CNRS Research Project

ACIS-IoT: sAfety and seCurIty asSurrance for critical IoT systems

Applicant*: Abdelhakim Baouya

Contents

*This document is dedicated to being submitted to the Centre national de la recherche scientifique (CNRS) to showcase the research project's outcomes.

1 Brief summary of the project

A common trend in the IoT field is the emergence of many cost-effective connected devices for specific domains. However, the advent of energy-efficient protocols for low-cost communication compromises the quality of service due to potential security threats they may be exposed to. Additionally, IoT applications tend to offer high scalability to cater to user needs in terms of functionality. In certain application domains, threats and errors that were not considered during the modeling phase may arise during system execution. Unexpected events and detected threats need to be coupled with the original systems through refinement or composition to construct more sophisticated attack mitigation schemes.

2 Project Leader Information

The proposed project leverages an existing collaboration between the project participants.

Abdelhakim Baouya is an Associate Professor of Computer Science at the University of Toulouse Jean-Jaurès and a member of the IRIT-ARGOS team. His primary research interests revolve around software language engineering for software and embedded systems. He specializes in software architectures, particularly dependability, security, and Artificial Intelligence. Table 1 provides details pertaining to the project settlement.

Long Project Title	Safety and Security Assurance for critical IoT systems
Project Acronym	ACIS-IoT
Project website	https://acis-iot.github.io/
Name and CV of the project lead	Baouya Abdelhakim
Research Unit (code; acronym)	IRIT (UMR 5505)
Project Lead's Employer	University Toulouse 2 – UT2
Project Lead's Email Address	abdelhakim.baouya@irit.fr
Amount Requested from CNRS	8 K€

Table 1: Project Details

3 Full description of the project

The concepts related to IoT architecture are not easy to handle due to numerous constraints from the designer's point of view: (1)Which processes and types of IoT software artifacts should be represented at the specification level? (2) What physical elements will be part of the specification? (3)What functional aspects need to be verified and validated? (4) What are the non-functional aspects, such as safety and security, that also need to be verified? Architectural approaches coupled with model-driven design approaches are a solution to consider for the specification of IoT systems [1]. The authors in [2] emphasized the importance of a reference model to organize IoT concepts at different levels of modeling (i.e., services and communications). Security capabilities are managed at all levels of the reference model, including authorization, authentication, data privacy, and integrity. In this project, we propose to enrich the model with a new modeling layer, which is an abstraction of the application layer, representing a virtual representation of the physical world (Devices) coupled with IoT security aspects, considering system evolution and its environment.

3.1 Objectifs

To achieve the project's intent, three challenges need to be addressed. Firstly, a domain model or a metamodel is defined as a description of concepts belonging to the IoT world. Additionally, the Metamodel defines the relationships between objects; for example, a temperature (sensor) decrease triggers the heating activation (actuator). These objects will be considered as digital entities (Virtual Entities). Secondly, based on the Metamodel, architectural instances in a Semi-formal Language such as AADL/Autofocus AF3 can be instantiated. These semi-formal languages rely on the Component-Port-Connector formalism [3], which allows separation between behavior and communication. Formal approaches are also considered to handle IoT domain concepts included in the Metamodel. The BIP (Behavior-Interaction-Priority) language [4] offers the possibility to formalize software and hardware behavior (representation of devices as digital entities) as well as communication in the IoT domain. We can build formal models with parametric and reusable artifacts with the language elements and their high expressivity in artifacts (atomic components, composite components, ports, and connectors). A monitoring part is defined to capture the execution traces of the system (i.e., code generated from the M1 model). These traces are also represented in a formal model LTS or PTS [5] that will compose the original M1 model. Through execution, the generated model can represent a refinement of the M1 model due to unexpected (or rare) events such as network attacks. The preservation of functional/non-functional requirements will be verified on the M1 and M2 modeling layers. Thirdly, functional and non-functional requirements must be verified using Model Checking and theorem-proving tools. Functional requirements should express the system's state qualitatively or quantitatively at a given time, for example, Has the room temperature increased after the heating is activated? Non-functional requirements related to the security and safety of the IoT system, such as Is device access secure? These non-functional requirements are also considered critical. From a practical standpoint, emerging IoT platforms involve lightweight communication protocols (MQTT, Bluetooth, CoAP), making them vulnerable to attacks. IoT communication protocols rely on existing communication styles with well-known behavior, such as message passing or remote procedure calls. Additionally, devices that are sensitive to the environment can also lead to failures [6] that can impact software behavior and the entire IoT system. In this case, device reliability must be considered at runtime. If functional and non-functional requirements are defined in natural language, they must be formalized to enable verification.

3.2 Research methodology

The project builds upon the metamodel used in previous work [3] to model IoT systems and communication styles. We utilize OMNeT++ [7] as a modeling tool for IoT systems, encompassing sensors and actuators. Additionally, we introduce RabbitMQ [8] as a novel communication protocol. This

protocol is known for its high message consumption and manipulation capabilities, prompting us to move away from modeling the system at the level of a formal language such as PRISM. However, we still monitor the IoT systems by collecting data traces within the IoT. These collected traces are then fed into a learning algorithm, which generates appropriate formal models. Subsequently, model checking is performed on these models. We summarize the scientific outputs of the project in two key points:

- The project focuses on studying properties related to data consumption and energy usage at the level of edge servers. Specifically, we consider STRIDE threats, including attack models for data tampering. Furthermore, we also investigate the impact of security issues on energy consumption. The system models employed in this study utilize concurrent stochastic games to represent concurrent access to the edge. The results obtained provide a unique perspective on probabilistic model checking, particularly from a competitive access standpoint.
- The project investigator discovered that modeling complex IoT systems from a formal perspective leads to a state space explosion, rendering it inadequate. As a result, the modeling approach shifted to OMNeT++, which relies on the Component-Port-Connector formalism [3]. Simulation can then be performed using the resulting modeling system. Furthermore, monitored traces are collected to facilitate learning and generate an approximate model. This approximate model can be checked against functional and non-functional properties that express the absence of system attacks.

3.3 Outcomes

The outcomes encompass three dimensions: scientific, pedagogical, and industrial, as illustrated in Figure 1.

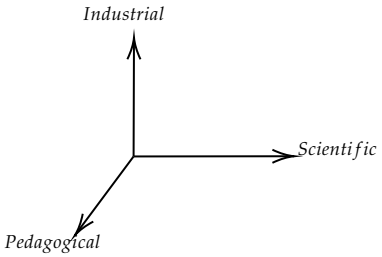

Figure 1: Project outcomes.

Scientific Publications. The research activities have resulted in the production of three papers, consisting of two journal articles and one conference paper. The details of these publications are provided below:

J1. Abdelhakim Baouya, Brahim Hamid, Levent Gürgen, and Saddek Bensalem Formal Modeling and Analysis of Tampering Attacks and Energy Consumption Effects on Edge Servers using Concurrent Stochastic Games. In Soft Computing, Springer, 2023 (Under Review).

J2. Abdelhakim Baouya, Brahim Hamid, Levent Gürgen, and Saddek Bensalem. Security Risk Assessment of the RabbitMQ Protocol through Concurrent Stochastic Games. In Internet of Things, Elsevier, 2023. (Under Review).

C1. Abdelhakim Baouya, Brahim Hamid and Saddek Bensalem. Modeling and Learning for Security Analysis of RabbitMQ Protocol. In International Conference on Engineering of Complex Computer Systems (ICECCS), 2024 (Submitted).

Pedagogical. The stemming results will be disseminated in undergraduate (L3 - Computer Science) and graduate (M1 and M2) level courses. Specifically, including practical examples in validation courses will enable students to use the provided materials and replicate the experiments. Furthermore, the L3 students will integrate the results into their supervised projects. Moreover, a scientific presentation was conducted at the Hardware Verification Group (HVG) on July 24, 2023, with the aim of presenting scientific findings to the members of the Lab.

Industrial. During the project, we collaborated with Kentyou [1], a company that utilizes a specific gateway for routing data through different protocols. To accomplish this, we leveraged the Sensinat Description Language (SDL). In addition, we applied a game model interpretation to the routing protocol, allowing us to model malicious behavior effectively.

Artefacts. The experiments described in this research project are publicly available and fully reproducible. The source code can be accessed from the public website [2]. The website provides detailed instructions on replicating the experiments.

4 Acknowledgement

Please consider that some of the outputs from the research project are currently under review, and the reviewers are still examining the publications. If you require further information regarding the publication of the results, please feel free to contact us.

References

[1] A. Lekidis, E. Stachtiari, P. Katsaros, M. Bozga, and C. K. Georgiadis, "Model-based design of iot systems with the bip component framework," *Software: Practice and Experience*, vol. 48, no. 6, pp. 1167–1194, 2018.

[2] A. Baouya, S. Chehida, S. Bensalem, L. Gürgen, R. Nicholson, M. Cantero, M. Diaznava, and E. Ferrera, "Deploying warehouse robots with confidence: the brain-iot framework's functional assurance," *The Journal of Supercomputing*, Jul 2023.

[3] Q. Rouland, B. Hamid, and J. Jaskolka, "Formal specification and verification of reusable communication models for distributed systems architecture," *Future Generation Computer Systems*, vol. 108, pp. 178–197, 2020.

[4] A. Basu, S. Bensalem, M. Bozga, J. Combaz, M. Jaber, T.-H. Nguyen, and J. Sifakis, "Rigorous component-based system design using the BIP framework," vol. 28, no. 3, pp. 41–48.

[5] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM 4.0: Verification of probabilistic real-time systems," in *Proc. 23rd International Conference on Computer Aided Verification (CAV'11)* (G. Gopalakrishnan and S. Qadeer, eds.), vol. 6806 of *LNCS*, pp. 585–591, Springer, 2011.

[6] J. Schiffer, C. A. Hans, T. Kral, R. Ortega, and J. Raisch, "Modeling, analysis, and experimental validation of clock drift effects in low-inertia power systems," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 7, pp. 5942–5951, 2017.

[7] OMNeT++, "Discrete Event Simulator." https://omnetpp.org/, Since 2008. [Accessed: January-2023].

[8] "RabbitMQ - amqp 0-9-1," 2019.

[1] https://kentyou.com/

[2] https://acis-iot.github.io/