Communications in Computer and Information Science 1564

More information about this series at https://link.springer.com/bookseries/7899

Imen Jemili · Mohamed Mosbah (Eds.)

Distributed Computing for Emerging Smart Networks

Third International Workshop, DiCES-N 2022
Bizerte, Tunisia, February 11, 2022
Proceedings

Springer

Editors

Imen Jemili
University of Carthage
Zarzouna Bizerte, Tunisia

Mohamed Mosbah
University of Bordeaux
Bordeaux, France

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-3-030-99003-9 ISBN 978-3-030-99004-6 (eBook)
https://doi.org/10.1007/978-3-030-99004-6

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the proceedings of the third Workshop in Distributed Computing for Emerging Smart Networks (DiCES-N 2022). The workshop was held on February 11, 2022, and took place virtually in order to ensure the safety of participants due to the COVID-19 pandemic. We received a total of 14 submissions, of which five were accepted for publication, and an invited paper. The acceptance rate was therefore approximately 35.7%. Reviewing was single-blind, where each paper was assigned to at least four reviewers.

Nowadays, the smart city concept is a rising vision of cities that seeks to enable broad connectivity and systems inter-operability and offer sustainable solutions and prevalent security. The smart cities are the nuclei from which smart networks and a new generation of solutions can be implemented to address their inherent challenges such as traffic congestion, air pollution, difficulty in waste management, scarcity of resources, and human health concerns. Smart cities rest on innovative paradigms and integrate new technologies into their infrastructures to enable their management and provide the basis for these innovative solutions. Smart living, smart mobility, smart people, smart environment, smart economy, and smart government are the main components of smart cities; these applications rely on the deployment of some sensing and tracking infrastructures for data collection from embedded sensors in smart devices, such as smart phones and connected cars. Thus, gathering data from the physical environment relies on a huge number of real-world physical entities, endowed with sensing, computation, and communication capabilities, and to some extent with some level of intelligence; this data will be forwarded, then stored, processed, and analyzed remotely to offer personalized services and support the proper functioning of these applications.

In this context, the Internet of Things (IoT), information and communication technologies (ICT), cloud computing and fog/edge computing are considered as key enabling technologies. In fact, IoT becomes a reality; a lot of applications in many domains rely on the new innovative IoT solutions. However, the fast-growing number of connected devices will require a new level of infrastructure deployment, both in terms of wired and wireless connectivity. Thus, the complex nature of IoT is reflected through the multitude of independent cyber-physical systems that operate with their own infrastructures and cooperate to achieve smart city sustainability through service reliability and security.

The workshop tackled issues relating to the design, development, and evaluation of distributed systems, platforms, and architectures for cyber-physical systems in the context of smart cities. The program included two sessions.

Session 1 was dedicated to emerging networks and communications, mainly wireless sensor networks (WSNs). In fact, the wide range of applications, potential uses, and great popularity of WSNs make them widely recognized as a major technology enabling the concept of smart cities. These networks are considered as the main sensing tool to collect contextual and environmental data and to observe real-world events, which will be exploited by upper-layer applications. This gathered data must be transmitted, shared, stored, and, finally, analyzed. This process requires the deployment of different technologies in each of these phases.

Designing the WSNs information life cycle in smart cities is a first step in understanding this complex process by identifying its phases and challenges, and the technologies involved. Thus, WSNs must coexist and collaborate with other networks, involving several technologies to support properly the functioning of the multiple smart applications. Depending on the application area, these networks may comprise a huge number of battery-operated sensor nodes, which are constrained in terms of energy and processing capabilities. Since it is imperative to keep such networks operative as long as possible, energy remains among the main issues. Replenishing the battery energy of the sensors can be difficult, expensive, or even impossible. Even the recourse to energy harvesting technology to capture energy from ambient power sources is costly and may be unaffordable for some applications. Moreover, communication through a wireless medium is inherently unreliable and is also prone to errors and link failures. Thus, the multiple challenges facing WSNs are related to the intrinsic characteristics of these networks and/or introduced by their large-scale deployment in the context of smart cities, as each smart application comes with its own challenges. Overcoming these issues is required as WSNs are a building block for data acquisition and innovative applications.

Session 1 covered the deployment of WSNs in smart farming applications and e-health. The recourse to WSNs in the field of agriculture has become a necessity for high added value and tangibility. Through smart agricultural applications, the optimization of agricultural production and resource utilization is targeted. Indeed, plants, trees, and shrubs can also suffer from insect infestations, diseases, and nutrient deficiencies. In addition, due to external factors, the losses to farming as a whole can be enormous. IoT is helping to overcome these challenges, mainly relating to extreme weather, climate change, and environmental impacts. With the introduction of IoT in agriculture, advanced sensors can be employed to collect data in real time, facilitating effective decision making.

The adoption of IoT has helped farmers in many activities such as monitoring water levels in reservoirs to increase the efficiency of the entire irrigation process and tracking seed growth. Indeed, smart farming applications allow the optimization of crop production and resource use. They cover a wide range of crop types monitored in diversified facilities, including greenhouse monitoring, vineyards, horticulture, and soil moisture monitoring in irrigation applications. However, the monitored field may extend over a large area, such as a greenhouse or a grassland, requiring the deployment of many sensors spread over the area. Thus, the sensor nodes need to cooperate to transmit the sensed data to a central node, called the sink node. The recourse to a routing protocol, suitable for the smart farming application, is essential to be able to deliver the data and commands correctly and in a timely manner; the automation process proposed by any smart farming application can exploit this information to achieve its objectives. Identifying the requirements of routing protocols in WSNs in the context of smart farming allows the selection of the most appropriate protocol for this application.

The suitability of a given protocol or technology depends mainly on the targeted application; the e-health domain was the second topic area discussed in Session 1 and wireless body area networks (WBANs) were introduced. WBANs are now widely deployed to provide effective and promising e-health solutions, such as ambulatory monitoring and assisted living at home. Indeed, technological advances have brought considerable and essential improvements to the health sector. Thank to biosensors, a patient's vital signs can be gathered around the clock and sent wirelessly to a mobile phone for self-remote monitoring or to a remote server for further analysis and storage. However, with the wide spread use of tablets, smartphones, and smartwatches and the integration of sensors in mobile devices, a huge amount of data is being collected. We rely on machine learning to deal with this large amount of data, which is beyond the capabilities of traditional data processing tools and techniques. By analyzing large volumes of data, machine-learning technology can assist healthcare professionals in generating accurate medical solutions tailored to individual characteristics.

Session 2 dealt with cyber security of connected devices. Despite the benefits brought by IoT, many issues remain unresolved and constitute a potential impediment to the uptake of IoT applications and the implementation of large-scale smart environments. Indeed, with the proliferation of smart devices and the rapid growth of high-speed networks, the Internet of Things has become an area of incredible impact and growth. The various connected smart devices, ranging from simple wearable accessories to large machines containing sensing chips, offer a panoply of services to facilitate the daily life of the citizen, ensure public safety, enhance public services, improve the productivity of companies, etc. These smart devices are starting to invade our lives; they collect a multitude of data relevant to services, in addition to contextual data that can improve data analysis and decision-making. However, this data can also be used to profile users and infiltrate their privacy. As IoT devices are easy to hack and compromise and are deployed in external and uncontrolled locations, new potential attack surfaces, that can be exploited by malicious cybercriminals, have emerged. In this context, traditional security solutions cannot be applied due to the intrinsic constraints of these intelligent systems and networks and their remarkable heterogeneity. Therefore, security has become one of the main concerns of this technology.

The manipulation of sensitive user information can lead to considerable damages, as in the field of e-health or intelligent transport. For instance, connected and self-driving cars present an attractive solution to major transport problems: improving road safety, alleviating traffic congestion, etc. To this end, vehicles will have to cooperate and exchange various information related to their position, behavior (deceleration, lane change, etc.), or the occurrence of external events (pedestrian, obstacle, etc.). However, to provide such safety-critical services, it is essential that communications between road users are secure. Healthcare applications also handle sensitive data related to patients; personal health data refers to a large range of information, including basic medical data (vital sign readings, patient status, and medical history), sensitive mental health data, or administrative data such as patient identity, address, etc. Due to the complexity of smart environments, preserving data privacy, confidentiality, and integrity is a challenging task. In this context, many emerging technologies have been employed to provide high-performance, privacy-friendly and secure architectures, such as the two tackled concepts, blockchain and software defined networking (SDN).

The key principle of blockchain rests on the notion of collective trust, without the intervention of a centralized trusted third party. Blockchain technology is a form of distributed ledger technology where each participant is responsible for the security of the network. This global and shared database is maintained among all these nodes, since each node in the network keeps all the transactions in the blockchain and participates in their verification and evolution. Once a transaction has been validated, no participant can sign or modify it. Thus, this distributed, synchronized, and duplicated ledger provides the same coherent, updated, and secure view to all participants in the network. Although this new system enables the exchange of data and money with low transaction costs and a privacy protection mechanism, it is relevant to identify the associated challenges and potential areas of application in different fields, such as e-health and vehicle networks as discussed in Session 2.

SDN also introduces many opportunities to protect the network more efficiently and flexibly, and to secure large-scale heterogeneous networks, by decoupling the data forwarding plane from the control plane. Thanks to the global view of a special node, called the SDN controller, such a node is able to provide network devices with the appropriate configuration, forwarding decisions, and security strategies. This functional behavior allows fast response to security threats, granular traffic filtering, and dynamic security policies. However, SDN can also come with its own security concerns. Indeed, through controllers, SDN enables centralized control and global visibility over the entire network. Even though a hybrid architecture involves multiple controllers, the failure of a single controller would put the entire network at risk; a component with malicious behavior can compromise the operation of the entire network. If the controllers in the network were attacked, the entire network would be paralyzed. In addition, threats to system vulnerabilities can affect the privacy, integrity, and confidentiality of the system, thus reducing the security, performance, and efficiency of the network. It is worthwhile to investigate the different threats against SDN and identify which part of the SDN paradigm they target and which aspects of security are affected, such as availability, integrity, and confidentiality.

We are grateful for the support provided by the many people who contributed to making DiCES-N 2022 success. Naturally, the workshop could not take place without the efforts made by the organizing committee who helped us to organize and publicize the event, particularly the Program Committee chairs (Sabra Mabrouk, Akka Zemmari, and Soumaya Dahi) and the publicity chair (Emna Ben Salem).

We are thankful to the members of the Programm Committee for providing their valuable time and helping us to review the received papers. We would also like to thank the authors for submitting and then revising a set of high-quality papers. Finally, we express our sincere gratitude to Springer for giving us the opportunity to publish the workshop proceedings, and we appreciate the support and advice provided by the editorial team.

February 2022

Imen Jemili
Mohamed Mosbah

Organization

General Chairs

Imen Jemili	University of Carthage, Tunisia
Mohamed Mosbah	Bordeaux INP, France

Program Committee Chairs

Sabra Mabrouk	University of Carthage, Tunisia
Soumaya Dahi	University of Carthage, Tunisia
Akka Zemmari	University of Bordeaux, France

Publicity Chair

Emna Ben Salem	University of Carthage, Tunisia

Program Committee

Salma Batti	University of Carthage, Tunisia
Raoudha Beltaifa	University of Manouba, Tunisia
Anis Ben Aicha	University of Carthage, Tunisia
Lotfi Ben Othmane	Iowa State University, USA
Ismail Berrada	Mohammed VI Polytechnic University, Morocco
Shridhar Devamane	TECSEC Technologies, India
Kamal E. Melkemi	University of Batna 2, Algeria
Ahmed El Oualkadi	Abdelmalek Essaâdi University, Morocco
Matthieu Gautier	University of Rennes 1, France
Tahani Gazdar	University of Jeddah, Saudi Arabia
Wilfried Yves Hamilton Adoni	Hassan II University of Casablanca, Morocco
Maha Jebalia	SUP'COM, Tunisia
Sondes Kallel	University of Paris-Saclay, France
Moez Krichen	Albaha University, Saudi Arabia
Hela Mahersia	University of Carthage, Tunisia
Bacem Mbarek	Masaryk University, Czech Republic
Nadhir Messai	University of Reims Champagne-Ardenne, France
Tarik Nahhal	Hassan II University of Casablanca, Morocco
Neha Pattan	Google, USA
Ashish Rauniyar	SINTEF Digital, Norway

Gautam Srivastava	Brandon University, Canada
Eiad Yafi	University of Kuala Lumpur, Malaysia
Anis Yazidi	Oslo Metropolitan University, Norway

Contents

Emerging Networks and Communications

Cyber Security of Connected Objects