EDITORIAL

Big data intelligence

Alfredo Cuzzocrea[1]

Big data is an emerging paradigm that embraces a very large collection of research topics ranging from big data management and analytics to big data architectures (mostly coupled with *Cloud-based solutions*). Authoritative and well-understood topics in big data research are: (i) *big data representation*, where the main issue consists in devising effective solutions to represent big data repositories according to heterogeneous formats and over different memory supports; (ii) *big data management*, where the main challenge is represented by the problem of efficiently managing big data for several data management tasks such as big data access, big data indexing, and big data querying; (iii) *big data processing*, where the main goal is to integrate big data with higher-level processes mostly related to big data analytics routines, which pervade a plethora of real-life applications running from social networks to smart cities, from *e*-life systems and tools to bio-informatics, and so forth.

"What you can do with big data?" is a critical, hot-topic question that is attracting the attention of a large and large community of interdisciplinary researchers. Indeed, looking at a proper process-like perspective, the usage and the fruition of big data in real-life applications is really critical, and it can represent an "enabling" key for the success of big data methodologies and technologies. From this basic intuition, the newly-coined term "big data intelligence" is a possible answer to that critical question. Big data intelligence refers to a wide collection of intelligent methods, methodologies techniques and algorithms whose main goal consists in effectively and efficiently representing, managing and processing big data within the core-layers of relevant (big-data) frameworks and systems in order to support big data management and analytics routines in a variegate number of applicative settings that include: social networks, smart cities, *e*-life systems and tools, bio-informatics, graph

analytics, *e*-government, machine learning tools, ambient intelligence systems, robotics, and so forth.

This special issue on "Big Data Intelligence" of the *Journal of Ambient Intelligence and Humanized Computing* focuses on latest research results and open research challenges in the context of extending big data representation, management and processing with intelligent methods, methodologies techniques and algorithms. With the aim of adequately fulfilling both theoretical and practical issues deriving from the wide context of big data intelligence, this special issue contains four papers, which have gone through two rigorous review rounds before being accepted for the final inclusion. In the following, a brief overview on each paper is provided.

The first paper, titled "Data Sharing among Wireless Client Devices in Cooperative Manner with Minimum Transmissions", by Nyan Lin, Brian M. Kurkoski, Yasuo Tan and Yuto Lim, focuses the attention on the problem of supporting data sharing among wireless devices *cooperatively* and at *a minimum transmission cost*. As authors recognize, a group of nearby wireless end-devices can benefit a fast service to satisfy their required packets by cooperating to exchange their packets after receiving collectively from a common base station. This problem can be formulated as *a coding and transmission scheme* and solved by the linear network coding. Therefore, authors propose *a balanced coding and transmission scheme*, named as BCT, which assigns suitable clients to find and transmit linear combinations of the received packets. The goals of the proposed scheme are to minimize the total number of transmissions, to maintain fairness on the number of transmissions among the participants in the cooperative group and to maintain the limited energy resources until all members satisfy their needs. Moreover, *a transmission scheme with physical layer network coding* (BCTS/PNC) for the same problem is also introduced, in order to further reduce the required transmission time slots and accomplish the data exchange process in short time. Performance of the schemes and discussion in terms of the fairness, the number of transmissions and the completion

✉ Alfredo Cuzzocrea
   alfredo.cuzzocrea@dia.units.it

[1] DIA Department, University of Trieste and ICAR-CNR, Trieste, Italy

time by testing with various simulation parameters and scenarios are finally presented and discussed in details.

The second paper, titled "Spatial Cloaking for Location-Based Queries in the Cloud", by Hiba Jadallah and Zaher Al Aghbari, moves the attention on the issue of *effectively and efficiently supporting location-based queries in the Cloud*, which is the emerging computational environment where people nowadays rely heavily on technology, and prefer being provided with personalized services. *Location Based Services* (LBS) are one of those highly popular services. Users provide their location information in some query to the LBS server, which in turn processes the query and returns *personalized* results. The major concern when dealing with these services is the *privacy issue*. Mainly, there are two privacy issues, the user's identity and the user's location. Not securing such information could result in some threats to the user. To preserve the user's privacy, researchers have proposed *spatial cloaking* to blur the user's location by a trusted location anonymizer server. Existing methods suffer from high communication cost due to the large number of communication rounds between the user's device and the cloud server to answer the query. Within the context of so-delineated framework, authors propose *an efficient k-anonymity algorithm*, called *Aman*, to compute the cloaked area with minimal number of communication rounds between the user and the cloud server. Unlike existing methods in which the server starts the search from the root or the leaves of the indexing structure, *Aman* algorithm reduces the search time by starting the search at an intermediate estimated level of the indexing structure that is as close as possible to the queried location. To preserve the user's privacy, *Aman* uses k-anonymity cloaking to hide the user's location. The experimental results using synthetic and real datasets show that *Aman* outperforms other state-of-the-art approaches.

The third paper, titled "A Self-Managing Volatile Key Scheme for Wireless Sensor Networks", by Abdelkader Laouid, Abdelnasser Dahmani, Hani Ragab Hassen, Ahcene Bounceur, Reinhardt Euler, Farid Lalem and Abdelkamel Tari, considers the challenge of *effectively and efficiently managing cryptographic keys over Wireless Sensor Networks* (WSN), which is, indeed, a relevant problem nowadays. Indeed, the limited amount of resources in WSNs is the main challenge for securing them. This essentially because sensors are inherently small devices with limited embedded storage, processor and battery capacity. The situation is even worse when attackers, with virtually unlimited amount of resources, have direct physical access to sensors. Cryptographic keys are used for authentication, authorization, confidentiality, data integrity, as well as many other security services. Several proposals have been made for key management in WSNs. In this paper, authors review some notable key management schemes and propose a new one. The originality of the proposed

scheme lies in two main facts: first, authors do not place a master key on all sensors before deploying them as several other proposals did, but they rather place the master key in a *subset* of sensors; second, the master keys are *volatile*, i.e. sensors use the master key to bootstrap the system and they delete them shortly after that. The proposed extensive simulations show the efficiency of this approach.

Finally, the fourth paper, titled "Software-defined Security Controller-based Group Management and End-to-End Security Management", by Enrique Festijo, Younchan Jung and Marnel Peradilla, proposes *a framework for supporting group management and end-to-end security management based on the horizontal model*, which is suitable for *group-based private systems*. The *software-defined security controller* (SDSC), which is located at the center of the control layer, acts as a software-defined networking controller responsible for group management and end-to-end security management. The proposed *group-key re-keying feature* uses the unicast method for distributing the signaling messages among the group members that belong to various heterogeneous networks. This network-independent-and-centralized architecture for group-key re-keying is specifically advantageous for *dynamic members* to constitute secure group. While the group-key management is responsible for securing control signaling messages within the group members, the purpose of the end-to-end security management is to protect the end-to-end data traffic within them. To achieve end-to-end security, authors introduce *an innovative packet-key scheme* that collaborates with the group-key management. Then, the members of the group-based private system are allowed to receive packet-key-based security service for their end-to-end data traffic. The packet-key scheme is based on the idea that the very short lifetime of the packet-key with a relatively-small key size can provide high level of security and satisfy the latency requirements especially for real-time applications. Because SDSC handles most of the burden in terms of communication and computational load, the workload for group-key and end-to-end security management are dramatically reduced from each group member viewpoint. The additional feature of subgroup-key management enables each group member to sustain less workload, which solves the scalability issue for big-size private groups.

grateful to the authors who have submitted papers to this special issue. The editor truly appreciates their patience and understanding throughout the review process.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.