Towards the Cross-Domain Interoperability of IoT Platforms

Sergios Soursos*, Ivana Podnar Žarko§, Patrick Zwickl¶, Ivan Gojmerac¬, Giuseppe Bianchi| and Gino Carrozzo**
* Intracom SA Telecom Solutions, Athens, Greece, Email: souse@intracom-telecom.com
§ University of Zagreb, Faculty of Electrical Engineering and Computing, Zagreb, Croatia, Email: ivana.podnar@fer.hr
¶ University of Vienna, Faculty of Computer Science, Vienna, Austria, Email: Patrick.Zwickl@univie.ac.at
¬ AIT Austrian Institute of Technology GmbH, Vienna, Austria, Email: ivan.gojmerac@ait.ac.at
| CNIT / University of Roma Tor Vergata, Rome, Italy, Email: giuseppe.bianchi@uniroma2.it
** Nextworks Srl, Rome, Italy, Email: g.carrozzo@nextworks.it

Abstract— **The Internet of Things is evolving around a plethora of vertical platforms, each specifically suited to a given scenario and often adopting proprietary communications, device and resource control protocols. The emerging need for cross-domain IoT applications and services highlights the necessity of interoperability across IoT platforms for a unified and secure sharing of and access to sensing/actuating resources. This position paper describes the current state of the IoT landscape, the opportunities that appear towards its sustainable evolution as well as the challenges that need to be addressed. In this context, the vision and objectives of the H2020 symbIoTe project are also presented; symbIoTe aims at the interoperability of IoT platforms by offering a flexible interoperability framework that will allow i) vertical IoT platforms to cooperate, ii) collaborative IoT platforms to form IoT-platform federations for exchange of resources and iii) independent developers to create innovative and cross-domain applications.**

Keywords— IoT; interoperability; federation; business models; resource virtualization; middleware

I. Introduction

Applications and services relying on *connected smart objects*, such as thermostats, motion detectors and light sensors, are increasingly deployed in many domains, from residences, offices and factories, to cities, transportation, logistics and energy production. The current landscape of *Internet of Things (IoT)* consists of vertical, highly specialized solutions that target niche markets. These solutions are traditionally developed and deployed in silos, in order for the companies that offer them to maintain the competitive advantage, secure the customer base and provide efficient support and maintenance. The number of available IoT solutions per domain is increasing rapidly, but so does their equipment footprint: even if the size of the involved devices lessens, their variety increases as more applications and services tackle with the different aspects of everyday business and personal life.

In addition, we are witnessing the proliferation of *wearable smart objects* that blend with surrounding environments, in accordance with the Weiser's vision of ubiquitous computing [1]. Such moving devices sense their environment and interact with their surroundings to take/give actuation orders. An increasing number of applications rely on such devices to offer people digital aids for their everyday activities.

In this continuously evolving *IoT landscape*, recent studies show that the number of connected smart objects will radically increase in the next years [2]. This blooming of smart devices will certainly boost the IoT business [3], introduce new services and open the way for innovative applications. Growth however will also bring some negative side-effects that will question the sustainability of current and future IoT solutions.

The need for cross-domain IoT applications that can cover multiple aspects of everyday life is becoming more apparent nowadays. Vertically isolated platforms will need to be extended and cover other domains in which, however, the supporting companies may not have the required expertise. Strategic partnerships are expected to be the only viable option. Moreover, the collocation of IoT platforms addressing different domains may result in resource inefficiencies, since similar sensors may be deployed by different platforms at the same locations. Furthermore, the burden of a single stakeholder deploying and managing the end-to-end infrastructure, from sensors and gateways to back-office servers and platforms, introduces a very high cost barrier for new entrants to the IoT market which will, in turn, hold back the innovation opportunities for SMEs and start-ups. Finally, it is not expected that a single communications protocol for smart devices or semantic representation for IoT resources will prevail; hence, the need for supporting even more protocols is becoming an integration nightmare for IoT application developers and device manufacturers.

In the remainder of this paper, we highlight the aspects considered to be crucial for the sustainable evolution of the IoT landscape towards cross-domain interoperability (cf. Section II). In Section III, we present the approach of *symbIoTe* (Symbiosis of smart objects across IoT environments) [4], an H2020 research project on the collaboration of IoT platforms. Finally, Section IV summarizes the main findings of the paper and identifies the next steps needed to be taken by the symbIoTe project in order to reach its objectives.

II. Beyond Vertical Solutions

The image of a fragmented IoT ecosystem is best depicted by a series of vertical solutions which, on the one hand, integrate connected objects within local environments that we call *smart spaces* and, on the other hand, connect smart spaces with proprietary back-end software solutions, typically hosted on the Cloud. A wide range of commercial offerings are based on the convergence of smart space infrastructure with Cloud resources and IoT platforms, e.g., Xively, Cumulocity, IBM Bluemix, and AWS IoT.

For the evolution towards an ecosystem where IoT platforms cooperate and potentially also collaborate by sharing their infrastructure, smart objects and Cloud resources to jointly address cross-domain challenges, a number of aspects need to be considered. The adoption of these aspects is expected to transform the IoT business landscape in a beneficial way for all existing and new stakeholders and, eventually, offer innovative solutions to end users.

A. IoT Platform Federations

Vertical IoT solutions focus on specific activities of everyday life, but are restricted to the ecosystem that can be created around a single platform (see "Closed Private" IoT Business models in [5]). Through interoperability [6] and federations, multiple IoT solutions can collaborate so as to i) provide cross-domain solutions, and ii) share IoT resources and the respective measurements in locations originally out of their reach. This represents an additional horizontal integration that enables "Open networked" IoT business models according to the classification in [5]. Such a federation will not try to enforce a specific (communications, semantic representation, control) protocol to be established as the sole standard across different domains. On the contrary, IoT platforms will continue to select the desired protocols to control the end-to-end communications and data exchange (from sensors to gateways to Cloud-based platforms) that suit their purposes. However, higher-level interfaces and (mainly) semantic ontologies can be used to communicate the desired data (sensor or service related) across platforms and domains. Northbound (REST) interfaces may already exist in some platforms at the Cloud level that expose (part of) the supported functionality to third parties, e.g. application developers. Such interfaces can be re-used to expose the functionality among different platforms (in an East-West manner). Moreover, a federation should be achieved at a lower level for collocated platforms by, i.e., allowing communications between different IoT gateways. Again, the envisioned communications can be supported by the current protocols (modern gateways typically support the most popular ones), so the work should again focus on the representation (and abstraction) of the useful information between different gateways.

B. Domain Enablers

It is crucial for the co-creation of cross-domain solutions that expertise in a certain domain by existing solutions is exploited. To achieve this, current IoT solution providers wrap and offer their domain-specific platforms in a 'Sensing as a Service' manner [7]. This way, important and useful information with respect to a single domain can be provided to third parties, typically after some pre-processing and aggregation. For example, an IoT platform for smart residence can offer *domain-specific enablers* for light conditions or house temperature. Such enablers can be used by other platforms, such as smart grid platforms or home security systems, to enrich their inputs and take more accurate decisions without having to deploy additional devices. Moreover, such enablers can be used from application developers for cross-domain applications without having to know the full details of the deployed systems.

C. Cooperation and Collaboration by Sharing of Resources

Apart from the communications technologies and data representation models, the IoT landscape is heavily characterized by the plethora of smart devices that are available. The equipment footprint of IoT solutions creates a burden of managing such distributed resources in an efficient manner. The fact that smart objects of similar type, but belonging to different IoT solutions may co-reside in the same location, introduces an additional complexity. To deal with this increasing complexity and reduce the deployment costs, collocated platforms can choose to be cooperative by opening up the access to their resources to third parties and by implementing generic high-level APIs. In addition, they may choose to collaborate by sharing the common physical resources in a coordinated way. For this reason, cooperative technologies and features can facilitate the immersion of IoT technologies into the real-world. Orthogonal features enabled through collaboration may encompass resource bartering and trading functionalities (see technical background on federated trading in [8]) in order to enrich the IoT landscape. Especially for the case of cross-domain solutions, resource sharing renders as the only way towards a sustainable solution, especially when SMEs are considered.

D. New Business Models in the IoT Value Chain

Putting the technical details aside, the federations among IoT solution providers need to be supported by the appropriate business models in order to be viable. While basic literature on IoT business models is arising [9][10], the horizontal integration in federations, as targeted by this paper, deserves more specific considerations: the current IoT value chain includes stakeholders like device and gateway manufacturers (or infrastructure providers, in general), IoT platform providers, Cloud operators, ISPs and application developers. In order for the envisioned federation to become a reality, different options are available. In case of a bilateral collaboration between two platform providers, specific SLAs (or equivalent lightweight structures) must be in place for the sharing of resources, the level of detail for the exchanged data and for the distribution of the new market value. But, if we consider a wider-scale federation, not only for the benefit of the participating operators but also for the realization of innovative cross-domain applications on top, then a new role may have to be introduced to handle a broader cooperation; that of the 'virtual IoT provider' (vIoT provider). The vIoT provider can be considered as a kind of broker that provides a clearing point for the federation, a kind of marketplace where standalone IoT providers can offer access to their (aggregated) resources, or offer domain specific enablers, either to other IoT providers or to application developers. The role of this virtual IoT Provider can be undertaken by existing stakeholders, such as Cloud operators or ISPs, but also new stakeholders may be introduced for this purpose. It becomes obvious that new business cases can be established as well: IoT providers can act as resource suppliers by advertising their offerings and charge the access to them and application developers or other IoT providers must pay for the resources or services they use. This creates a transition to more specialized stakeholders that can focus on their specific competencies. Apart from this, innovators in the IoT scene, such as small startups, can profit from a converged IoT landscape, as the market barriers are reduced whenever the competition on “own platforms” becomes a secondary consideration. This facilitates the process of quickly deploying and commercializing innovative ideas with limited budget. Moreover, new business cases may be created for existing stakeholders: infrastructure providers can let their deployed equipment to multiple IoT providers for cross-domain purposes and cost efficient solutions. For example, a modern office space could additionally provide various kinds of IoT resources for tenants that are included in the rent.

III. THE SYMBIOTE APPROACH

symbIoTe is an H2020 research and innovation project that aims at addressing the challenging objective of an interoperable IoT ecosystem that will allow for the collaboration of vertical IoT platforms towards the creation of cross-domain applications. This section presents the technical foundations of the symbIoTe concept and the envisioned use cases that will demonstrate the applicability of the proposed solution.

A. *Technical overview*

The symbIoTe approach is built around a hierarchical IoT stack connecting smart objects and IoT gateways within smart spaces with the Cloud. Smart spaces share the available local resources (connectivity, computing and storage), while platform services running in the Cloud should enable Cloud federations and open up the northbound interface to third parties. The architecture comprises four layered domains, as depicted in Fig. 1.

The *Application Domain* offers a high-level API for a unified view on different platforms to enable cooperation and support cross-platform discovery and management of IoT resources, as well as data acquisition and actuation in accordance with platform-specific business rules. It needs to rely on a common semantic representation for IoT resources, and, in addition, it will offer domain-specific enablers to ease the development of domain-specific applications. In essence, this domain materializes the vIoT concept mentioned earlier.

The *Cloud Domain* hosts the Cloud-adjusted building blocks of specific platforms (e.g., a data store, data analytics and stream processing tools, tools for platform management, etc.). To enable platform federations and sharing of resources, we envision a symbIoTe interworking interface to be defined and implemented for the exchange of information between two collaborating IoT platforms. The interworking API will expose a directory of open platform resources and will implement an interworking protocol for the exchange of information between platforms by means of platform-specific adaptors.

The *Smart Space Domain* comprises smart objects, IoT gateways as well as local computing and storage resources available within, e.g., a home environment or campus building. We assume that IoT platform-specific gateways are setup in the smart space domain. To enable dynamic sensor discovery and configuration in smart spaces as well as dynamic sharing of the wireless medium, symbIoTe adds a new software component, *symbIoTe middleware*, to the smart space domain. The symbIoTe middleware exposes a standardized API for resource discovery and configuration within a smart space, and implements a sensor-discovery protocol for a simplified integration of sensors with platforms hosted in particular smart space domains. After the initial interaction with the middleware, a smart object is connected to and configured with the platform gateway serving the domain (either home or visited). This protocol will also enable that a smart object entering a visited domain becomes part of a new smart space, enabling thus *device roaming*. An SLA needs to be in place between a home and visited domain which also specifies services exposed to the visiting device in the new domain.

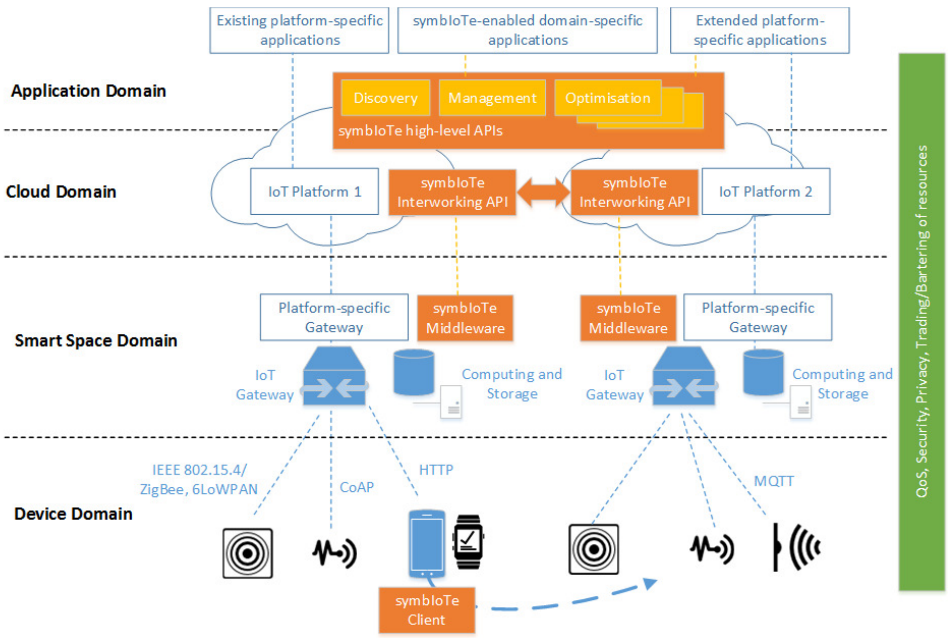

Fig. 1. The symbIoTe high-level architecture.

The *Device Domain* spans over heterogeneous devices which may use proprietary link layer protocols, or ZigBee and 6LoWPAN, while it can be expected that future smart objects will also support application-layer protocols such as HTTP, CoAP and MQTT. Devices should be capable to dynamically blend with the surrounding environment and get discovered by the symbIoTe middleware which performs the initial "introduction" of devices within a smart space. Smart objects can self-organize and can be configured on the fly to be integrated with different IoT platforms hosted within the smart space, preventing thus the lock-in of customers to a specific IoT platform and IoT provider. We envision that device specific *symbIoTe clients* will be running on, e.g., smartphones, to realize these properties.

B. Architectural considerations

symbIoTe is not yet another IoT platform, but aims at designing an architecture that will enable the interconnection of existing IoT platforms at different levels, as identified above. Hence, symbIoTe builds upon existing and well defined reference architectures which, with the appropriate extensions, can support the envisioned platform cooperation and coordination. A number of IoT reference architectures already exist and the compatibility of the symbIoTe architecture with (some of) them is one of the key project objectives.

The FP7 IoT-A project defined the *IoT-A Architectural Reference Model (IoT-A ARM)* focusing on the architectural principles pertaining mainly to required functionality offered by a single IoT platform [11]. symbIoTe is in-line with the IoT-A ARM approach, since the envisioned symbIoTe domains can be mapped to the IoT-A ARM, with focus on the Management, Security, Service Organization, Virtual Entity and IoT Service aspects of the IoT-A Functional Model (at the Application and Cloud domains). The *oneM2M Architecture* [12] is considered as the basis for symbIoTe to provide extensions towards the IoT interoperability. Initial investigations place the symbIoTe extensions (at the Cloud domain) around the Mca, Mcc and Mcc' Reference Points, involving the Application Service/Dedicated, Infrastructure and Middle Nodes. Moreover, it is expected that the works of the W3C's Web of Things Interest Group [13] will also help to shape the envisioned functionality at the Application domain. Finally, although symbIoTe will provide its middleware to any IoT platform that wants to benefit from its offerings, the OpenIoT platform [14] will be used as a reference IoT platform to build the Open Source symbIoTe adapters.

C. Envisioned use cases

symbIoTe use cases are targeting typical daily environments, both indoor and outdoor, to assist people seamlessly while performing their daily activities. These environments can range from homes, offices and public spaces (e.g. campuses, stadiums or ports), to smart mobility solutions that assist travelers and commuters. The diversity of the considered environments is optimal to showcase platform interoperability, since it spans over a number of various IoT installations, which are currently isolated and managed as closed systems. In contrast to the current situation, when a user has to use different applications at home, for public transport, at the university, etc., symbIoTe use cases will be able to demonstrate a completely new type of applications built on top of interoperable platforms. These context-based applications will accompany a person as true virtual personal assistants during their daily activities and use resources within his/her environment without requiring any specific user action.

Smart residence will enable automatic discovery and configuration of devices in homes and offices as well as sharing of available resources (processing power, storage and wireless medium) is smart spaces with collocated platforms. The basic idea is to exploit local resources and dynamic service composition to manage and access functions across any available device, from smart phones and tablets, to automation devices, media players, as well as personal health and environmental sensors. Depending on the context and usage scenario, dynamically discovered functions can be presented on different devices, instantiated in a local/remote cloud and finally executed by the appropriate physical devices across-different platforms. The use case will showcase the potential of symbIoTe middleware to realize the interoperability of collocated deployments in smart spaces.

Smart campus will develop campus-wide smart services across various platforms with a focus on collaboration services which utilize indoor navigation and room/equipment booking in accordance with access scopes varying from public low-restriction resources to highly-restricted resources In addition, it will enable "eduroam-like" IoT services for visiting students and staff and showcase device roaming across IoT domains, e.g., when a visiting student enters a campus area while his/her smart phone or smart watch becomes a visiting device in the campus smart space. This is an ideal use case to showcase IoT platform federations in public and collaborative environments.

Smart stadium will enable indoor location services while supporting strict security and privacy policies. The goal is to link digital and physical worlds so as to create a unique experience for stadium visitors. The use case will showcase an easy and transparent use of indoor location platforms to be integrated with various context-based information services so that, e.g., visitors are guided to their seating places or closest available facilities, and provided with more information regarding their favorite football player. Platform interoperability will be enabled at the application domain through the symbIoTe high-level API and a specially-designed symbIoTe location enabler.

Smart mobility and ecological urban routing aims at addressing the problem of inefficient transport and poor air quality that many European cities face nowadays. This use case will offer the ecologically most preferable routes for motorists, bicyclists and pedestrians based of the available traffic and environmental data acquired through various platforms. For air quality monitoring, in-situ environmental monitoring stations can be combined with wearable sensors and mobile devices (mobile crowd sensing approach) to provide enriched environmental measurements which are dense both in space and time. At the same time, traffic information related to road traffic congestion and occupancy of parking spaces offered by fixed sensors also offers the input data for ecologically preferable route calculation. The use case will showcase platform interoperability within the application domain with a

TABLE I. SYMBIOTE USE CASES AND INTEROPERABILITY FOCUS

Smart residence	Interoperability of collocated deployments within smart spaces
Smart campus	IoT platform federation within the cloud domain
Smart stadium	Interoperability of cooperative platforms at the application domain
Smart mobility and ecological urban routing	Interoperability of cooperative platforms at the application domain; potential for resource bartering/trading
Smart yachting	Interoperability of cooperative platforms at the application domain with time- and safety-critical requirements

potential for business models for bartering and trading of resources which also require IoT platform federations.

Smart yachting will automate the exchange of information between a boat and the port, operated by two different platforms. It will enable enhanced information services during mooring to allow users on a boat to identify automatically the territorial characteristics, while a port authority will be able to automatically send various notifications to the boat. Another service is automated supply chain activation for refitting, maintenance and yacht services. From an IoT integration perspective, this scenario represents a challenging environment with multiple control platforms on board and in the port area which require time- and safety-critical coordination.

TABLE I. lists the previously introduced use cases and identifies their interoperability focus with respect to the symbIoTe high-level architecture and its four domains.

IV. SUMMARY AND NEXT STEPS

The *first part* of this paper highlights the current state of the IoT ecosystem. The IoT market is expected to grow in the near future, but at the same time, the need for broader IoT applications to cover multiple aspects of the everyday life is still unmet. To this direction, the inherent deficiencies that prevent the appearance of cross-domain IoT applications are discussed. Through the analysis, a number of steps towards the interoperability of IoT platforms are presented. IoT interoperability and federations are expected to boost the IoT market, as well as lower the entry barriers to new and small-to-medium stakeholders. Cooperation and collaboration by sharing of IoT resources on multiple levels are the first steps towards the new IoT paradigm. All these must be complemented with the proper business models so as to offer sustainable and innovative IoT solutions to the end users. In the *second part* of the paper, the general concepts of the symbIoTe project are presented. symbIoTe aims to design and build an interoperability framework for IoT platforms to simplify the process of cross-platform application development as well as flexible integration of smart space infrastructure within symbIoTe-enabled environments for the benefit of all IoT stakeholders. This will be achieved by providing a unifying abstraction layer for generic access to virtualized resources exposed by the actual underlying IoT platforms. In addition, a number of domain-specific enablers are envisioned to ease the development of end-user applications across platforms. IoT platform interoperability is a challenging task due to dynamic environments requiring context-aware and adaptive capabilities of smart objects which reflect in the complexity of end-user applications and IoT platform management. symbIoTe will identify the functional and nonfunctional requirements for such a dynamic environment and will implement the symbIoTe middleware for smart device discovery and reconfiguration, protocols for platform interworking and components enabling smart object roaming. The offered functionality will be showcased through a number of pilots. Finally, the resulting framework will be offered as Open Source to third parties, either to extend it to integrate more IoT platforms into the symbIoTe framework, or to use it to create innovative applications benefiting from the available smart resources.

ACKNOWLEDGMENT

This work is supported by the H2020 symbIoTe project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688156. The authors would like to cordially thank the entire symbIoTe consortium for their valuable comments and discussions.

REFERENCES

[1] M. Weiser, "Hot topics-ubiquitous computing," Computer, vol. 26, no. 10, pp. 71–72, Oct 1993.

[2] Gartner, "Predicts 2015: The Internet of Things," December 2014, Avaulable Online: https://www.gartner.com/doc/2952822/predicts--internet-things

[3] GSMA Intelligence, "From concept to delivery: the M2M market today", February 2014, Available Online: https://gsmaintelligence.com/research/?file=140217-m2m.pdf

[4] The H2020 symbIoTe project, Available Online: https://www.symbiote-h2020.eu

[5] S. Leminen, M. Westerlund, M. Rajahonka, R. Siuruainen, S. Andreev, S. Balandin, Y. Koucheryavy, "Towards IoT ecosystems and business models," in: Internet of Things, Smart Spaces, and Next Generation Networking. Springer Berlin Heidelberg, 2012. 15-26.

[6] M. Blackstock and R. Lea, "Toward interoperability in a web of things," in Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication (UbiComp '13 Adjunct), ACM, New York, NY, USA, pp. 1565-1574, 2013.

[7] J. Soldatos, N. Kefalakis, M, Serrano, M. Hauswirth, "Design principles for utility-driven services and cloud-based computing modelling for the Internet of Things," in: International Journal of Web and Grid Services (IJWGS) 10.2/3 (2014), pp. 139–167.

[8] O.K. Lee, S. Benford, "An explorative approach to federated trading," Computer Communications, 1998, 21. Jg., Nr. 2, S. 162-170.

[9] M. Westerlund, S. Leminen, M. Rajahonka, "Designing business models for the internet of things," Technology Innovation Management Review, 2014, 4. Jg., Nr. 7, S. 5

[10] S. Turber, C. Smiela, "A Business Model Type for the Internet of Things," 2014.

[11] "Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model", A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, and S. Meissner (Eds.). Springer, Heidelberg, (2013)

[12] "oneM2M Functional Architecture", Technical Report, oneM2M TS-0001, version 1.13.1, Release 1, Available Online: http://www.onem2m.org/technical/published-documents

[13] "Web of Things Interest Group", W3C, Available Online: https://www.w3.org/WoT/

[14] J.Soldatos et al. "OpenIoT: Open Source Internet-of-Things in the Cloud," in Interoperability and Open-Source Solutions for the Internet of Things, Lecture Notes in Computer Science 9001, Springer 2015, pp. 13-25.