


RESEARCH ARTICLE

Combinatorial methods for testing Internet of Things smart home systems

Bernhard Garn¹ | Dominik-Philip Schreiber¹ | Dimitris E. Simos¹  | Rick Kuhn² | Jeff Voas² | Raghu Kacker²

¹MATRIS, SBA Research, Vienna, Austria

²ITL, NIST, Gaithersburg, Maryland, USA

Correspondence

Dimitris E. Simos, MATRIS, SBA Research,
Floragasse 7, 1040 Vienna, Austria.
Email: dsimos@sba-research.org

Funding information

National Institute of Standards and
Technology; FFG

Summary

In this paper, we report on applying combinatorial testing to Internet of Things (IoT) home automation hub systems. We detail how to create a dedicated input parameter model of an IoT home automation hub system for use with combinatorial test case generation strategies. Further, we developed an automated test execution framework and two test oracles for evaluation purposes. We applied and evaluated our proposed methodological approach to a real-world IoT system and analysed the obtained results of various combinatorial test sets with different properties generated based on the derived input model. Additionally, we compare these results to a random testing approach. Our empirical testing evaluations revealed multiple errors in the tested devices and also showed that all considered approaches performed nearly equally well.

KEYWORDS

combinatorial testing, IoT, software testing

1 | INTRODUCTION

Several recent works in the literature point to quality, assurance and security issues in the growing Internet of Things (IoT) landscape [1–8], all describing a trend that is causing increased concern, since these types of devices and systems are deployed more and more via commercial offerings used in the daily life of many people as ubiquitous technology. Generally, when observing past publicized software failures [9] and failure studies [10], it unfortunately becomes clear that insufficient testing at many steps in the software and hardware (development) life cycle is prevalent in the global software industry. The IoT landscape is no exception and has inherited many of these problems [11,12]. The defining properties of IoT have been described in NIST SP 1900-202 [13] as follows: the close designed connection and interdependence between the physical world; software and network access. Testing such systems poses many challenges and the use of combinatorial methods to address this complexity has been suggested in Bures et al. [1]. Moreover, many works also point to privacy and trust issues within the IoT universe [14–16], and the important goal of certification faces various challenges [17]. For a recent survey on existing approaches, tools and techniques for attack and system modelling applicable to IoT, cloud computing and mobile computing, we point to Sequeiros et al. [18].

The devices produced by the IoT industry targeting consumers are usually marketed as *smart devices*, enabling prospective owners to build a *smart home* [19,20], which commonly aims to offer a plethora of useful functionality, ranging from controlling physical aspects of the home (e.g., heating, and lights and watering of plants) to the gathering and display of information (e.g., temperature and occupation). To address the problems of interconnectivity and compatibility between different kinds and types of devices from potentially many different vendors, some IoT home automation systems have been realized with a central hub, which controls all connected IoT devices in the home and is reachable in the local and sometimes also wide area network¹ for accessing its functionality.

¹This includes, but is not limited to, the Internet.