Lecture Notes in Computer Science 9688

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7408

Elvira Albert · Ivan Lanese (Eds.)

Formal Techniques for Distributed Objects, Components, and Systems

36th IFIP WG 6.1 International Conference, FORTE 2016
Held as Part of the 11th International Federated Conference on Distributed Computing Techniques, DisCoTec 2016
Heraklion, Crete, Greece, June 6–9, 2016
Proceedings

Springer

Editors
Elvira Albert
Complutense University of Madrid
Madrid
Spain

Ivan Lanese
University of Bologna/INRIA
Bologna
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-39569-2 ISBN 978-3-319-39570-8 (eBook)
DOI 10.1007/978-3-319-39570-8

Library of Congress Control Number: 2016939908

LNCS Sublibrary: SL2 – Programming and Software Engineering

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Foreword

The 11th International Federated Conference on Distributed Computing Techniques (DisCoTec) took place at Aquila Atlantis Hotel in Heraklion, Greece, during June 6–9, 2016. It was organized by the Institute of Computer Science of the Foundation for Research and Technology – Hellas and the University of Ioannina, Greece. The DisCoTec series is one of the major events sponsored by the International Federation for Information Processing (IFIP). It comprises three conferences:

- COORDINATION, the IFIP WG 6.1 International Conference on Coordination Models and Languages
- DAIS, the IFIP WG 6.1 International Conference on Distributed Applications and Interoperable Systems
- FORTE, the IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components and Systems

Together, these conferences cover a broad spectrum of distributed computing subjects, ranging from theoretical foundations and formal description techniques to systems research issues.

Each day of the federated event began with a plenary speaker nominated by one of the conferences. The three invited speakers were Tim Harris (Oracle Labs, UK), Catuscia Palamidessi (Inria, France), and Vijay Saraswat (IBM T.J. Watson Research Center, USA).

Associated with the federated event were also two satellite workshops, that took place during June 8–9, 2016:

- The 9th Workshop on Interaction and Concurrency Experience (ICE) with keynote lectures by Uwe Nestmann (Technische Universität Berlin, Germany) and Alexandra Silva (University College London, UK)
- The Final Public Workshop from the LeanBigData and CoherentPaaS projects

Sincere thanks go to the chairs and members of the Program and Steering Committees of the involved conferences and workshops for their highly appreciated efforts. Organizing DisCoTec 2016 was only possible thanks to the dedicated work of the Organizing Committee, including George Baryannis (Publicity Chair) and Vincenzo Gulisano (Workshops Chair), with excellent support from Nikos Antonopoulos and Alkis Polyrakis of PCO-Convin. Finally, many thanks go to IFIP WG 6.1 for sponsoring this event, to Springer *Lecture Notes in Computer Science* for their support and sponsorship, and to EasyChair for providing the refereeing infrastructure.

April 2016 Kostas Magoutis

Preface

This volume contains the papers presented at FORTE 2016, the 36th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems. This conference was organized as part of the 11th International Federated Conference on Distributed Computing Techniques (DisCoTec) and was held during June 5–7, 2016 in Heraklion (Greece).

The FORTE conference series represents a forum for fundamental research on theory, models, tools, and applications for distributed systems. The conference encourages contributions that combine theory and practice, and that exploit formal methods and theoretical foundations to present novel solutions to problems arising from the development of distributed systems. FORTE covers distributed computing models and formal specification, testing, and verification methods. The application domains include all kinds of application-level distributed systems, telecommunication services, Internet, embedded, and real-time systems, as well as networking and communication security and reliability.

The conference received 44 submissions of authors from 21 countries. All full papers were reviewed by at least three members of the Program Committee. After careful deliberations, the Program Committee selected 18 papers for presentation. In addition to these papers, this volume contains an abstract of the invited talk by an outstanding researcher, Catuscia Palamidessi, on "Verifying Generalized Differential Privacy in Concurrent Systems."

The conference would not have been possible without the enthusiasm and dedication of the general chair, Kostas Magoutis (University of Ioannina, Greece), and the support of the Organizing Committee with George Baryannis (University of Huddersfield, UK) and Vincenzo Gulisano (Chalmers University of Technology, Sweden). For the work of the Program Committee and the compilation of the proceedings, the EasyChair system was employed; it freed us from many technical matters and allowed us to focus on the program, for which we are grateful. Conferences like FORTE rely on the willingness of experts to serve in the Program Committee; their professionalism and their helpfulness were exemplary. Finally, we would like to thank all the authors for their submissions, their willingness to continue improving their papers, and their presentations!

April 2016

Elvira Albert
Ivan Lanese

Organization

Program Committee

Erika Abraham	RWTH Aachen University, Germany
Gul Agha	University of Illinois at Urbana-Champaign, USA
Elvira Albert	Complutense University of Madrid, Spain
Ahmed Bouajjani	LIAFA, University Paris Diderot, France
Frank De Boer	CWI, The Netherlands
Lars-Ake Fredlund	Universidad Politécnica de Madrid, Spain
David Frutos Escrig	Universidad Complutense de Madrid, Spain
Stefania Gnesi	ISTI-CNR, Italy
Kim Guldstrand Larsen	Aalborg University, Denmark
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Einar Broch Johnsen	University of Oslo, Norway
Ivan Lanese	University of Bologna, Italy, and Inria, France
Antónia Lopes	University of Lisbon, Portugal
Hernan Melgratti	Universidad de Buenos Aires, Argentina
Massimo Merro	University of Verona, Italy
Peter Olveczky	University of Oslo, Norway
Luca Padovani	Università di Torino, Italy
Anna Philippou	University of Cyprus
Arnd Poetzsch-Heffter	University of Kaiserslautern, Germany
Kostis Sagonas	Uppsala University, Sweden
Alexandra Silva	University College London, UK
Jean-Bernard Stefani	Inria, France
Emilio Tuosto	University of Leicester, UK
Mahesh Viswanathan	University of Illinois, Urbana-Champaign, USA

Additional Reviewers

Abdoullah, Houssam
Akkoorath, Deepthi
Akshay, S.
Alborodo, Raul Nestor Neri
Aronis, Stavros
Azadbakht, Keyvan
Basile, Davide
Benac Earle, Clara
Bezirgiannis, Nikolaos
Bliudze, Simon
Brunnlieb, Malte
Charalambides, Minas
Chatain, Thomas
Cruz-Filipe, Luís
De Gouw, Stijn
Fábregas, Ignacio
Jensen, Peter Gjøl
Lang, Frederic
Lange, Julien
Lienhardt, Michael

Löscher, Andreas
Mariegaard, Anders
Mariño, Julio
Marti-Oliet, Narciso
Mathur, Umang
Mauro, Jacopo
Meyer, Roland
Mikučionis, Marius
Montenegro, Manuel
Nyman, Ulrik
Palmskog, Karl
Petri, Gustavo
Pichon, Jean
Rodriguez, Ismael
Roohi, Nima
Rubio, Albert
Sammartino, Matteo
Sandur, Atul
Semini, Laura
Stumpf, Johanna Beate
Suzuki, Tomoyuki
Taankvist, Jakob Haahr
Tamarit, Salvador
Tiezzi, Francesco
Toninho, Bernardo
Van Glabbeek, Rob
Weber, Mathias
Zeller, Peter

Verifying Generalized Differential Privacy in Concurrent Systems (Abstract of Invited Talk)

Catuscia Palamidessi

INRIA Saclay and LIX, École Polytechnique

Privacy is a broad concept affecting a variety of modern-life activities. As a consequence, during the last decade there has been a vast amount of research on techniques to protect privacy, such as communication anonymisers [8], electronic voting systems [7], Radio-Frequency Identification (RFID) protocols [12] and private information retrieval schemes [6], to name a few.

In recent years, a new framework for privacy, called *differential privacy* (DP) has become increasingly popular in the area of statistical databases [9–11]. The idea is that, first, the access to the data should be allowed only through a query-based interface. Second, it should not be possible for the adversary to *distinguish*, from the answer to the query, whether a *certain individual is present or not* in the database. Formally, the *likelihood* of obtaining a certain answer should not change too much (i.e., more than a factor e^{ϵ}, where ϵ is a parameter) when the individual joins (or leaves) the database. This is achieved by adding *random noise* to the answer, resulting in a trade-off between the privacy of the mechanism and the utility of the answer: the stronger privacy we wish to achieve, the more the answer needs to be perturbed, thus the less useful it is. One of the important features of DP is that it does not depend on the side information available to the adversary. Related to this, another important advantage is that DP is robust with respect to composition attacks: by combining the results of several queries, the level of privacy of every mechanism necessarily decreases, but with DP it declines in a controlled way. This is a feature that can only be achieved with randomized mechanisms: With deterministic methods, such as *k-anonymity* [13, 14], composition attacks may be catastrophic.

DP has proved to be a solid foundation for privacy in statistical databases. Various people have also tried to extend it to other domains. The problem is that DP assumes that the disclosed information is produced by aggregating the data of multiple individuals. However, many privacy applications involve only a single individual, making differential privacy inapplicable.

In our team, we have addressed this issue by defining an extended DP framework in which the indistinguishability requirement is based on an arbitrary notion of distance (d_x-privacy, [3]). In this way we can naturally express (protection against) privacy threats that cannot be represented with the standard notion, leading to new applications of the differential privacy framework. In particular, we have explored applications in

This work is partially supported by the Large Scale Initiative CAPPRIS.

geolocation [1, 2] and smart metering [3]. In the context of geolocation, the problem of the correlated data becomes particularly relevant when we consider traces, which usually are composed of a large amount of highly related points. We addressed this issue using *prediction functions* [5], obtaining encouraging results.

Another shortcoming of the current approaches to privacy is that they are only applicable when the public information is well delimited and acquired in finite in time. Unfortunately, in most situation the source of public information is not necessarily bound, and some additional information can always be revealed in the future. At present, there are no techniques to verify privacy guarantees in situations in which the revelation of public information is not bound in time. This is a serious limitation, especially given that most of the systems which we use nowadays have an interactive nature, and usually are not under the control of the user.

In our team, we have started exploring a possible approach to this problem by defining a generalized version of the bisimulation distance based on the Kantorovich metric [4]. The standard Kantorovich lifting is based on an additive notion of distance, hence it is not suitable to capture d_x-privacy, that, like differential privacy, is inherently multiplicative. In contrast, our framework generalizes the Kantorovich lifting to arbitrary distances, and can therefore be applied also to d_x-privacy.

We show that the standard results extend smoothly to the generalized case, and that a bound on the generalized bisimulation distance is also a bound for the distance on traces, which guarantees the soundness of the method for proving DP. Furthermore, we provide an efficient method to compute it based on a dual form of the Kantorovich lifting. Finally, we explore an Hennessy-Milner-like logical characterization of our bisimulation distance, and we show how it can be use for reasoning about DP.

References

1. Andrés, M.E., Bordenabe, N.E., Chatzikokolakis, K., Palamidessi, C.: Geo-indistinguishability: differential privacy for location-based systems. In: Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS 2013), pp. 901–914. ACM, New York (2013)
2. Bordenabe. N.E., Chatzikokolakis, N., Palamidessi, C.: Optimal geo-indistinguishable mechanisms for location privacy. In: Proceedings of the 21th ACM Conference on Computer and Communications Security (CCS 2014) (2014)
3. Chatzikokolakis, K., Andrés, M.E., Bordenabe, N.E., Palamidessi, C.: Broadening the scope of differential privacy using metrics. In: De Cristofaro, E., Wright, M. (eds.) PETS 2013, LNCS, vol. 7981, pp. 82–102. Springer, Heidelberg (2013)
4. Chatzikokolakis, K., Gebler, D., Palamidessi, C., Xu, L.: Generalized bisimulation metrics. In: Baldan, P., Gorla, D. (eds.) CONCUR 2014, LNCS, vol. 8704, pp. 32–46. Springer, Heidelberg (2014)
5. Chatzikokolakis, K., Palamidessi, C., Stronati, M.: A predictive differentially-private mechanism for mobility traces. In: De Cristofaro, E., Murdoch, S.J. (eds.) PETS 2014, LNCS, vol. 8555, pp. 21–41. Springer, Heidelberg (2014)

6. Chor, B., Goldreich, O., Kushilevitz, E., Sudan, M.: Private information retrieval. In: Proceedings of 36th Annual Symposium on Foundations of Computer Science, pp. 41–50. IEEE (1995)
7. Delaune, S., Kremer, S., Ryan, M.: Verifying privacy-type properties of electronic voting protocols. J. Comput. Secur. **17**(4), 435–487 (2009)
8. Dingledine, R., Mathewson, N., Syverson, P.F.: Tor: the second-generation onion router. In: Proceedings of the 13th USENIX Security Symposium, pp. 303–320. USENIX, (2004)
9. Dwork, C.: Differential privacy. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) CALP 2006, Part II, LNCS, vol. 4052, pp. 1–12. Springer, Heidelberg (2006)
10. Dwork, C.: A firm foundation for private data analysis. Commun. ACM, **54**(1), 86–96 (2011)
11. Dwork, C., Lei, J.: Differential privacy and robust statistics. In: Mitzenmacher, M. (ed.) Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC), Bethesda, MD, USA, May 31 – June 2, pp. 371–380. ACM (2009)
12. Juels, A.: Rfid security and privacy: a research survey. IEEE J. Sel. Areas Commun. **24**(2), 381–394 (2006)
13. Samarati, P.: Protecting respondents' identities in microdata release. IEEE Trans. Knowl. Data Eng. **13**(6), 1010–1027 (2001)
14. Samarati, P., Sweeney, L.: Generalizing data to provide anonymity when disclosing information (abstract). In: Proceedings of the ACM SIGACT–SIGMOD–SIGART Symposium on Principles of Database Systems, Seattle, Washington, June 1–3, 1998, p. 188. ACM Press (1998)

Contents