Computational Social Networks

Ajith Abraham
Editor

Computational Social Networks

Security and Privacy

Springer

Editor
Dr. Ajith Abraham
Machine Intelligence Research Labs
(MIR Labs)
Scientific Network for Innovation
and Research Excellence
Auburn, WA
USA

ISBN 978-1-4471-4050-4 ISBN 978-1-4471-4051-1 (eBook)
DOI 10.1007/978-1-4471-4051-1
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2012944711

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Computational Social Network (CSN) is a new emerging field that has overlapping regions from Mathematics, Psychology, Computer Sciences, Sociology, and Management. E-mails, blogs, instant messages, social network services, wikis, social bookmarking, and other instances of what is often called social software illustrate ideas from social computing.

Social network analysis is the study of relationships among social entities. Very often, all the necessary information is distributed over a number of websites and servers, which brings several research challenges from a data mining perspective. Recently, privacy concerns with social network services have become a much-publicized topic since the creation and increasing popularity of social networking sites such as Myspace and Facebook, etc. Issues relating to stalking, identity theft, sexual predators, and employment consistently arise, as well as the ethics regarding data storage and the management and sharing of such data. This book is a collection of chapters authored by world-class experts focusing on the security and privacy aspects from a computational point of view, with a focus on practical tools, applications, and open avenues for further research.

The main topics cover the design and use of various computational tools and software, simulations of social networks, representation and analysis of social networks, with a focus on security, privacy, and anonymization. Authors present some of the latest advances of in security and privacy issues related to social networks and illustrate how organizations/individuals can be protected from real-world threats. Experience reports, survey articles, and intelligence techniques and theories with specific networks technology problems are depicted. We hope that this book will be useful for researchers, scholars, postgraduate students and developers who are interested in social networks research and related issues. In particular, the book will be a valuable companion and comprehensive reference for both postgraduate and senior undergraduate students who are taking a course in Social Networks. The book contains 13 chapters (including an introductory chapter) and is divided into three parts, and all chapters are self-contained to provide greatest reading flexibility.

Part I deals with six chapters focusing on different research issues related to trust and privacy in social networks. In Chap. 1, Salama et al. provide an overview of a number of social network related concepts from a computational perspective, such as different performance measures, network services and applications. Further the chapter presents an overview of the social networks security and privacy issues and illustrates the various security risks and the tasks applied to minimize those risks. The authors explain some of the common strategies that attackers often use and some possible counter measures against such issues.

Karupannan in Chap. 2 presents detailed research studies in the areas of security, trust, and privacy applicable to social networks. Novel technologies and methodologies for securely building and managing social networks are discussed and the relevant secure applications as well as practical issues are narrated.

In Chap. 3, Kobayashi focuses on the development of blogs and the blogosphere around the globe. The author found that according to various National surveys conducted by numerous international teams of researchers, motivations for blogging and attitudes regarding privacy are strikingly different in countries with large blogging communities. These differences are reflected in the content of blogs and profoundly influence blog-based social networks, which tend to be region-centric.

Beye et al. in Chap. 4 provide deep insight into privacy in social networks. The authors discuss about the associated privacy risks in relation to both users and service providers, and finally relevant research areas for privacy protecting techniques are illustrated. Mappings are made to reflect typical relations that exist between the type of social network, data type, particular privacy risks, and privacy-preserving solutions.

In Chap. 5, Ulbricht analyzes the options users of online social networks like Facebook have to adjust in the privacy settings. The author illustrates how Facebook as a provider of an online social network designs its platform in such a way that their own interests, as many users data to keep visible and searchable, is implemented.

Guo and Kraines in Chap. 6 introduce the role of trust and recommendation in knowledge sharing networks. To infer the trustworthiness of a knowledge sharing "agent," the authors present a reliability-based trust metric for generating locally calculated inferred trust values using recommendations from trusted agents.

Part II deals with four chapters related to security, measurements, and various real-world applications.

In Chap. 7, Gyarmati and Trinh present the various measurements of user behavior in online social networks that also allows measuring diverse facets of human activities. The authors consider both passive and active methods. The measurement frameworks are compared based on several properties including the details of the datasets and the resource consumption of the different methods.

Simoes et al. in Chap. 8 illustrate the usage of clustering techniques to study how user interests group together and identify the most popular users within these groups. The authors used multiple dimensions of user-related data, providing a more detailed process model of how influence spreads within the network according to interest's dependencies.

In Chap. 9, Varga et al. introduce Gedda-Headz, a novel social mobile gaming concept that focuses on multiplayer mobile gaming. The authors discuss how users may cooperate in Gedda-Headz, and how such cooperation might help users to use services that would otherwise be unreachable for them, or greatly decrease the energy cost of certain activities. Finally, the Gedda-Headz spreader, a novel method to spread the word about the network, is also presented.

Silas et al. in Chap. 10 propose an effective framework for service selection of social network. The experimental results on overhead, social service deduction time, average delay, etc., are illustrated.

Part III deals with three chapters related to various anonymity issues in real-world social network environments.

Chertov and Tavrov in Chap. 11 attempt to solve the problem of group anonymity in a social network. Group anonymity refers to a group of people to be indistinguishable within a particular dataset and the authors propose a wavelet transforms approach for solving this difficult issue.

In Chap. 12, Tripathy presents the status of research on anonymization of social networks and introduces a rough set based algorithm for anonymization. The author also describes some recent algorithms, which use isomorphism of graphs for anonymization, and some future research challenges.

Malinka and Hanacek in the last chapter deal with anonymous communication. The authors perform a set of analyses targeting the behavioral patterns of users and their impact on such systems. The analyses are focused on the properties of e-mail communication relevant to the designers of anonymous systems, information about user profiling, and properties of identifiable social networks and their development in time within the context of the security of anonymous systems.

I am very much grateful to the authors of this volume and to the reviewers for their tremendous service by critically reviewing the chapters. Most of the authors of chapters included in this book also served as referees for chapters written by other authors. Thanks go to all those who provided constructive and comprehensive reviews. I would like to thank Wayne Wheeler and Simon Rees of Springer Verlag, London, for the editorial assistance and excellent cooperative collaboration to produce this important scientific work. Finally, I hope that the reader will share our excitement to present this volume on social networks and will find it useful.

Prof. (Dr.) Ajith Abraham

Machine Intelligence Research Labs (MIR Labs)
Scientific Network for Innovation and Research Excellence (SNIRE)
P.O. Box 2259, Auburn, Washington 98071, USA
http://www.mirlabs.org
Email: ajith.abraham@ieee.org
Personal WWW: http://www.softcomputing.net

Contents

Part I Privacy and Trust

1 Computational Social Networks: Security and Privacy 3
Mostafa Salama, Mrutyunjaya Panda, Yomna Elbarawy, Aboul Ella Hassanien, and Ajith Abraham

2 Security, Privacy, and Trust in Social Networks 23
Komathy Karuppanan

3 Blogging Around the Globe: Motivations, Privacy Concerns, and Social Networking 55
Mei Kobayashi

4 Privacy in Online Social Networks 87
Michael Beye, Arjan J.P. Jeckmans, Zekeriya Erkin, Pieter Hartel, Reginald L. Lagendijk, and Qiang Tang

5 Privacy Settings in Online Social Networks as a Conflict of Interests: Regulating User Behavior on *Facebook* 115
Max-R. Ulbricht

6 A Reliability-Based Metric for Inferring Trust from Recommendations in Knowledge Sharing Networks..... 133
Weisen Guo and Steven B. Kraines

Part II Security and Applications

7 Measurement Methods of User Behavior in Online Social Networks..... 157
László Gyarmati and Tuan Anh Trinh

8 Exploring Influence and Interests Among Users Within Social Networks 177
Jose Simoes, Julia Kiseleva, Elena Sivogolovko, and Boris Novikov

9 User Cooperation, Virality and Gaming in a Social Mobile Network: The Gedda-Headz Concept 207
Csaba Varga, Laszlo Blazovics, Hassan Charaf, and Frank H.P. Fitzek

10 An Effective User-Driven Framework for Selection of Social Network Services 229
Salaja Silas, Kirubakaran Ezra, and Elijah Blessing Rajsingh

Part III Anonymity

11 Providing Group Anonymity in Social Networks 249
Oleg Chertov and Dan Tavrov

12 Anonymisation of Social Networks and Rough Set Approach 269
Bala Krishna Tripathy

13 Behavioural Patterns and Social Networks in Anonymity Systems ... 311
Kamil Malinka and Petr Hanáček

Index 341

Contributors

Ajith Abraham Machine Intelligence Research Labs (MIR Labs), Scientific Network for Innovation and Research Excellence, Auburn, WA, USA

Michael Beye Information Security and Privacy Lab, Faculty of EEMCS, Delft University of Technology, Delft, The Netherlands

Laszlo Blazovics Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Budapest, Hungary

Hassan Charaf Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Budapest, Hungary

Oleg Chertov Kyiv Polytechnic Institute, National Technical University of Ukraine, Kyiv, Ukraine

Ashwini Dalvi Department of Information Technology, K.J. Somaiya College of Engineering, Vidyavihar, Mumbai, India

Yomna Elbarawy Faculty of Computers and Information, BUE, Cairo, Egypt

Zekeriya Erkin Information Security and Privacy Lab, Faculty of EEMCS, Delft University of Technology, Delft, The Netherlands

Kirubakaran Ezra BHEL, Trichy, India

Frank H.P. Fitzek Mobile Device Group, Aalborg University, Aalborg, Denmark

Weisen Guo Science Integration Programme (Human), Department of Frontier Sciences and Science Integration, Division of Project Coordination, The University of Tokyo, Kashiwa, Japan

László Gyarmati Telefonica Research, Plaza de Ernest Lluch i Martín 5, 08019 Barcelona-Spain

Petr Hanáček Faculty of Information Technologies, Brno University of Technology, Brno, Czech Republic

Pieter Hartel Distributed and Embedded Security, Faculty of EEMCS, University of Twente, Enschede, The Netherlands

Aboul Ella Hassanien Faculty of Computers and Information, Cairo University, Cairo, Egypt

Arjan J.P. Jeckmans Distributed and Embedded Security, Faculty of EEMCS, University of Twente, Enschede, The Netherlands

Komathy Karuppanan DCSE, Easwari Engineering College, Chennai, India

Julia Kiseleva St. Petersburg State University, St. Petersburg, Russia

Mei Kobayashi IBM Research-Tokyo, Toyosu, Koto-ku, Tokyo, Japan

Steven B. Kraines Science Integration Programme (Human), Department of Frontier Sciences and Science Integration, Division of Project Coordination, The University of Tokyo, Kashiwa, Japan

Reginald L. Lagendijk Information Security and Privacy Lab, Faculty of EEMCS, Delft University of Technology, Delft, The Netherlands

Kamil Malinka Faculty of Information Technologies, Brno University of Technology, Brno, Czech Republic

Boris Novikov St. Petersburg State University, St. Petersburg, Russia

Mrutyunjaya Panda Department of ECE, Gandhi Institute of Engineering and Technology, Gunupur, India

Elijah Blessing Rajsingh Department of Information Technology, Karunya University, Coimbatore, India

Mostafa Salama British University in Egypt, Cairo, Egypt

Irfan Siddavatam Department of Information Technology, K.J. Somaiya College of Engineering, Vidyavihar, Mumbai, India

Salaja Silas Department of Information Technology, Karunya University, Coimbatore, India

Jose Simoes Fraunhofer FOKUS, Berlin, Germany

Elena Sivogolovko St. Petersburg State University, St. Petersburg, Russia

Qiang Tang Distributed and Embedded Security, Faculty of EEMCS, University of Twente, Enschede, The Netherlands

Dan Tavrov Kyiv Polytechnic Institute, National Technical University of Ukraine, Kyiv, Ukraine

Tuan Anh Trinh Network Economics Group, Department of Telecommunications and Media Informatics, Budapest University of Technology and Economics, Budapest, Hungary

Bala Krishna Tripathy School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India

Max-R. Ulbricht Department of Commercial Information Technology and Quantitative Methods, Computers and Society, Technical University of Berlin, Berlin, Germany

Csaba Varga Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Budapest, Hungary