Formal Methods for Internet of Things: a Concise Classification

Ibtissem Talamali[1], Razika Lounas[1], and Mohamed Mezghiche[1]

[1] ***LIMOSE Laboratory, Computer Science Department, Faculty of Sciences University of M'hamed Bougara of Boumerdes, Independency Avenue, 35000 Algeria, i.talamali@univ-boumerdes.dz***

Abstract

The Internet of Things (IoT) has now become a key technology that can span several technology areas, from data discovery and processing to networking and data analysis. It is used in many applications ranging from home security and factory automation to healthcare provision and autonomous driving. Many IoT devices can connect and communicate at the same time, and this exchange of data enables better decision-making in an increasingly complex environment. However, for some safety-critical systems, any failure of a function can have very serious consequences. This is why we need to adopt appropriate and effective testing techniques to detect errors and flaws in the system design and correct them as soon as possible. The formal method is one of the crucial methods for detecting possible weaknesses and vulnerabilities at an early stage of the design in order to verify the correctness of the system. This article provides an overview of the use of model checking and theorem proving to establish correctness properties on IoT systems.

Keywords: Internet of Things, formal methods, model checking, theorem proving.

1 Introduction

The Internet of Things (IoT) is a new paradigm aimed at creating connectivity for "everything" that can support minimal storage and processing power. This allows these connected elements to work together anywhere, anytime and in any form within an application to cover different domains, health, transport infrastructure, smart home, smart shopping, e-commerce, etc. Ensuring the accuracy, reliability and the correctness of IoT systems is critical to advancing IoT projects. Sufficient verification before the actual introduction of the IoT system is very important to discover and improve system design errors and flaws as soon as possible. Moreover, some of these errors may cause catastrophic loss of money, time, or even human life. To help overcoming such problems, it has been suggested to use formal methods in the development of critical systems. Formal methods is a method using mathematic based languages, techniques, and tools for specifying and verifying such systems. It is an important means to improve the system safety and reliability. In fact, in various stages of development trend of formal methods gradually integrated into the software development process, from the demand analysis, function description (description), (Architecture / design, programming algorithm), testing and maintenance[15]. As an efficient means of pre-deployment inspection of Internet of Things systems, formal methods have received widespread attention in recent years[25].
In this paper, we provide a survey of the application of formal methods in Internet of Things systems. The objective of this paper is three fold:

- classify research papers according to the used formal techniques;
- gaining insight about the objective of applying formal methods on IoT through the established properties;
- draw recommendations about a future use at the light of the surveyed papers.

The rest of this paper is organized as follows. Section 2 presents the related Work. Internet of Things with architectures and protocols are presented in Section 3. In Section 4 the use of formal methods for IoT is described. The conclusion and discussion is given in Section 5.

2 Related work

Several researchers endeavored to analyse the application of formal methods for Internet of Things systems. In [11], the authors reviewed researches about the formal verification of IoT protocols. The authors

distinguished the main objectives for the formal verification: functional checks, security properties and gave suggestions for enhanced schemes and implementation checks of protocols."

In [6], the authors presented tools used in formal verification for distributed systems. These tools: Isabelle/HOL, Coq, Verdi, and TLA+, are compared in terms of functionality, interface, and application. The authors gave some recommendations of use according to the aim of formalisation. In [12], the authors proposes to formalize things information in three theories: graphs, sets, and abstract expressions. The description is related to things information in several situations such as coded by UID, stored in RFID. In [20], the authors studied the use of formal verification in IoT from an application point of view. The survey considered model checking , process algebraic, and automated theorem proving in different application areas such as monitoring, health, and protocols. The survey find out that security issues are the most studied issue with model checking. Existing surveys helped us in the assimilation of formal methods and techniques in the context of IoT, but there is an evident lack in response to the increasing need to establish formal correctness using theorem proving with regard to model checking. Our survey complements the existing surveys by bringing new points to the discussion about the established properties using theorem proving.

3 Internet of Things in Critical Applications

In recent years, several definitions of the Internet of Things have appeared. The ITU (International Telecommunication Union) defines IoT as:" a global infrastructure for the information society that enables advanced services by interconnecting objects (physical or virtual) through existing or evolving interoperable information and communication technologies". This section details the concept of IoT through its architecture, protocols, and applications.

3.1 IoT Architecture

Due to the fast development of IoT, it became essential to have a reference architecture that could standardize system design and facilitate communication and interoperability between different IoT ecosystems [18]. IoT architecture design involves many factors such as networking, communication, processes, etc. Scalability, extensibility, and interoperability amongst devices must all be taken into consideration while creating the IoT architecture. Due to the fact that things can move and need to interact with others in real time, the IoT architecture should be adaptive to make devices interact with others dynamically and support communication between them. In addition, the IoT should possess the decentralized and heterogeneous nature[7]. There is no single consensus on which IoT architecture is universally adopted. Different architectures have been proposed by different researchers[3]. The layered architecture of the Internet of Things is illustrated as assumed by the ITU-T (International Telecommunication Union - Telecommunications Standardization Sector) and is composed of four layers(Figure **??**).

1. **Sensor Layer (Device Layer/ Perception Layer)** : It consists of data sensors in various forms such as RFID tags, IR sensors or other sensor networks that could detect temperature, humidity, speed and location, etc. This layer collects useful information from objects from related sensors and converts the information into digital signals that are then transmitted to the network layer for further action[5].

2. **Network Layer** This layer is responsible for the reliable transmission of data generated in the perception layer as well as the assurance of connected inter-object connectivity and between smart objects and other Internet hosts. On the other hand, a massive volume of data will be produced by these tiny sensors, which requires a robust and efficient wired or wireless network infrastructure as a means of transport[16].

3. **Service and Middleware Layer** This layer receives data from the Network layer. Its purpose is service management and data storage. It also processes information and makes decisions automatically based on the results and passes the output to the next layer[13].

4. **Application Layer** This layer provides the different types of services requestd by the customer that depends on his specific use case adopted. For example, if the smart home is the use case, the customer may request specific parameters such as heating, ventilation and air conditioning (HVAC) measurements or temperature and humidity values[13].

3.2 IOT Applications domains

The potential applications of IoT are numerous reaching every area of the daily lives of individuals, businesses and society as a whole. This section provides an overview of the main application areas of IoT.

- **Smart Cities** A Smart City is a city that monitors and integrates the conditions of all critical infrastructure including road bridges, tunnels, rail/metro, airports, seaports, even large buildings, etc. Structural health, Digital video surveillance, fire management, intelligent and weather-adaptive lighting are examples of smart cities applications.
- **Smart Health** The IoT plays an important role in the health sector, putting in place new technologies not only in hospitals, but also in the workplace and at your fingertips, whether to keep track of medical records, monitor vital signs or treat remotely. There are some IoT technologies in this field[16] : Patient monitoring, medical refrigerators control, pharmaceuticals monitoring, and chronic disease management systems.
- **Smart industry** The Industrial Internet of Things (IIoT) or the factory of the future is the fourth industrial revolution or Industry 4.0 (started in Germany, 2010). It is basically characterized by intelligent automation and integration of new technologies in factories such as sensors and smart tools in general allow collecting more data about the manufacturing process to check compliance and optimize production in real time[14].
- **Smart Agriculture** The automation of agricultural events is moving the agricultural sector from a static and manual situation to a dynamic and intelligent automation, to facilitate farmer's tasks, such as the irrigation, fertilizer application and others, resulting in improved production with reduced human efforts. Some of the objectives of IoT usage in this sector include: Control of the microclimatic conditions to maximize the production of fruits and vegetables and their quality, control humidity and temperature levels to prevent microbial contaminants, and identification of animals grazing in open pastures.
- **Smart energy** The IoT allows the countless devices that make up the electricity grid to share information in real time to improve the efficiency of energy distribution and management, such as [16] : monitoring and analysis of wind turbine and power plant energy flows, and AC-DC power control, and monitoring and optimisation of solar power plant performance.

4 Formal methods and internet of Things

In complex systems, it is very important to ensure that there are no dangerous or unexpected behaviors. Therefore, errors need to be identified early in the system lifecycle. In such cases, formal methods have proven to be the most appropriate technique to ensure and guarantee the absence of bugs and defects[9]. A formal method is a mathematically-based technique and formal logic used in computer science to describe properties of hardware and/or software systems. A method is formal if it has a sound mathematical basis, typically given by a formal specification language[22]. This basis provides the means of precisely defining notions like consistency and completeness and, more relevantly, specification, implementation, and correctness. It provides the means of proving that a specification is realizable, proving that a system has been implemented correctly, and proving properties of a system without necessarily running it to determine its behavior[23]. In fact, there are several formal languages and techniques that allow different types of properties to be inspected at different levels of the development process.

4.1 Formal verification

Formal Verification is a promising method to provide security guarantees by mathematically ascertaining the correctness of designs using a diverse set of mathematical and logical methods. These methods are particularly useful in order to get quantitative statements about safety and security properties of digital systems[11]. There are two major state of the art approaches to formal verification: theorem proving and model checking.

1. **Model checking** Model checking is an automated approach to verify that a model of a finite state system satisfies a formal specification of requirements to the system. In this approach the models describe how the state of the system may evolve over time, and the requirements are some constraints on how the state of the system is allowed to evolve over time. Tools that automatically perform model checking are called model checkers[10]. In other way, the user specifies the system through a set of states connected by a set of transitions. Then, an algorithm is executed to enumerate the possible execution states of the system. This algorithm verifies if the model satisfies the different properties[9]. Among the model checking tools, we mention: SPIN, DIVINE, PAT, and UPPAAL. Now, we describe some related work in current literature. In [25], the authors proposes a hierarchical formal modeling approach for IoT systems that focuses on user behavior and improves pre-deployment correctness checking and reliability analysis. The hierarchical modeling of the three-layer architecture of the IoT system perception layer, middle layer, and application layer has been completed, and the model verification tool PAT was used to analyze and verify the model from aspects such as security, accessibility, and system consistency.

   In [19], the authors proposed a formal verification of interoperability in IoT systems. The proposal answers the question about consistency of IoT solutions in terms of interoperability. The system is formalized in terms of web services concepts. The authors used TLA+ specification and the TLA Checker to establish the interoperability property. In [24], the authors proposed a probabilistic model checking approach for run-time verification of industrial IoT. The approach combines sensor level and data-driven models to establish the property of quantified trustworthiness of sensors through the study of several types of sensor data faults. The framework is evaluated using a CNC turn-mill machine with the PRISM tool.

2. **Theorem proving**

   Theorem proving is a technique by which both the system and its desired properties are expressed as formulas in some mathematical logic. This logic is given by a formal system, which defines a set of axioms and a set of inference rules. Theorem proving is the process of finding a proof of a property from the axioms of the system. Steps in the proof appeal to the axioms and rules, and possibly derived definitions and intermediate lemmas. Theorem provers are increasingly being used today in the mechanical verification of safety-critical properties of hardware and software designs[2]. Examples of some notable proof checkers are MetaMath and Mizar. Examples of some notable interactive theorem provers are the PVS, Isabelle/ HOL, ACL2 and Coq. The rest of this part, we outline a few related works in the current literature.

   In [17] The authors define a formal model of real-time networks, in the field of embedded networks, based on the NC theory (computational network) a method of analysis of temporal properties based on the algebra of min-plus dioids. And for that, they formalized the proofs related to the network calculation in Coq to ensure guaranteed delays in embedded real-time networks. In this article [8], the authors propose a formal approach for the validation and certification of smart city systems by formalizing them as cyber-physical systems. These have been formalized as finite state machines and interpreted and formally verified by the Coq proof assistant. this article show that the Coq proof assistant plays an essential role in software validation in the smart cities domain. In this work [1], The authors present the IoT Conflict Checker (IoTC2) as a formal method to ensure the safe behavior of controllers and actuators in IoT systems. The study includes the definition of security policies, their implementation in Prolog for logical completeness, the implementation of detection policies in the Matlab Simulink environment, creating an intelligent home environment in Simulink to demonstrate conflict and test scaling, efficiency and accuracy in a simulated environment. In [21] the authors proposed a refinement-based approach for modeling IoT design patterns, which takes advantage of formal methods by the specification of design pattern models with the Event-B method. They checked the design correctness and verify properties of IoT design patterns using the model checking to check the correctness of the behavior of the pattern and absence of deadlocks with ProB tool and theorem proving to ensure the consistency of an Event-B pattern model with the Rodin platform. Finally, they illustrated their approach with a case study in healthcare domain.

At the end of this section, we have classified the articles already mentioned according to the formal method used, the tool and the properties checked (Table 1). This classification provides a clear vision of existing approaches from 2016 to 2020 to formally refine and verify IoT systems against a set of criteria.

Years	Approach	Formal method	Tools	Verified properties
2016	[4]	Theorem Proving	HOL	Evaluate the coverage properties
2018	[8]	Theorem Proving	The proof assistant CoQ	System proprieties
2018	[19]	Model checking	TLA Checker	interoperability property
2019	[17]	Theorem Proving	The proof assistant CoQ	Temporal properties
2019	[1]	Theorem Proving	Prolog tool	Security policies properties
2020	[25]	Model checking	PAT tool	Security, Accessibility ,Consistency
2020	[24]	Model checking	PRISM tool	quantified trustworthiness property
2023	[21]	Model checking/ Theorem proving	Rodin/ProB	Structural consistency, behavioral features, absence of deadlocks.

Table 1: Classification of pertinent works about IoT systems formal verification

5 Conclusion

The Internet of Things (IoT) has become an important part of our lives. However, the increasing complexity of IoT systems makes it essential to ensure their reliability and correctness. Formal methods have emerged as a powerful tool for verifying the correctness of these systems. In this paper, we have presented a survey of the use of formal methods, specifically model checking and theorem proving, in IoT systems. We have classified the research papers according to the formal techniques used and discussed the objectives of applying these methods. Our survey has shown that formal methods can significantly improve the safety and reliability of IoT systems. We recommend that formal methods be used in the early stages of IoT system design to identify errors and to ensure their correctness. Finally, we believe that this paper will stimulate further research in the use of formal methods in the development of IoT systems.

References

[1] Abdullah Al Farooq, Ehab Al-Shaer, Thomas Moyer, and Krishna Kant. Iotc 2: A formal method approach for detecting conflicts in large scale iot systems. In *Symposium on integrated network and service management*, pages 442–447. IEEE, 2019.

[2] Edmund M Clarke and Jeannette M Wing. Formal methods: State of the art and future directions. *ACM Computing Surveys (CSUR)*, 28(4):626–643, 1996.

[3] Sakina Elhadi, Abdelaziz Marzak, Nawal Sael, and Soukaina Merzouk. Comparative study of iot protocols. *Smart Application and Data Analysis for Smart Cities (SADASC'18)*, 2018.

[4] Maissa Elleuch, Osman Hasan, Sofiene Tahar, and Mohamed Abid. Formal probabilistic analysis of a wsn-based monitoring framework for iot applications. In *Formal Techniques for Safety-Critical Systems: 5th International Workshop, FTSCS 2016, Tokyo, Japan, November 14, 2016*, pages 93–108. Springer, 2017.

[5] M Umar Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, and Talha Kamal. A review on internet of things (iot). *International journal of computer applications*, 113(1):1–7, 2015.

[6] Anna Fatkina, Oleg Iakushkin, Dmitry Selivanov, and Vladimir Korkhov. Methods of formal software verification in the context of distributed systems. In *Computational Science and Its Application: 19th International Conference, Saint Petersburg, Russia, July 1–4, Proceedings, Part II 19*, pages 546–555. Springer, 2019.

[7] Pradyumna Gokhale, Omkar Bhat, and Sagar Bhat. Introduction to iot. *International Advanced Research Journal in Science, Engineering and Technology*, 5(1):41–44, 2018.

[8] Erick Simas Grilo and Bruno Lopes. Formalization and certification of software for smart cities. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE, 2018.

[9] Marwa Hachicha, Riadh Ben Halima, and Ahmed Hadj Kacem. Formal verification approaches of self-adaptive systems: A survey. *Procedia Computer Science*, 159:1853–1862, 2019.

[10] Anne E Haxthausen. An introduction to formal methods for the development of safety-critical applications. *Technical University of Denmark*, 2010.

[11] Katharina Hofer-Schmitz and Branka Stojanović. Towards formal verification of iot protocols: A review. *Computer Networks*, 174:107233, 2020.

[12] Yinghui Huang and Guanyu Li. Descriptive models for internet of things. In *2010 International Conference on Intelligent Control and Information Processing*, pages 483–486. IEEE, 2010.

[13] Muhammad Azhar Iqbal, Sajjad Hussain, Huanlai Xing, and Muhammad Ali Imran. *Enabling the internet of things: fundamentals, design and applications*. John Wiley & Sons, 2020.

[14] AKSA Karima, Khayreddine BOUHAFNA, Souleymen BELAYATI, and Dina DJEGHAR. Vers une nouvelle révolution industrielle: Industrie 4.0. *Revue Méditerranéenne des Télécommunications*, 11(1), 2021.

[15] Chunlin Kuang and Weiling Li. Application of formalization method in construction zigbee technology and rfid system in internet of things. In *2015 International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC-15)*, pages 874–879. Atlantis Press, 2015.

[16] Keyur K Patel, Sunil M Patel, and P Scholar. Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, 6(5), 2016.

[17] Lucien Rakotomalala, Marc Boyer, and Pierre Roux. Formal verification of real-time networks. In *JRWRTC 2019, Junior Workshop RTNS 2019*, 2019.

[18] Imad Saleh. Les enjeux et les défis de l'internet des objets (ido). *Internet des objets*, 1(1):5, 2017.

[19] Vadym Shkarupylo, Ravil Kudermetov, Tetiana Golub, Olga Polska, and Mariia Tiahunova. Towards model checking of the internet of things solutions interoperability. In *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, pages 465–468. IEEE, 2018.

[20] Alireza Souri and Monire Norouzi. A state-of-the-art survey on formal verification of the internet of things applications. *Journal of Service Science Research*, 11(1):47–67, 2019.

[21] Imen Tounsi, Abdessamad Saidi, Mohamed Hadj Kacem, and Ahmed Hadj Kacem. Internet of things design patterns modeling proven correct by construction: Application to aged care solution. *Future Generation Computer Systems*, 148:395–407, 2023.

[22] Jeannette M Wing. *What is a formal method?* Carnegie-Mellon University. Department of Computer Science, 1989.

[23] Jeannette M Wing. A specifier's introduction to formal methods. *Computer*, 23(9):8–22, 1990.

[24] Xin Xin, Sye Loong Keoh, Michele Sevegnani, and Martin Saerbeck. Dynamic probabilistic model checking for sensor validation in industry 4.0 applications. In *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pages 43–50. IEEE, 2020.

[25] Lei Yu, Yang Lu, Benhong Zhang, Lei Shi, Fangliang Huang, Ya Li, and Yulian Shen. Hierarchical formal modeling of internet of things system oriented to user behavior. In *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pages 282–289. IEEE, 2020.