Computer Communications 89–90 (2016) 1–4

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Editorial

Special issue on “Internet of Things: Research challenges and Solutions”

1. Introduction

The past decade has witnessed a significant proliferation of Internet-capable devices. While its greatest commercial impact has been in the area of consumer electronics, with the smartphone revolution and the uptake of wearables, connecting humans is only part of a greater trend toward the interconnection of the physical world with the digital world.

While the Internet is a communication network connecting people to information, the Internet of Things (IoT) is an interconnected ecosystem of uniquely addressable physical objects with varying degrees of sensing, processing, and actuation capabilities, sharing the ability to communicate and interoperate through the Internet as their common denominator [1].

With the IoT paradigm, sensor-equipped devices can provide fine-grained information about the physical world, allowing cloud-based resources to extract value from such information and possibly make decisions to be implemented by actuator-equipped devices, blurring the line between the IoT and the broader concept of Cyber-Physical Systems [2–4], which does not necessarily presuppose Internet connectivity per se.

The vagueness of the term “Things”makes it hard to define the ever expanding boundaries of the IoT, but at the same time offers a clear idea of its heterogeneity and its virtually limitless application potential. This has spawned very encouraging projections from market analysts and corporate players who envision a multi-trillion dollar market for the IoT.

As commercial success materializes, the IoT continues to offer a seemingly boundless supply of opportunities for both business and research. This special issue of Computer Communications is dedicated to the latter, offering a varied collection of research contributions to cutting-edge themes within the IoT space. This special issue complements [5], which focused on architectures, protocols, and services.

2. Research areas

As the IoT is the result of heterogeneous technologies used to sense, collect, act, process, infer, transmit, notify, manage, and store data, there are many research challenges to be addressed spanning several research areas (see Fig. 1). In the following, we will discuss the key research directions for each area.

2.1. Monitoring and sensing

Although monitoring and sensing technologies have achieved some level of maturity, they continue to evolve, in particular with regard to energy-efficiency and form factor. Since tags and sensors are expected to be constantly active to acquire real-time data, energy-efficiency is crucial to lifetime extension. At the same time, recent advances in miniaturization and nanotechnology/biotechnology have enabled the development of sensors and actuators at the nano-scale, fleshing out Kris Pister’s smart dust vision [6,7].

Given the heterogeneity of sensing technologies and the increasingly large number of devices, IPv6 has been proposed as solution to identify IoT objects independently of the sensing technology. However, what is missing is standard solutions to map the address scheme of the sensing technologies into IPv6 addresses. Additionally, efficient services for retrieving the object associated with a global identifier, and vice-versa, are also required.

2.2. M2M communication

While there already exist IoT-oriented communication protocols, such as MQTT [8] and CoAP [9], we still do not have a standard for a truly open IoT. While every object needs connectivity, not every object needs to be Internet-capable, but only capable enough to get its data to a gateway. As for the most suitable wireless technology for any given object, there are many options, ranging from Bluetooth Low Energy and LoRa [10] to IEEE 802.15.4, but it is unclear whether they will continue to cover the whole range of IoT connectivity needs going forward.

Following the recent trend of pushing processing and storage towards the edge of the network, Software Defined Networking (SDN) and Network Function Virtualization (NFV) techniques promise to deliver the next generation of networks [11,12]. The inclusion of virtualization capabilities in the network nodes (e.g., on access routers) brings the service representation (e.g., cloud services) closer to the users, resulting in a better match for the application requirements as well as lower costs.

2.3. Process, analysis, management

Processing, analyzing and managing data is extremely challenging due to the heterogeneity and the scale of collected data. The current trend is to use centralized solutions to offload data

http://dx.doi.org/10.1016/j.comcom.2016.04.024

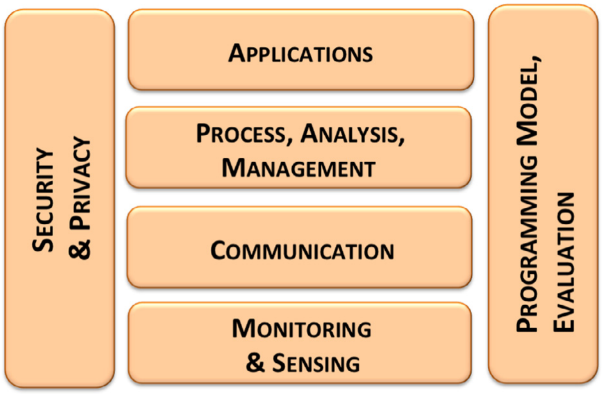

Fig. 1. Overview of the IoT research areas.

and perform computationally intensive tasks on a global cloud platform. However, there is an increasing concern that traditional cloud architectures may not be able to transfer the massive volume of data produced and consumed by IoT devices and to support the associated computational load while meeting timing constraints. To this end, emerging solutions such as Fog Computing and Mobile Cloud Computing rely on edge processing to address this challenge [13–15].

Another research direction that is gaining momentum is the application of Information Centric Networking to the IoT. As information-centric solutions natively support the efficient retrieval of content and the access to services and applications by name, they seem valuable and scalable solutions to access, transfer and manage the generated content and its distribution. Obviously, several challenges arise: for instance, how to efficiently extend the ICN paradigm beyond the edge of the fixed network, how to include IoT static and mobile devices, and how to allocate ICN functionality on resource-constrained devices [16,17].

The management of devices is also of paramount importance, and is a complex problem that includes numerous actions to be taken on devices with different available resources. While the lightweight implementation of traditional management solutions [18] might be beneficial in those scenarios where many devices already use traditional solutions, OMA-DM and OMA Lightweight M2M (LWM2M) are mainly targeted to scenarios where there are only IoT constrained devices. However, how to efficiently integrate these protocols into the IoT architecture are open issues [19]. Moreover, what is missing is open software solutions spanning security and device management that allow IoT devices and systems to seamlessly discover each other, dynamically communicate and interact with nearby devices regardless of brand, communication layer, platform type, or operating system.

How to perform essential services such as dynamic service composition and efficient service discovery is a further IoT challenge. There exist several approaches currently under investigation, including the aforementioned Fog Computing or, alternatively, the application of context-aware computing, as most of IoT services and applications are tailored to the specific context and users' needs. A further solution relies on the Social Internet of Things [20,21], i.e., the social network paradigm applied to objects, that allows to independently establish trust social relationships among objects that are then exploited to make services more efficient.

2.4. Applications

Due to the range and breadth of IoT technologies, application development employs a diverse set of approaches and models ranging from device-centric embedded systems to fully distributed real-time approaches. IoT applications need to address a number of issues that are intrinsic to the nature of the IoT, including real-time communication, the presence of both sensing and actuation with humans in the loop, and the distributed and heterogeneous nature of the IoT.

While none of these requirements are unique and many of them have already been explored individually by the research community, they must often be addressed jointly by IoT applications.

2.5. Security and privacy

Researchers have long known of the vulnerabilities that currently exist in numerous IoT devices [22]. Recent attacks on IoT systems demonstrate the need for comprehensive security architectures that protect systems and data from end to end. The threat of stepping stone attacks that exploit weaknesses in individual devices to enter a system and gain access to devices that are more secure from the outside is a driving motivation for comprehensive security solutions. This includes research in efficient applied cryptography for both system and data security [23], non-cryptographic techniques for security [24], and frameworks for helping developers more easily develop secure systems on heterogeneous devices [25]. Even with cryptographic security services that are capable of running on resource constrained IoT devices, we need research to enable users of all skill levels to securely deploy and use IoT systems despite the limited user interfaces available with most IoT devices.

Recent privacy research in IoT has focused on the important trade-offs between security, functionality, and privacy. These trade-offs often focus on balancing the system's ability to use information, authenticate and establish trust in users, and hide sensitive user information. Since IoT devices often record large amounts of personal information, users need to understand what is being recorded, how it is being used, who it is available to, and who has control of it. This information is critical as IoT devices that are deployed by casual users and these systems become more connected to cloud-based services that the user seldom has significant control over.

2.6. Programming models, evaluation

Due to the diverse nature of the IoT, there has been a variety of approaches to programming IoT applications. For IoT applications and services that are focused on edge devices, and work within a single control domain, e.g., a factory or machine, programming models tend to exploit the principles of real time and embedded computing. For general-purpose applications such as Smart Buildings, or Smart Cities [26], researchers have explored the use of centralized cloud based programming models with traditional synchronous and asynchronous APIs [27] as well as more distributed approaches such as Cloudlets or Fog Computing.

One promising approach recently explored by the research community is the use of data-flow programming models to process streams of events from IoT devices asynchronously. To accommodate the distributed nature of IoT applications, Distributed Data-Flow (DDF) has been proposed as a potential solution and is currently an active research area [28]. Reactive Programming, also built on a data-flow model, has recently gained traction in the IoT community with various research groups exploring dynamic and functional variants in the search for a general purpose IoT programming model.

3. Contributions on this special issue

This special issue includes fourteen contributions covering a wide subset of the IoT research areas discussed in Section 2. The

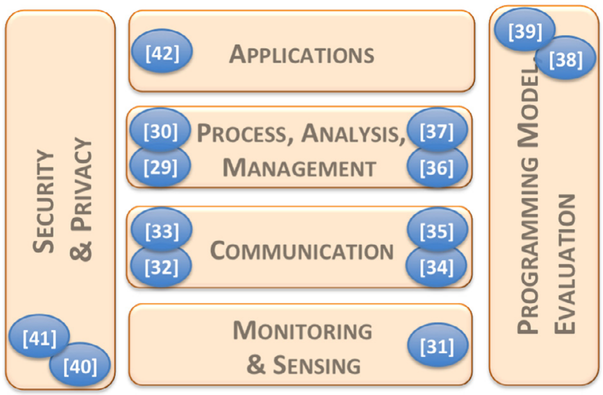

Fig. 2. Distribution of the accepted papers on IoT research areas.

selected papers have been chosen among forty-four submissions from around the globe and after a rigorous review process with two rounds of reviews by the Guest Editors and several expert reviewers. The accepted papers confirm the increasing interest by the research community in this field. Fig. 2 shows the distribution of the accepted papers across the research areas discussed in the previous section.

This special issue opens with a set of surveys that provide an overview of the current solutions in various IoT research areas. Specifically, [29] focuses on the middleware platforms currently available for IoT, and identifies the key features and missing functionality of the most representative platforms. In [30], the authors report a systematic literature review of the integration of the IoT with Cloud Computing. Alongside their classification, the authors identify numerous open challenges and potential directions that can be relevant for future research in this field. In [31], the authors present an extensive survey of the technologies used for detecting indoor daily indoor activities, and provide a taxonomy for activity recognition.

A second set of papers deals with communication issues from different technological perspectives. In [32], the authors investigate the feasibility of multimedia communication in resource-constrained devices, and propose an application solution that exploits Bluetooth Low Energy (LE) to enable efficient streaming services. In [33], interference problems caused by adjacent channels in WiFi-based WLANs are discussed, and the authors present an interference-aware self-optimizing (IASO) WiFi solution to mitigate the above issues. Congestion problems that may arise when a large number of IoT devices try to connect to the network are investigated in [34]. Specifically, the authors propose a novel LTE uplink scheduler that controls the congestion level dynamically based on traffic information as well as the allocations logs available on the device. The last paper in this group proposes a routing protocol where paths are determined based on content [35]. The main idea is to create application-specific overlay trees based on the content, and to route correlated data to intermediate nodes to increase data aggregation while reducing network congestion and latency. Notably, the paper illustrates the integration of the proposed solution with the IETF RPL protocol.

Two papers explore the efficient integration of the Information Centric Networking (ICN) paradigm with the IoT and treat this emerging research direction from different perspectives. Specifically, paper [36] proposes an ICN-based communication solution to retrieve the resources available within a local area network. The key role is assumed by the gateway, which is responsible for resource naming and acts as a proxy translating incoming resources requests into ICN messages. The proposed solution is totally compliant with the *European Telecommunications Standards Institute (ETSI)* M2M specifications, thus enabling remote applications to access the resources available within the local area network. The authors of [37] focus on efficient and flexible mechanisms to improve service discovery in the IoT. To this end, they propose a system based on Named Data Networking that is enriched with semantic similarity techniques to deal with the significant and growing diversity of the service descriptions. The discovery brokerage and the semantic matching engine are the two entities designed to match the incoming queries to the available services.

Novel flexible software frameworks for the easy development, integration, and communication of IoT devices and applications are the subjects of papers [38] and [39]. Specifically, the authors of [38] propose a new programming model for the Arduino platform that enables the integration and management of multiple micro-controllers over numerous communication channel (e.g., socket connections, bridging, MQTT-based publish-subscribe messaging). The platform presented in [39] provides software tools to develop IoT fault-tolerant applications while supporting the heterogeneity of IoT devices. It relies on the Erlang programming language that helps programmers to write concise code with a relatively low debugging and maintenance effort.

This special issue also includes two papers that deal with security and privacy issues. Paper [40] proposes a hybrid access control system that integrates WNSs with the Internet under the IoT umbrella. Specifically, as the two environments are characterized by different crypto-systems, the proposal relies on the adoption of a heterogeneous cryptosystem and a signcryption solution that enables a seamless and secure communication. The implementation and experimental evaluation of a lightweight multi-OS security platform is the focus of paper [41]. The proposed solution, designed for IoT smart parking applications, relies on Zero Knowledge Proof protocols to hide sensitive user information while guaranteeing proper authentication, and on Elliptic Curve Cryptography to reduce the computational burden.

Finally, paper [42] explores the application of the IoT to the e-health space, proposing a system that employs face recognition and facial expression analysis techniques to determine the emotional state of patients and provide them the correct in-home treatment.

Acknowledgments

We wish to thank all the authors for submitting their work to this special issue. We also wish to express our gratitude to our reviewers, who contributed to improving the quality of the papers through their efforts.

We are extremely grateful to Marco Conti, Editor-in-Chief of the Elsevier Computer Communications, for giving us the possibility of serving the community with this special issue. We also appreciate his constant advice and support as well as the assistance received by the editorial team of the journal.

References

[1] E. Borgia, The Internet of Things vision: key features, applications and open issues, Comput. Commun. 54 (2014) 1–31.
[2] R. Poovendran, Cyber-physical systems: close encounters between two parallel worlds [point of view], Proc. IEEE 98 (8) (2010) 1363–1366.
[3] M. Conti, S.K. Das, C. Bisdikian, M. Kumar, L.M. Ni, A. Passarella, G. Roussos, G. Tröster, G. Tsudik, F. Zambonelli, Looking ahead in pervasive computing: challenges and opportunities in the era of cyber-physical convergence, Pervasive Mob. Comput. 8 (1) (2012) 2–21.
[4] K.-J. Park, R. Zheng, X. Liu, Cyber-physical systems: milestones and research challenges, Comput. Commun. 36 (1) (2012) 1–7.
[5] M. Whlisch, D. Turgut, T. Pfeifer, A.P. Jayasumana, Special issue: Current and future architectures, protocols, and services for the Internet of Things, Comput. Commun. 74 (2016) 1–2. Editorial
[6] I. Akyildiz, J. Jornet, The Internet of nano-Things, IEEE Wirel. Commun. 17 (6) (2010) 58–63.

[7] I.F. Akyildiz, M. Pierobon, S. Balasubramaniam, Y. Koucheryavy, The Internet of bio-nano Things, IEEE Commun. Mag. 53 (3) (2015) 32–40.
[8] International Business Machines Corporation (IBM) – Eurotech, MQTT V3.1 Protocol Specification, 2010, (http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html).
[9] C. Bormann, A.P. Castellani, Z. Shelby, CoAP: an application protocol for billions of tiny Internet nodes, IEEE Internet Comput. 16 (2) (2012) 62.
[10] M. Bor, J. Vidler, U. Roedig, LoRa for the Internet of Things, in: Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, EWSN '16, 2016, pp. 361–366.
[11] A. Manzalini, R. Minerva, F. Callegati, W. Cerroni, A. Campi, Clouds of virtual machines in edge networks, IEEE Commun. Mag. 51 (7) (2013) 63–70.
[12] R. Ravindran, X. Liu, A. Chakraborti, X. Zhang, G. Wang, Towards software defined ICN based edge-cloud services, in: Proceedings of the 2013 IEEE 2nd International Conference on Cloud Networking, CloudNet, 2013, pp. 227–235.
[13] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the Internet of Things, in: Proceedings of the First Edition of the ACM Workshop on Mobile Cloud Computing, MCC '12, 2012, pp. 13–16.
[14] C. Shi, M.H. Ammar, E.W. Zegura, M. Naik, Computing in cirrus clouds: the challenge of intermittent connectivity, in: Proceedings of the First Edition of the ACM Workshop on Mobile Cloud Computing, MCC '12, 2012, pp. 23–28.
[15] E. Borgia, R. Bruno, M. Conti, D. Mascitti, A. Passarella, Mobile edge clouds for information-centric IoT services, in: Proceedings of the Twenty-First IEEE Symposium on Computers and Communications, ISCC '16, 2016.
[16] A. Lindgren, F.B. Abdesslem, B. Ahlgren, O. Schelen, A. Malik, Applicability and tradeoffs of information-centric networking for efficient IoT, Technical Report, IETF, ICN Research Group Internet Draft, 2015.
[17] E. Baccelli, C. Mehlis, O. Hahm, T.C. Schmidt, M. Wählisch, Information-centric networking in the IoT: experiments with NDN in the wild, in: Proceedings of ACM Conference of Information-Centric Networking, 2014, pp. pp.77–86.
[18] A. Sehgal, V. Perelman, S. Kuryla, J. Schonwalder, Management of resource constrained devices in the Internet of Things, IEEE Commun. Mag. 50 (12) (2012) 144–149.
[19] C.A.L. Putera, F.J. Lin, Incorporating OMA lightweight M2M protocol in IoT/M2M standard architecture, in: Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things, WF-IoT, 2015, pp. 559–564.
[20] L. Atzori, A. Iera, G. Morabito, M. Nitti, The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: concept, architecture and network characterization, Comput. Netw. 56 (16) (2012) 3594–3608.
[21] L. Atzori, A. Iera, G. Morabito, From "smart objects" to "social objects": the next evolutionary step of the Internet of Things, IEEE Commun. Mag. 52 (1) (2014) 97–105.
[22] A. Cui, S.J. Stolfo, A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan, in: Proceedings of the 26th ACM Annual Computer Security Applications Conference, ACSAC '10, 2010, pp. 97–106.
[23] D. Dinu, Y.L. Corre, D. Khovratovich, L. Perrin, J. Groschłdl, A. Biryukov, Triathlon of lightweight Block Ciphers for the Internet of Things, 2015, (Cryptology ePrint Archive, Report 2015/209). http://eprint.iacr.org/.
[24] B. Lagesse, M. Kumar, M. Wright, AREX: an adaptive system for secure resource access in mobile P2P systems, in: Proceedings of the 2008 Eighth International Conference on Peer-to-Peer Computing, 2008, pp. 43–52.
[25] B. Lagesse, M. Kumar, J.M. Paluska, M. Wright, DTT: a distributed trust toolkit for pervasive systems, in: Proceedings of IEEE International Conference on Pervasive Computing and Communications, PerCom 2009, 2009, pp. 1–8.
[26] D.G. Gomes, A. Förster, Introduction to the special issue on Green engineering, Comput. Electr. Eng. 45 (C) (2015) 141–142.
[27] R. Lea, M. Blackstock, City hub: a cloud-based IoT platform for smart cities, in: Proceedings of the 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, CloudCom, 2014, pp. 799–804.
[28] N.K. Giang, M. Blackstock, R. Lea, V.C.M. Leung, Developing IoT applications in the fog: a distributed dataflow approach, in: Proceedings of the 2015 5th International Conference on the Internet of Things, IOT, 2015, pp. 155–162.
[29] J. Mineraud, O. Mazhelis, X. Su, S. Tarkoma, A gap analysis of Internet-of-Things platforms, Comput. Commun. (2016).
[30] E. Cavalcante, J. Pereira, M.P. Alves, P. Maia, R. Moura, T. Batista, F.C. Delicato, P.F. Pires, On the interplay of Internet of Things and cloud computing: a systematic mapping study, Comput. Commun. (2016).
[31] P. Woznowski, D. Kaleshi, G. Oikonomou, I. Craddock, Classification and suitability of sensing technologies for activity recognition, Comput. Commun. (2016).
[32] M. Gentili, R. Sannino, M. Petracca, BlueVoice: voice communications over Bluetooth Low Energy in the Internet of Things scenario, Comput. Commun. (2016).
[33] I.-G. Lee, M. Kim, Interference-aware self-optimizing Wi-Fi for high efficiency Internet of Things in dense networks, Comput. Commun. (2016).
[34] A.M. Maia, D. Vieira, M.F. de Castro, Y. Ghamri-Doudane, A fair QoS-aware dynamic LTE scheduler for machine-to-machine communication, Comput. Commun. (2016).
[35] Y. Jin, S. Gormus, P. Kulkarni, M. Sooriyabandara, Content centric routing in IoT networks and its integration in RPL, Comput. Commun. (2016).
[36] M. Amadeo, O. Briante, C. Campolo, A. Molinaro, G. Ruggeri, Information-centric networking for M2M communications: design and deployment, Comput. Commun. (2016).
[37] J. Quevedo, M. Antunes, D. Corujo, D. Gomes, R.L. Aguiar, On the application of contextual IoT service discovery in information centric networks, Comput. Commun. (2016).
[38] G. Barbon, M. Margolis, F. Palumbo, F. Raimondi, N. Weldin, Taking Arduino to the Internet of Things: the ASIP programming model, Comput. Commun. (2016).
[39] A. Sivieri, L. Mottola, G. Cugola, Building Internet of Things software with ELIoT, Comput. Commun. (2016).
[40] F. Li, Y. Han, C. Jin, Practical access control for sensor networks in the context of the Internet of Things, Comput. Commun. (2016).
[41] I. Chatzigiannakis, A. Vitaletti, A. Pyrgelis, A privacy-preserving smart parking system using an IoT elliptic curve based security platform, Comput. Commun. (2016).
[42] L.Y. Mano, B.S. Faial, L.H. Nakamura, P.H. Gomes, G.L. Libralon, R.I. Meneguete, G.P. Filho, G.T. Giancristofaro, G. Pessin, B. Krishnamachari, J. Ueyama, Exploiting IoT technologies for enhancing health smart homes through patient identification and emotion recognition, Comput. Commun. (2016).

Eleonora Borgia*
Institute of Informatics and Telematics (IIT), Italian National Research Council (CNR), Pisa, Italy

Danielo G. Gomes
Grupo de Redes de Computadores, Engenharia de Software e Sistemas (GREat), Departamento de Engenharia de Teleinformatica, Universidade Federal do Cear (UFC), Fortaleza-CE, Brazil

Brent Lagesse
Computer and Software Systems, University of Washington, Bothell, USA

Rodger Lea
Department of Computing and Communications, Lancaster University, UK

Daniele Puccinelli
Institute for Information Systems and Networking (ISIN), University of Applied Sciences of Southern Switzerland (SUPSI), Switzerland

*Corresponding author.
E-mail addresses: eleonora.borgia@iit.cnr.it (E. Borgia), danielo@ufc.br (D.G. Gomes), lagesse@uw.edu (B. Lagesse), rodgerl@ece.ubc.ca (R. Lea), daniele.puccinelli@supsi.ch (D. Puccinelli)