A Requirements-based Approach for the Evaluation of Emulated IoT Systems

A. Omar Portillo-Dominguez*, Vanessa Ayala-Rivera*
* Lero@UCD, School of Computer Science, University College Dublin, Ireland
Email: {andres.portillodominguez,vanessa.ayalarivera}@ucd.ie

***Abstract*—The Internet of Things (IoT) has become a major technological revolution. Evaluating any IoT advancements comprehensively is critical to understand the conditions under which they can be more useful, as well as to assess the robustness and efficiency of IoT systems to validate them before their deployment in real life. Nevertheless, the creation of an appropriate IoT test environment is a difficult, effort-intensive, and expensive task; typically requiring a significant amount of human effort and physical hardware to build it. To tackle this problem, emulation tools to test IoT devices have been proposed. However, there is a lack of systematic approaches for evaluating IoT emulation environments. In this paper, we present a requirements-based framework to enable the systematic evaluation of the suitability of an emulated IoT environment to fulfil the requirements that secure the quality of an adequate test environment for IoT.**

I. Introduction

The Internet of Things (IoT) has become a major technological revolution impacting all major industry fields and business areas. Driven by the huge economic impact and benefits (estimated in $2.7 to $6.2 trillion until 2025 by Gartner [1]), the IoT is leading to an explosive growth in the number of Internet-connected devices worldwide. One estimate is that there will be more than 50 billion connected devices on the IoT by the year 2020 [2], [3]. While the criticality of the services provided by IoT varies by applications (which range from household devices to critical systems), the quality of all services can be affected by similar factors. For instance, an IoT system's performance can be impacted over potentially heavily congested networks -or low power lossy networks- and as a result, the IoT system may fail to fulfil its service level agreements. Additionally, IoT devices can also be affected by other vulnerabilities such as the lack of security mechanisms, which can increase the risk to consumers and the Internet [4].

Hence, it is critical to properly test such IoT systems to fully understand their capabilities and to know the conditions under which they can operate effectively [3], [5]. Nonetheless, testing IoT deployments is a very challenging task [6] due to the intrinsic characteristics of a typical IoT system such as the vast number of devices involved and the complex nature of their inter-connectivity. These types of aspects make the creation of an appropriate test environment of real devices particularly effort-intensive and costly. The lack of test beds to trial new IoT technologies for wide-scale deployments is one of the most significant barriers that researchers and practitioners have identified to the development of the IoT industry [7]. This outlines the need for an IoT testing environment that is inexpensive, simple to configure, and easy-to-use to deploy IoT applications. However, a large amount of human effort and investment in hardware is typically required to create such environments, with real IoT deployments costing up to millions of US dollars [8] depending on the complexity.

To help tackle these problems, researchers have proposed different easy and cost-effective approaches to emulate IoT devices which range from simple computer scripts to sophisticated software platforms [9]. While there is a growing interest in using emulation tools to test IoT devices, selecting the most appropriate one remains a challenging and error-prone task. Practitioners (hereinafter referred as users) mainly lean towards those tools that have been previously used by others in the community. However, there are no formal or systematic approaches for evaluating IoT emulation environments.

To assist users in this task, our research aims to offer a requirements-based framework that enhances the assessment of IoT technological advancements. Our vision is to enable users to increase their productivity by facilitating the creation of suitable IoT testing environments in which IoT advancements can be easily tested during their research and development cycles. This is useful particularly in the early stages of research or development before the level of maturity of an IoT advancement justifies the costs that are involved when testing in a real environment (i.e., when prototyping). This also helps to accommodate small research and development teams who may not have the budget to create a hardware-based test environment of a decent size. Moreover, a framework supported by requirements engineering theory and practice [10] would help researchers to develop better prototypes and foster replicability of experiments (as emulated environments can be easily mimicked). As a first step in that direction, this work discusses a set of minimum requirements (modelled witin a conceptual framework) which are needed to properly emulate an IoT system through network virtualisation. Then, we provide research directions and open challenges that this work brings.

II. Proposed Approach

The long-term objective of this research work is to provide an efficient and effective systematic evaluation approach for network virtualisation emulators to determine which ones satisfy a set of requirements that secure the quality of an emulated IoT environment created for testing IoT systems. In this manner, users can make a more informed decision about the

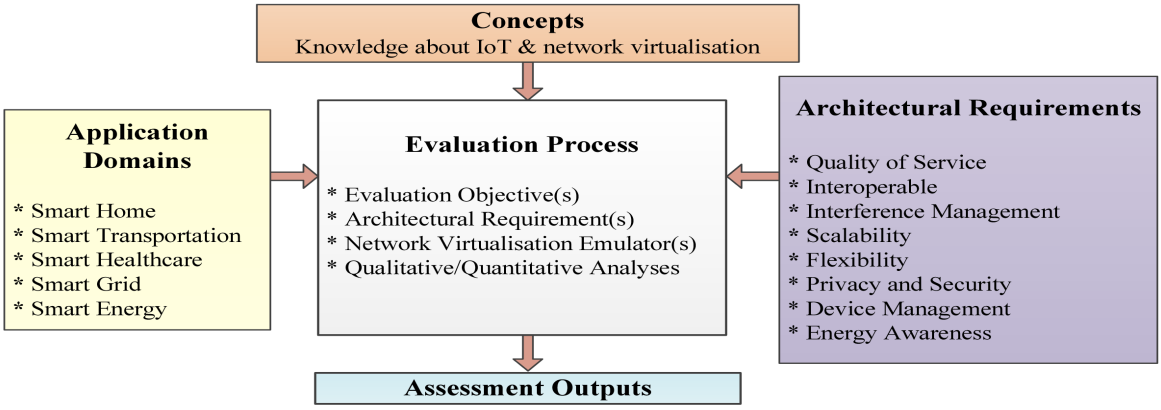

Fig. 1. Conceptual Framework to Assess the Fulfilment of IoT Architectural Requirements

selection of an appropriate emulator for their particular needs. This would facilitate the practical application of emulated IoT test environments.

We plan to develop a conceptual framework (depicted in Fig. 1) which comprises elements that we consider are the most relevant ones in IoT emulated environment evaluation. In the following paragraphs, we explain these elements.

Concepts. This consists of the broader knowledge areas that a user should be familiar with in order to understand IoT, its diverse application domains, and architectural requirements, as well as the available network virtualisation alternatives. In essence, this can be seen as the invisible groundwork (or understructure) required to effectively use the framework. For instance, concepts of IoT such as its enabling technologies (e.g., software-defined networks or protocols like Zigbee), as well as network terminology such as available network topologies (e.g., star, mesh, and point-to-point).

Architectural requirements. This is the key element of the framework, consisting of the set of requirements that a typical test environment should have in order to be IoT suitable. These requirements (described next) have been gathered from the IoT literature, initially focusing on those which are more widely-discussed in the IoT area. Each requirement has been characterised by a name, followed by a short description including its relevance (within the IoT context), as well as the benefits of fulfiling it (and/or the impacts of not fulfiling it). The identified requirements are the following:

- *Quality of Service (QoS):* Typically, this is one of the most important requirements to fulfil [11]. It is defined as the capability of an IoT system to provide quality services to users. In our context, it would also mean that the emulated IoT environment is able to achieve a similar degree of quality than the real environment. QoS is particularly important in the IoT domain because different types of applications might have different demands. For instance, a different level of quality would be required for a low data rate monitoring (scenario typically found in smart buildings to monitor variables such as the temperature or humidity of the rooms) in comparison to many real-time applications in the smart health area (e.g., a smart pacemaker would certainly have more stringent QoS requirements).
- *Interoperability:* In the IoT paradigm, this requirement is defined as the capability of an IoT system to enable the inter-operations among heterogeneous elements (e.g., different networks or devices such as Raspberry Pis). Enabling such communication across diverse types of devices (probably from different vendors) is a critical requirement in IoT nowadays [12]. In the near future, this requirement will become even more relevant, as it is expected an exponential growth in the number of interconnected IoT devices (at least 50 billions by 2020, a per the estimation of IT experts [2]).
- *Interference Management:* A highly desirable requirement of an IoT system is to efficiently handle the (potential) interference that might occur within its networks and interfaces to other systems (e.g., potentially other IoT platforms or services in the Cloud) [13]. This is because it is expected that a large percentage of the future interconnected devices will rely on some sort of wireless capabilities to be connect to the Internet (e.g., multi-radio frequencies). Under those circumstances, interference might become a major communication problem. Therefore, having interference-free capabilities will gradually become a key requirement of an IoT system to achieve reliable services.
- *Scalability:* This requirement involves the capability of managing the connectivity among a huge amount of network devices without causing any (major) performance degradation issues (e.g., caused by the overhead of keeping the components of the IoT system coordinated among each other) [14]. Furthermore, scalability can be measured by different means. For instance, using the network size (metric traditionally used to measure the size of a typical IT system, including IoT ones) or the mobility rate (i.e., how much the components of the IoT system change through time).
- *Flexibility:* This requirement involves the capability of provisioning services in such a way that a given IoT system can be flexibly programmed in order to optimise

the performance of certain functions or applications [14]. For instance, in cases of low workload (e.g., based on the number of events in the IoT system within a time period), it might be necessary to temporarily put a percentage of the IoT devices in sleep mode (e.g., a subset of the monitoring sensors) to save power consumption (to be better used in times of high workloads). Additionally, this requirement becomes more challenging within a heterogeneous environment (which has been gradually becoming a very common type of IoT system).

- *Privacy and Security:* This is another key requirement in IoT due to the potential serious consequences of having a security breach. For instance, if personal information is compromised, it might not only undermine the customers' trust in the IoT system (as well as the companies involved in the provided services), but it might also have significant legal and financial consequences. For example, infringements to the General Data Protection Regulation (GDPR), which has come into effect in Europe, can merit fines up to 20 million EUR or 4% of the annual revenues of the company [15]. For these reasons, strengthening security in an IoT environment has become an essential requirement [16]. For instance, it is usually expected that an IoT system should be secure enough to avoid devices being activated by unauthorized means. Safeguarding personal privacy and achieving such level of security can be even more challenging in many IoT components which are (heavily) resource-constrained.
- *Device Management:* This requirement refers to the capability of the components of the IoT system (i.e., the smart devices) to be both configurable and accessible remotely [17], [14]. This is required because it is not typically possible (and/or feasible) for an IoT administrator to physically access the IoT components in order to configure them (e.g., to perform a software upgrade).
- *Energy Awareness:* This requirement refers to the capability of an IoT system to be energy-aware. This is particularly relevant in IoT because most of the devices are usually resource-constrained [11]. Therefore, having this capability can help minimise energy consumption by avoiding unnecessary energy waste. For instance, putting the IoT device into an idle mode and just monitoring the wake-up events would save valuable energy. Furthermore, this might benefit the overall costs of the IoT system, as well as the quality of service (as the saved energy might be better utilised to address peaks of high workloads, or extend the life of the system's components).

Application Domains. The IoT paradigm might refer to many diverse (and considerably different) IoT systems depending on the application domain. The objective of this element is to reflect that situation into the framework by representing the different application contexts under which an IoT system might reside. This is important because, depending on the domain, the relevance (and even the applicability) of some of the architectural requirements might vary. For example, some important IoT application domains are smart transportation (e.g., to reduce traffic congestion), intelligent buildings (i.e., buildings empowered by information and communication technologies), smart homes (e.g., to allow inhabitants to control some appliances remotely), smart energy (e.g., to automatically measure energy consumption), or smart healthcare (e.g., to help diagnose diseases or monitor the health of people). The ultimate goal here is to capture the relevance of each architectural requirement per application domain. This information will be useful to have a baseline against which to compare the outcomes of evaluating the emulated IoT environment. Such baseline will also help to determine if the emulated IoT environment sufficiently conforms to the requirements needed to be useful for testing.

Evaluation process. Once the previous elements have framed an IoT scenario, the evaluation of the IoT emulated environment is conducted. In this step, the performance of the in-scope network virtualisation emulations is analysed under different qualitative and quantitative perspectives. For instance, a qualitative analysis of their capabilities might be conducted by doing a systematic literature review of the available works in academia and industry. Likewise, a quantitative analysis (probably centred on the subset of requirements of interest which have passed the qualitative analysis) is carried out to assess the degree of fulfilment of the architectural requirements. For instance, a user might be interested in assessing the QoS under the different ranges of workloads typically exhibited by a particular type of IoT system (e.g., an smart building) for a particular business objective (e.g., an anomaly detection) in order to assess if a particular network emulator (e.g., NEMU [18]) is capable of support it. Depending on the objective, a representative real environment might be required to act as a baseline against which the performance of the emulated environments are compared (e.g., in an ideal scenario, an emulated environment should achieve a similar or close level of results than a real environment for the metrics of interest).

Assessment outputs. Finally, once the evaluation results are obtained, they are consolidated. We foresee that this phase will involve comparing the degree in which the in-scope architectural requirements have been fulfiled against the needs of the particular in-scope application domain (as it reflects the user's particular IoT needs). Also, we plan to have a rating scale to make the final results of the framework more easily-digestible for users (as this strategy has proved useful in other fields [19]). We anticipate a rating scale consisting of five categories to classify the level of fulfilment of a particular requirement (i.e., Very Good, Good, Moderate, Poor, Very Poor). Such categories can serve as a guide for users to know what to expect about the utility of the emulated IoT environment w.r.t. each requirement of interest. This strategy is also inspired by the rule of thumb used for interpreting correlation coefficients (e.g., Spearman), which offer a fair and intuitive range of qualitative descriptors.

III. Conclusions and Research Agenda

This paper proposed a requirements-based framework to evaluate the suitability of emulated IoT environments to properly fulfil the requirements of an IoT test environment. The goal is to help create emulated test environments where IoT advancements can be tested before their level of maturity justify the costs involved in testing in a real IoT environment. We believe that this research can make a positive contribution towards that goal. Nevertheless, this vision paper only represents the "tip of the iceberg". There are multiple directions to extend this work. In the following paragraphs, some plans for possible future work are presented.

We plan to conduct a first instantiation of the framework by carrying out an initial case study to refine the steps to perform the evaluation process of the framework (i.e., both the quantitative and the qualitative assessments). We will initially focus on a particular application domain (e.g., anomaly detection in a smart building context), a single network virtualisation emulator (e.g., NEMU), and one architectural requirement (e.g., Quality of Service).

Although the above tasks are challenging by themselves, we consider they will only set the ground for the most interesting research aspects from a requirement engineering perspective. Such work involves the gradual (and iterative) analysis and modelling of the level of minimum fulfilment required (per architectural requirement) for each one of the application domains. Our expectation is that the application domains will need to be recursively broke down into more specific application scenarios. Such analysis will allow to generate a knowledge base where each application scenario has identified (under a set of assumptions) the subset of architecture requirements required and their level of relevance.

A similar challenge will occur with the in-scope network virtualisation emulators. Even though we plan to initially focus on one emulator, a broader set will need to be evaluated, as it is unlikely that a single emulator will be able to fulfil all architectural requirements for all application scenarios. Also, an expected (medium/long-term) contribution of this work is to produce guidelines for practitioners to know how to apply the framework to assess the suitability of a network virtualisation emulator to fulfil their particular requirements for IoT test environment, as well as the conditions under our pre-assessed emulators can be useful (e.g., preconditions, and assumptions). Developing such guidelines will require a comprehensive experimental evaluation of the emulators from an IoT perspective.

Likewise, it is expected that a single evaluation process will not be applicable to all IoT scenarios. Thus, an interesting line of research is to extend (and/or tailor) the evaluation process to make it applicable to different sets of application domains. For example, one evaluation process might be suitable to the typically more stringent requirements exhibited by smart health usages, while a different one might be used by smart home scenarios. Also, the processes might need to be tailored to suit to the specific characteristics of the architectural requirements.

Finally, another interesting research extension is to make the knowledge produced by the framework as intuitive as possible (so that it can be easily used by practitioners). Many different techniques can be used to attenuate the complexity of the derived knowledge. For instance, the information can be abstracted into simplified descriptions such as taxonomies, flow diagrams, ontologies, and characterisation tables.

Acknowledgment

This work is supported by ERC Advanced Grant no. 291652 (ASAP), and SFI Grants 10/CE/I1855, 13/RC/2094, and 15/SIRG/3501.

References

[1] "Internet of things forecasts and market estimates." [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#7efd789292d5

[2] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," Cisco, Tech. Rep.

[3] S. Brady, A. Hava, P. Perry, J. Murphy, D. Magoni, and A. O. Portillo-Dominguez, "Towards an emulated IoT test environment for anomaly detection using NEMU," in *Global Internet of Things Summit*, 2017.

[4] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," in *Int. Conf. on Service-Oriented Computing and Applications*, 2014.

[5] R. H. Weber, "Internet of things new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[6] Z. Farahmandpour, S. Versteeg, J. Han, and A. Kameswaran, "Service virtualisation of internet-of-things devices: techniques and challenges," in *Workshop on Rapid Continuous Software Engineering*, 2017.

[7] "Croke park is the worlds first internet of things stadium." [Online]. Available: https://www.siliconrepublic.com/machines/croke-park-is-the-worlds-first-internet-of-things-stadium

[8] "Internet of things: How much does it cost to build IoT solution?" [Online]. Available: http://r-stylelab.com/company/blog/iot/internet-of-things-how-much-does-it-cost-to-build-iot-solution

[9] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Communications Magazine*, vol. 49, no. 11, 2011.

[10] B. Nuseibeh and S. Easterbrook, "Requirements engineering: a roadmap," in *Future of Software Engineering*, 2000.

[11] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE wireless communications*, vol. 24, no. 3, pp. 10–16, 2017.

[12] J. Kim, J. Yun, S.-C. Choi, D. N. Seed, G. Lu, M. Bauer, A. Al-Hezmi, K. Campowsky, and J. Song, "Standard-based IoT platforms interworking: implementation, experiences, and lessons learned," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 48–54, 2016.

[13] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. Leung, "Network slicing based 5G and future mobile networks: mobility, resource management, and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[14] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, 2016.

[15] "GDPR chapters and recitals." [Online]. Available: https://gdpr-info.eu/

[16] J. L. Hernandez-Ramos, J. B. Bernabé, and A. Skarmeta, "Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 28–35, 2016.

[17] V. Autefage and D. Magoni, "NEmu: A distributed testbed for the virtualization of dynamic, fixed and mobile networks," *Computer Communications*, vol. 80, pp. 33–44, 2016.

[18] "Network emulator for mobile universes (nemu)." [Online]. Available: http://nemu.valab.net/

[19] V. Ayala-Rivera, T. Cerqueus, L. Murphy, and C. Thorpe, "Improving the Utility of Anonymized Datasets through Dynamic Evaluation of Generalization Hierarchies," in *International Conference on Information Reuse and Integration*, 2016.