not only RPC (Remote Procedure Call) server-side operations but client-side calls as well. By using only the XML configuration file, the Sim unit can be configured to read/write inputs/outputs of models run by remote Sim units. These are mapped to the inputs/outputs of the model running locally, enabling complex interactions between models running in parallel on different machines. The Proxy unit has several roles within AMICI. First of all, it is able to run remote control code, thus enabling the integration of more complex control hardware emulators. At the same time, it can be used to handle Modbus protocol calls, transforming them to RPC calls and finally sending requests to the Sim unit.

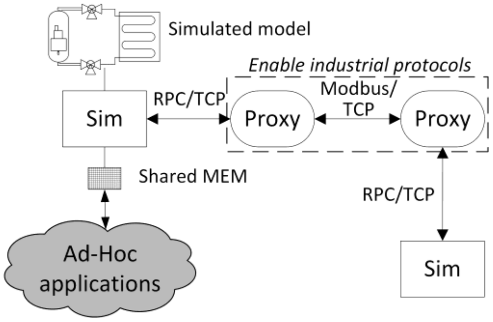


Figure 1: Architectural overview of AMICI.

As demonstrated in [12], AMICI can be applied to a wide range of security experiments. Its software units have been tested with several physical process models such as oil-fired electrical power plants, chemical processes, railway systems, and large-scale power grid models. AMICI's software units are available as open source under EUPL license and can be freely downloaded from SourceForge (http://sourceforge.net/projects/amici/).

D. SCYAMIX: Fusing HERMIX With AMICI

We propose *Smart grid CYber security assessment platform based on AMIci and hermiX (SCYAMIX)*, which fuses together the communication features provided by HERMIX with the physical process simulation capabilities brought by AMICI. SCYAMIX is thus able to provide realistic communication architectures and protocols which have been proved to be well-adapted to large infrastructures such as the Smart Grid [4]. At the same time SCYAMIX brings additional capabilities to enable the recreation of the physical dimension, which constitutes a significant component of any industrial system.

Fundamentally, from an architectural point of view, SCYAMIX provides capabilities to recreate the cyber and physical dimension of Smart Grid. For the cyber dimension SCYAMIX adopts HERMIX to provide real software and protocols running on real networking infrastructures. This approach is well established in the field of cyber security, since the use of real infrastructures provides high fidelity of results and in many cases it can capture not only whether a system will fail but also how it will fail. In contrast, the use of simulation to recreate the cyber dimension of Smart Grid would provide an effective approach to model normal network and software conditions, but it would fail to capture the way computer networks fail. This aspect has been well documented and studied by previous work [12, 14, 15, 17].

For the physical dimension SCYAMIX uses simulation since this provides an efficient, low-cost and safe approach to recreate the physical dimension. Apparently, this might be interpreted as a lack of realism and low experiment fidelity, however, the use of software simulation for cyber security experimentation scenarios enables disruptive experiments on multiple heterogeneous physical processes.

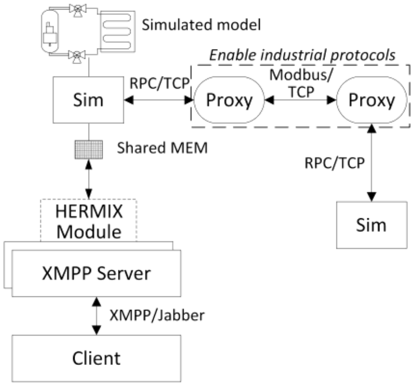


Figure 2: SCYAMIX architecture.

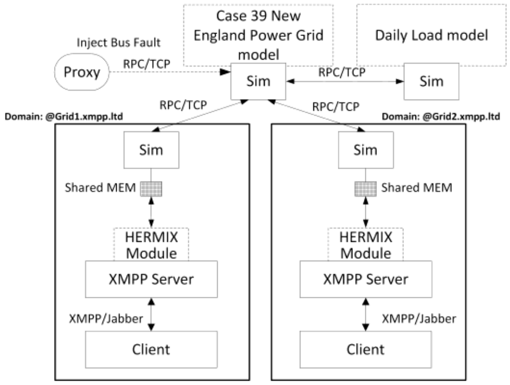


Figure 3: Experiment setup.

This is not possible with production systems since security and resilience tests entail risks of potential side effects to mission critical services [16]. Furthermore, today several complex models are freely available and are actually applied in different industries. For example, in the energy sector simulation has become so accurate and trusted that it is commonly used to aid decision making between transmission system operators.

The architecture of SCYAMIX, as a result of fusing HERMIX and AMICI is depicted in Figure 2. The procedure followed for this purpose exploits the features provided by each of the two software platforms. As such, we implemented an additional HERMIX module to access the shared memory region created by AMICI's simulation unit. Model inputs and outputs are written and read by the implemented module, ensuring the required communication between cyber components and the simulated physical processes.

Devices exposed by simulated models, e.g., valves and sensors, are given different JIDs and are accessed through standard XMPP stanzas. Each device is registered in the HERMIX database (Mongodb) and users (client software) can subscribe to receive events. The proposed platform is thus compatible with any client software implementing an XMPP communication interface according to the standard description. This provides a powerful feature and enables the integration of heterogeneous software which can interact with simulated physical processes in a wide range of scenarios.

IV. Case Study

In this section we present a case study showing the applicability of the proposed middleware. We start by presenting a description of the experiment setup and scenario, and we continue with the presentation of results.

A. *Experiment Setup and Scenario*

The aim of this particular scenario is to illustrate the interdependence property of physical processes and how this property can be used to detect attacks/faults by indirect monitoring of process parameters. The experiment also shows the applicability of the proposed middleware in constructing realistic Smart Grid scenarios and conducting realistic cyber security experiments.

For the physical process we adopted the IEEE 39-bus New England system [18], representing a portion of the American Electric Power System as of early 1960. The model is run by a simulator unit and includes 39 buses, i.e., substations, together with 10 generators. The daily load applied to our system derives from real data [19] and is run in parallel with the power grid model by a separate simulation unit.

We defined two separate XMPP/Jabber domains: *@Grid1.xmpp.ltd* and *@Grid2.xmpp.ltd*. As it would happen in reality, we used each domain to monitor a subset of substations. More specifically, client applications in *@Grid1.xmpp.ltd* monitored buses 1 to 18 while client applications in *@Grid2.xmpp.ltd* monitored buses 19 to 39.

The disturbance we applied to the grid consisted of a 100ms bus fault issued with the help of Proxy unit from AMICI software. The fault replicates the effect of an attack on the power grid which causes circuit breakers to trip, which finally leads to a brief disconnection of a specific bus from the grid. The experiment setup is depicted in Figure 3.

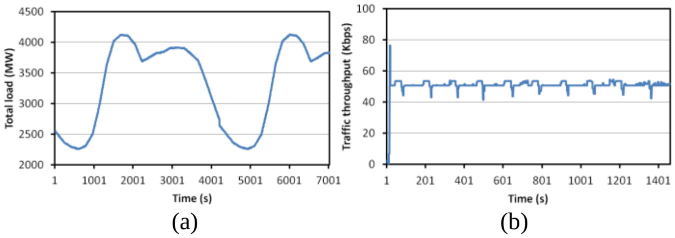
B. *Experimental Results*

The daily load applied to the grid during this scenario is similar to a typical daily load curve and is depicted in Figure 4 (a). The XMPP traffic measured in both domains is highly regular and mostly constant, as shown in Figure 4 (b). The visible bursts in the same figure are caused by concentrator mechanisms implemented within HERMIX modules.

In Figure 5 we have depicted the measured voltages in the two power grid domains. As shown in both sub-figures, voltages are highly sensitive to the injected disturbance. The bust fault is applied to bus 1, belonging to the first domain, and the effect of this action is clearly visible in Figure 5 (a).

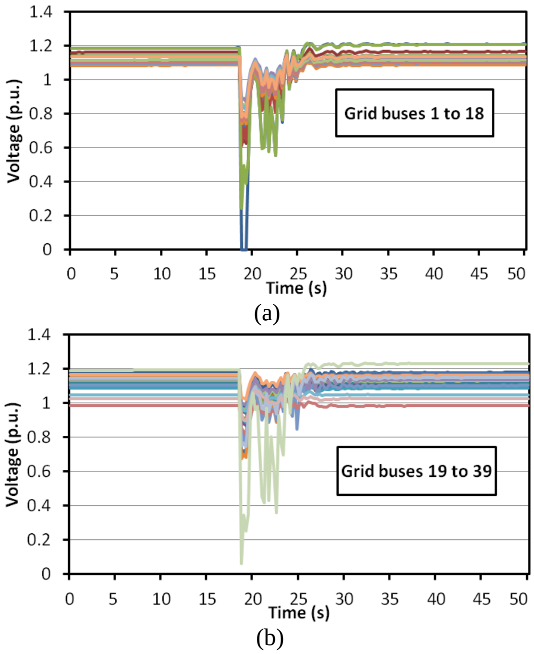
The injected disturbance is highly visible in the second domain as well (see Figure 5 (b)). Here we recorded voltage collapse for only one bus (bus 39), which is directly connected to bus 1. Nevertheless, the effect is also visible on the voltage level of all the other buses.

This close relationship between different power grid substation voltages comes from the interconnections and interdependencies between different buses. Electricity grids require the establishment of a certain balance between the generated and consumed power. When this balance is disturbed, there can be serious consequences leading to power failure and massive black-outs. Cyber attacks might have a similar effect to the one reported in this study, since circuit breakers and control mechanisms have the ability to respond to commands issued remotely. These can lead to severe loss of load which can have a similar effect to the Tempe, AZ incident [3] from 2007, as mentioned earlier in this paper.



(a) (b)

Figure 4: Daily load (a) and XMPP traffic throughput in the first domain (b)



(a)

(b)

Figure 5: Measured disturbance on power grid by client in *@Grid1.xmpp.ltd* (a) and by client in *@Grid2.xmpp.ltd* (b)

V. Conclusion

The middleware proposed in this paper provides a suite of software components and protocols to enable cyber security experimentation with the recent Sensei/IoT* standard proposal. We believe that SCYAMIX advances the state of the art from several perspectives: (i) the approach fuses a XMPP/Jabber-compliant implementation with software simulators in order to provide a complex set of features; (ii) the middleware is highly scalable, supporting scalable cyber and physical dimensions of Smart Grid; and (iii) to the best of our knowledge SCYAMIX is the first reported approach providing a Sensei/IoT* compliant implementation combining communication architectures and protocols with real-time software simulation. As future work we intend to extend SCYAMIX's capabilities and to test its performances in scenarios including real sensor networks.

Acknowledgment

This research was supported by a Marie Curie FP7 Integration Grant within the 7th European Union Framework Programme.

References

[1] T. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, April 2011.

[2] BBC News, *Iran 'fends off new Stuxnet cyber attack'*, 22 December 2012.

[3] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*, New York, Momentum Press, May 2010.

[4] P. Haller, A. Bica, and I.C. Szanto, "Middleware for heterogeneous subsystems integration in health care services," *Interdisciplinarity in Engineering International Conference*, Tirgu Mures, pp. 349–354, 2012.

[5] B. Genge, C. Siaterlis, and M. Hohenadel, "AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures," *7th International Conference on Critical Information Infrastructures Security*, Lillehammer, Norway, Lecture Notes in Computer Science 7722, pp. 228–239, 2012.

[6] M. Presser, P.M. Barnaghi, M. Eurich, and C. Villalonga, "The SENSEI project: integrating the physical world with the digital world of the network of the future," IEEE Communications Magazine, vol. 47, no. 4, pp. 1-4, April 2009.

[7] A. Zaballos, A. Vallejo, and J.M. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Network*, vol. 25, no. 5, pp. 30–37, 2011.

[8] Young-Jin Kim, Jaehwan Lee, G. Atkinson, Kim Hongseok, and M. Thottan, "SeDAX: A Scalable, Resilient, and Secure Platform for Smart Grid Communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1119-1136, July 2012.

[9] M. Hoefling, C.G. Mills, and M. Menth, "Analyzing storage requirements of the resilient information-centric SeDAX architecture," *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 306-311, Oct. 2013.

[10] Jiazhen Zhou, R.Q. Hu, and Yi Qian, "Scalable Distributed Communication Architectures to Support Advanced Metering Infrastructure in Smart Grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1632-1642, Sept. 2012.

[11] A.P. Athreya and P. Tague, "Self-organization of a mesh hierarchy for smart grid monitoring in outage scenarios," *2013 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1-6, Feb. 2013.

[12] C. Siaterlis, B. Genge, and M. Hohenadel, "EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, Dec. 2013.

[13] XEP-0030: Service Discovery, 2008, http://xmpp.org/extensions/xep-0030.html.

[14] R. Chertov, S. Fahmy, B. Ness Shroff, "Fidelity of Network Simulation and Emulation: A Case Study of TCP-targeted Denial of Service Attacks," *ACM Trans. Model. Comput. Simul.*, vol. 19, no. 1, pp. 4:1-4:29, Jan 2009.

[15] B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera, "A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems," *Computers and Electrical Engineering*, Elsevier, vol. 38, no. 5, pp. 1146-1161, 2012.

[16] D. Duggan, "Penetration testing of industrial control systems," Technical Report, SAND2005-2846P, Sandia National Laboratories, 2005.

[17] B. Genge and C. Siaterlis, "Analysis of the effects of distributed denial-of-service attacks on MPLS networks," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 87-95, 2013.

[18] University of Washington – Electrical Engineering, "Power Systems Test Case Archive," http://www.ee.washington.edu/research/pstca/

[19] M. Manera and A. Marzullo, "Modelling the load curve of aggregate electricity consumption using principal components," *Environ. Model. Softw.*, vol. 20, no. 11, pp. 1389-1400, Nov 2005.