MULTIMEDIA COMMUNICATIONS TECHNICAL COMMITTEE
http://www.comsoc.org/~mmc

MMTC Communications - Frontiers

Vol. 12, No. 2, March 2017

CONTENTS

Message from the MMTC Chair

Dear MMTC colleagues and friends,

Greetings! This team of officers was elected at IEEE ICC 2016 in Kualar Lumpar, Malaysia last May, while we are planning the MMTC meeting at IEEE ICC 2017 in Paris, France now. Time flies! It is a great honor and pleasure to serve as MMTC Chair for 2016 ~ 2018. In the first year of our term, I enjoyed working with our steering committee chair Dr. Zhu Li, our MMTC officers, boards, IGs, our web master Dr. Haixia Zhang, our newsletter editor Dr. Mugen Peng, to serve the MMTC community and to continue the past success of MMTC. Thank you all for your collaboration and support!

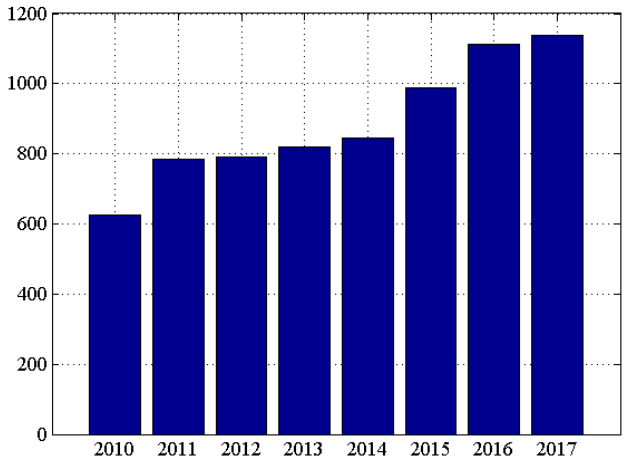
I would like to take this opportunity to invite all of you to the following two MMTC meetings. We will review the MMTC activities with updates from the officers, boards, and IGs, as well as updates of MMTC sponsored conferences/workshops at these meetings. We will also discuss potential problems and challenges, as well as any issues that are raised at the meetings.

(i) The MMTC meeting at IEEE ICC 2017 in Paris, France.
Time: 12:00-14:00, Wednesday May 24, 2017
Room: Hyatt Regency Etoile, Monceau

(ii) The MMTC meeting at IEEE ICME 2017 in Hong Kong, China.
Time: Thursday, July 13, 2017 (hours TBD)
Room: Harbour Grand Kowloon hotel in Hong Kong, Salon II.

Recently we conducted a self-evaluation as required by the ComSoc Technical Services Board, and submitted a self-evaluation report. As you may know, each ComSoc technical committee (TC) will be recertified every three years. MMTC was recertified in 2013 under Dr. Jianwei Huang's leadership. It is expected that we will go through recertification soon. This self-study helps us to better understand the expectations, be prepared for the next round recertification, and to reexamine our organization and activities.

While preparing the self-evaluation report, I was greatly impressed by the many activities and contributions that have been achieved. Thanks to the past chairs and officers, who laid the foundation and shape the structure of the MMTC we have today, and thanks to all our members for your hard work to make such a vibrant MMTC! Another finding that I am impressed with, and would like to share with you all, is the fast increase of MMTC members in the past few years. Our past and current membership board directors have done an excellent job on growing the MMTC community. See the following figure of number of MMTC members over the past few years. MMTC is now a big community of 1100+ members!



The streamlined membership subscription website is: http://mmc.committees.comsoc.org/membership/. Anyone who is working on related fields can enter his/her name and email address to become an MMTC member. Note that

no IEEE or IEEE Communications Society membership is required. Please spread the word and encourage your friends, colleagues, and more important, your students to subscribe. I am sure your students will greatly benefit from participation in MMTC events, as I did years ago.

I would also like to bring to your attention of the many resources and opportunities MMTC offers to its members. Please check out the MMTC website http://mmc.committees.comsoc.org, for MMTC sponsored journals, conferences/workshops, MMTC Communications—Frontiers and Reviews, and MMTC Interest Groups. Every year, MMTC recommends associate editors and special issue proposals to sponsored journals (e.g., IEEE Transactions on Multimedia) and TPC or Track Co-Chairs to sponsored conferences (e.g., IEEE ICC, IEEE GLBOECOM, IEEE ICME, IEEE CCNC, etc.). MMTC also helps its members for elevation to senior member or Fellow of the IEEE, and nominates Distinguished Lectures to ComSoc. In addition, MMTC recognizes its members with Best Journal and Conference Paper Awards, Distinguished Service Award, Outstanding Leadership Award, and Excellent Editor Awards every year. Please stay tuned for announcements from the MMTC mailing list and consider nominating a colleague or a self-nomination.

I hope you enjoy reading this MMTC Communications—Frontiers issue, and strongly encourage you find the IG of interest to get involved and to contribute to future Frontiers special issues. If you have any suggestions or comments, please do not hesitate to contact me.

Sincerely,

Shiwen Mao
Chair, Multimedia Communications Technical Committee
IEEE Communications Society

SPECIAL ISSUE ON Content-Driven Communications and Computing for Multimedia in Emerging Mobile Networks

Guest Editors: Tao Jiang, Wei Wang, Huazhong University of Science and Technology, Cheng Long, Queen's University Belfast
{taojiang,weiwang}@hust.edu.cn, cheng.long@qub.ac.uk

Due to continuing advances in wireless communications and mobile devices, we are entering an era of rapid expansion in multimedia applications and services. Multimedia-based services, such as video streaming (Youtube, Netflix) and content sharing (Instagram, Snapchat) are the dominant driving forces behind the expansion. Current connection-centric mobile network architectures have become a barrier to meet the diverse application requirements and the quality expectation of the end users. The developments of multimedia transmission systems and services call for new understanding and evaluation of user's perceived quality of experience (QoE) to meet the proliferation of content-centric services. There exist increasing demands for content-driven communications and computing technologies to break the bottleneck of current connection-centric network architectures and lead to a clean-slate redesign of network architecture.

The four papers included in this special issue on content-driven communications and computing for multimedia aim to address a number of noteworthy challenges and present the corresponding solutions and suggestions. Most of these contributions are made by authors who are renowned researchers in the field, and the audience will find in these papers the research advances for content-driven communications and computing performance for multimedia in terms of better video quality, larger average Mean Opinion Score (MOS) and many other metrics. Each of these four papers is briefly introduced in the following paragraphs.

In cognitive radio network (CRN), CR has been recognized as an effective approach to support bandwidth-demanding mobile services, and perceived quality of experience (QoE) for users is an important part that needs to be taken into account in multimedia communications. "*QoE Driven Video Streaming over Cognitive Radio Networks for Multi-User with Single Channel Access*" presents the contribution made by Mingjie Feng, Zhifeng He and Shiwen Mao, where a Hungarian method-based approach was proposed to design the access polices for QoE-aware multi-user video streaming. In this research, the channel assignment problem was formulated as an IP and solved with the Hungarian Method to derive the optimal solution, where QoE is used as performance metric. Simulation results demonstrate that the proposed algorithm can achieve optimal solutions for channel access.

With the coming waves of big data, data-driven analysis receives serious attention and is becoming an important approach to assess user QoE. However, the imbalanced dataset will cause a lot of problems in data-driven analysis, in contribution "*Data-driven QoE analysis in imbalanced dataset*", Ruochen Huang, Xin Wei, and Liang Zhou presented their research in building a QoE model over imbalanced datasets. In this research, they firstly gave a typical procedure of data-driven QoE analysis in the imbalanced dataset and then exploited different improved algorithms in every step for handling imbalanced dataset. Simulation results evidence superior performance of the improved algorithms in terms of the metric G-mean.

Since human's QoE can be inferred through psychophysiological signals, Electroencephalogram (EEG), the system that has long been utilized in psychophysiology research and clinical diagnosis can be able to play an important role in evaluation and monitoring of user's QoE. In contribution "*An EEG-Based Assessment of Integrated Video QoE*", Xiaoming Tao, Xiwen Liu, Zhao Chen, Jie Liu and Yifeng Liu have further explored the EEG's potential capability of measuring users' integrated QoE during watching videos. In this research, both internal and external factors, which correspond to video performance and environment, have been further considered in the integrated QoE assessment model and the stimulus-related features of EEG are extracted, either from time domain or from the frequency domain. This research is valuable to understand the effects of internal factors and external factors on QoE.

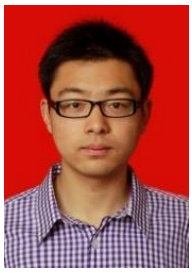
Hao Zhu, Jing Ren, and Yang Cao tried to design D2D networks from the users' perspective in their paper "*QoE-aware on-demand content delivery through device-to-device communications*". In this research, they gave a typical process of D2D content delivery, which contains four steps: content caching, pair matching, resource allocation and content transmission. Moreover, they introduced their research on this topic from the viewpoint of QoE. Specifically, a user-centric pair matching mechanism paring content requesters with content owners is introduced, followed by a

QoE-aware resource allocation mechanism for D2D content delivery when the specific content type is adaptive video stream. Simulation results showed that the proposed QoE-aware mechanisms outperform the QoE-oblivious mechanisms.

Due to the limited time and volume, this special issue has no intent to present a complete scope of content-driven communications and computing for multimedia in emerging mobile networks. Nonetheless, we hope to bring to the audience the essence of selected innovative and original research ideas and progress for the purpose of inspiring future research in this fast growing area.

The guest editors are thankful for all the authors for their contributions to this special issue, as well as the consistent support from the MMTC Communications – Frontier Board.

Tao Jiang is currently a Distinguished Professor in the School of Electronics Information and Communications, Huazhong University of Science and Technology, Wuhan, P. R. China. He received the B.S. and M.S. degrees in applied geophysics from China University of Geosciences, Wuhan, P. R. China, in 1997 and 2000, respectively, and the Ph.D. degree in information and communication engineering from Huazhong University of Science and Technology, Wuhan, P. R. China, in April 2004. He served or is serving as symposium technical program committee membership of some major IEEE conferences, including INFOCOM, GLOBECOM, and ICC, etc.. He is invited to serve as TPC Symposium Chair for the IEEE GLOBECOM 2013, IEEE WCNC 2013 and ICCC 2013. He is served or serving as associate editor of some technical journals in communications, including in IEEE Transactions on Signal Processing, IEEE Communications Surveys and Tutorials, IEEE Transactions on Vehicular Technology, and IEEE Internet of Things Journal, etc.. He is a recipient of the NSFC for Distinguished Young Scholars Award in 2013, and he is also a recipient of the Young and Middle-Aged Leading Scientists, Engineers and Innovators by the Ministry of Science and Technology of China in 2014. He was awarded as the Most Cited Chinese Researchers in Computer Science announced by Elsevier in 2014 and 2015.



Wei Wang is a professor in School of Electronic Information and Communications, Huazhong University of Science and Technology. During Jan. 2015 to Aug. 2016, he was a Research Assistant Professor in Fok Ying Tung Graduate School, Hong Kong University of Science and Technology (HKUST). He received his Ph.D. degree in Department of Computer Science and Engineering from HKUST, where his Ph.D. advisor is Prof. Qian Zhang. Before he joined HKUST, he received his bachelor degree in Electronics and Information Engineering from Huazhong University of Science& Technology in June 2010.

Cheng Long is a lecturer based in the Knowledge Data Engineering (KDE) group of School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast (QUB). Prior to that, he did his PhD study under the supervision of Prof. Raymond Chi-Wing Wong at the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology (HKUST) and got a PhD degree in 2015. During his PhD study, he did a research visit at University of Southern California (USC) under the supervision of Prof. Cyrus Shahabi from Feb 2014 to May 2014 and did another research visit at University of Michigan (UM) under the supervision of Prof. H. V. Jagadish from Oct 2014 to Apr 2015.

QoE Driven Video Streaming over Cognitive Radio Networks for Multi-User with Single Channel Access

Mingjie Feng, Zhifeng He and Shiwen Mao
Auburn University, Auburn, AL, USA
mzf0022@auburn.edu, zzh0008@auburn.edu, smao@ieee.org

1. Introduction

A study by Cisco indicates a drastic increase in mobile data and that almost 66% of the mobile data was video-related by 2015 [1]. Such dramatic increase in wireless video traffic, coupled with the depleting spectrum resource, poses great challenges to today's wireless networks. It is of great importance to improve the wireless network capacity by promoting more efficient use of spectrum, which can be accomplished by the cognitive radio (CR) technology. CR is an evolutionary technology for more efficient and flexible access to the radio spectrum. In a cognitive radio network (CRN), Cognitive Users (CUs) search for the unoccupied licensed spectrum of the Primary User (PU) network and then opportunistically access detected spectrum holes in an unobtrusive manner. CR has been recognized as an effective approach to support bandwidth-demanding mobile services such as wireless video streaming [2].

In the area of multimedia communications, subjective assessment methods have been studied intensively [3]. The International Telecommunication Union (ITU) has proposed standards on subjective assessment methods for various application scenarios [4]. For video transmission, quality of experience (QoE) is an effective subjective quality assessment model for the perceptual visual quality of video sequences. One of the most widely used QoE metric is the Mean Opinion Score (MOS) [5]. In the MOS model, the visual quality of a video sequence is not only dependent on the network environment such as packet loss rate, network delay, but also dependent on the content type. For example, under the same network conditions, the visual quality of video contents of fast motions (e.g., sports) is generally worse than that of video contents of slow motions (e.g., news). Since the ultimate goal of most multimedia communication services is to achieve high perceptual quality for viewers, it is desirable to incorporate QoE models in such applications.

In this paper, we address the challenging problem of downlink multi-user video streaming in CRNs. We consider a CRN consisting of one cognitive base station (CBS) and multiple CUs. Without loss of generality, we assume each CU can sense and access one channel at a time. The CUs cooperatively sense the PU signals on licensed channels and the CBS infers the licensed channel states based on the CU sensing results with an OR fusion rule. Once the idle channels are detected, the CBS then assigns them to active CUs for downlink multi-user video streaming. We incorporate the video assessment model proposed in [5], [6], aiming to maximize the CU QoE by optimal designs of spectrum sensing and access policies.

It is obviously a challenging problem to design the access polices for QoE-aware multi-user video streaming, due to the large number of design factors and the complex interactions that should be modeled in a cross- layer optimization framework. We propose a Hungarian method-based approach to achieve optimal solution to the channel assignment problem. Simulation results demonstrate the superior performance of the proposed methods in terms of the MOS that CUs can achieve under various network scenarios.

2. Problem Statement and Solution Algorithm

We consider a primary network operating on N1 orthogonal licensed channels. There is a CR network co-located with the primary network, consisting of a CBS supporting M1 CUs. The CUs sense the PUs' usage of the licensed channels and access the licensed channels in an opportunistic manner. We assume the CUs, when they are not receiving data, measure the SNRs of the PU transmissions over all the licensed channels and report the measured SNRs to the CBS through some feedback mechanism. Based on such feedback, the CBS then assigns those CUs with good channel conditions to sense each licensed channel, so as to improve the sensing performance. We consider the downlink multi-user video streaming scenario, where the CBS streams a video to each active CU using the license channels that are detected idle. We assume time is divided into a series of non-overlap GOP windows, each consisting of T time slots.

1) Formulation of Optimal Assignment Problem for Video Transmission (OAPVT).

We consider the QoE model named Mean Score Opinion (MOS) proposed in [6]. The MOS of CU i during time slot

t, denoted by Ψ_{ij}^{t}, can be expressed as

$$\begin{aligned}\Psi_{ij}^{t} &= \alpha + CT_i\gamma + \left(\beta + CT_i\delta\right)\ln\left(SBR_{ij}^{t}\right)\\ &= \alpha + CT_i\gamma + \left(\beta + CT_i\delta\right)\ln\left(B_j \log_2\left(1+SNR_{ij}^{t}\right)\right)\end{aligned}$$

where α = 3.9860, β = 0.0919, γ = −5.8497, and δ = 0.9844 are constants, CTi is the Content Type of the video sequences required by CU i, Bj is the bandwidth of channel j in kbps, and SNR_{ij}^{t} is the SNR of the video signal using channel j measured at CU i at time slot t [6].

We assume that N2 channels are sensed as idle after the sensing phase, where N2 $\leq$ N1. We consider a general case where not all the CUs have data to receive at all times. Instead, the probability of a CU has data to receive at each GOP window is 0 $\leq$ ξ $\leq$ 1. The number of CUs that have data to receive in a GOP window is denoted as M2, where M2 $\leq$ M1. An M2 $\times$ N2 matrix Y is used to represent channel access assignment on time slot t, with the entry given as

$$y_{ij}^{t} = \begin{cases} 1, \text{ assign channel } j \text{ to CU } i \text{ in time slot } t \\ 0, \text{ otherwise.} \end{cases}$$

We consider the case where each CU can use at most one channel at each time slot due to hardware constraints, and each channel can be used by at most one CU at each time slot. We aim to maximize the expected average MOS of all the CUs during a GOP window by assigning the available channels.

$$\max : \sum_{i=1}^{M_2} \mathrm{E}\left[\frac{1}{T}\sum_{t=1}^{T}\Psi_i^t\right] = \frac{1}{T}\sum_{t=1}^{T}\sum_{i=1}^{M_2}\mathrm{E}\left[\Psi_i^t\right].$$

The above objective function can be maximized if we maximize the expected MOS increment of the M2 CUs during each time slot [2], which can be written as

$$\begin{aligned}\sum_{i=1}^{M_2}\mathrm{E}\left[\Psi_i^t\right] &= \sum_{i=1}^{M_2}\sum_{j=1}^{N_2}\mathrm{E}\left[\Psi_{ij}^t\right]y_{ij}^t\\ &= \sum_{i=1}^{M_2}\sum_{j=1}^{N_2}\left[\Pr\left(H_{0j}^t \mid s_j = 1\right)\phi_{ij}^t + \Pr\left(H_{1j}^t \mid s_j^t = 1\right)\theta_{ij}^t\right]y_{ij}^t,\end{aligned}$$

where $s_j^t = 1$ indicates the channel is sensed as idle; $\Pr(H_{0j}^t)$ and $\Pr(H_{1j}^t)$ are the probability of channel j to be idle or busy at time slot t, respectively; $\Pr(H_{0j}^t \mid s_j^t = 1)$ and $\Pr(H_{1j}^t \mid s_j^t = 1)$ are the conditional probability for channel j to be idle or busy conditioned on the sensing result, respectively; μ_{ij}^t and ν_{ij}^t are the received SNR at CU i using channel j which is indeed idle or busy at time slot t, respectively; and

$$\begin{aligned}\Pr\left(H_{0j}^t \mid s_j^t = 1\right) &= \frac{\left(1-P_{f_j}^t\right)\Pr\left(H_{0j}^t\right)}{\left(1-P_{d_j}^t\right)\Pr\left(H_{1j}^t\right) + \left(1-P_{f_j}^t\right)\Pr\left(H_{0j}^t\right)}\\ \Pr\left(H_{1j}^t \mid s_j^t = 1\right) &= 1 - \Pr\left(H_{0j}^t \mid s_j^t = 1\right)\\ \phi_{ij}^t &= \alpha + CT_i\gamma + \left(\beta + CT_i\delta\right)\ln\left(B_j \log_2\left(1+\mu_{ij}^t\right)\right)\\ \theta_{ij}^t &= \alpha + CT_i\gamma + \left(\beta + CT_i\delta\right)\ln\left(B_j \log_2\left(1+\nu_{ij}^t\right)\right)\end{aligned}$$

Define ω_{ij}^t as

$$\omega_{ij}^t = \Pr\left(H_{0j}^t \mid s_j^t = 1\right)\phi_{ij}^t + \Pr\left(H_{1j}^t \mid s_j^t = 1\right)\theta_{ij}^t$$

The optimal channel access problem is formulated as

$$\max: \sum_{i=1}^{M_2}\sum_{j=1}^{N_2} \omega_{ij}^t y_{ij}^t$$

$$\text{s.t.} \quad \sum_{j=1}^{N_2} y_{ij}^t \le 1,\ i \in \{1,\cdots,M_2\},$$

$$\sum_{i=1}^{M_2} y_{ij}^t \le 1,\ j \in \{1,\cdots,N_2\},$$

$$y_{ij}^t \in \{0,1\},\ \forall\ i,\ j$$

2) Solution Algorithm Based on Hungarian Method

In the OAPVT problem, each CU can use at most one channel and each channel can be used by at most one CU. Then, the OAPVT problem becomes a maximum weight matching problem in a bipartite graph that matches active CUs to available channels, while only one edge is allowed for any CU and channel and the edge weights are defined as ω_{ij}^t. This maximum weight matching problem can be effectively solved in polynomial time using the Hungarian method, and the solution is optimal.

The time complexity of using Hungarian method to solve the OAPVT problem is $\mathcal{O}\big((M_2+N_2)(M_2N_2)\big)$, where M_2+N_2 is the total number of vertices and M_2N_2 is the total number of possible edges in the bipartite graph representing the OAPVT problem.

3. Performance Evaluation

The performance of the proposed algorithm is validated with Matlab simulations. We assume the PUs and CUs are randomly distributed within the coverage of a CBS. Table I lists the values of the parameters used in the simulations. fs is the sampling frequency at the CUs for energy detection. We compare the proposed scheme with a benchmark scheme presented in [11], called Data Rate (DR) Driven, in which channels are assigned to end users to maximize the sum data rate of all users.

TABLE I
SIMULATION PARAMETERS

Parameters	*Value*	*Parameters*	*Value*
M_1	30	μ_{ij}^t	−25 dB to −15 dB
N_1	30	ν_{ij}^t	−80 dB to −60 dB
K	10^4	ς_{ij}^t	−30 dB to −10 dB
f_s	10^6 Hz	$\bar{P}_d$	0.95
T	100	$\max_j \left\{\Pr\left(H_{0j}^t\right)\right\}$	0.9
B_j	10^6 Hz		

Fig. 1 demonstrates the effect of the traffic load of CUs (i.e., ξ) on video quality. The average sum MOS achieved by the proposed scheme and the DR Driven scheme are plotted with 95% confidence intervals as error bars. As the CU traffic load increases, more channels are required. We can see that while the number of idle channels is greater than the number of active CUs, the average MOS sum of both schemes increases with ξ, and the performance gap between the two schemes grows larger.

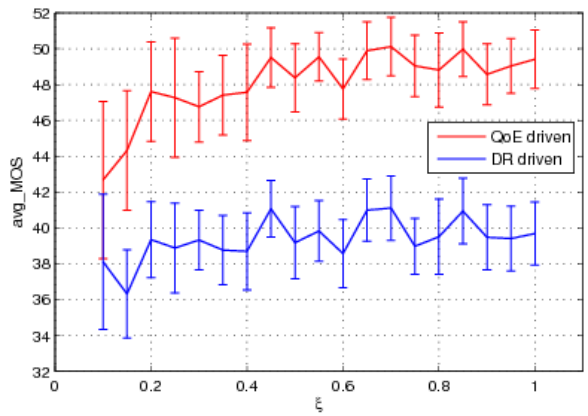


Fig. 1. Average MOS sum of the CUs over an entire GOP window, avg_Ψ, for different CU traffic loads ξ

In Fig. 2, we examine the impact of PU channel utilization and the SNR at the CUs on CU video quality. In the 3-D plots, the x-axis is the minimum channel idle probability, i.e., $\min_{i,j}\left\{\Pr\left(H_{0j}^{t}\right)\right\}$, and the y-axis is the minimum SNR of CUs, i.e., $\min_{i,j}\left\{\mu_{ij}^{t}\right\}$. It can be observed from the figure that as channel utilization is decreased, a channel has a higher probability of being at the idle state and there will be more channels available for CUs in the transmission phase. Thus, the average MOS sum of the CUs is improved.

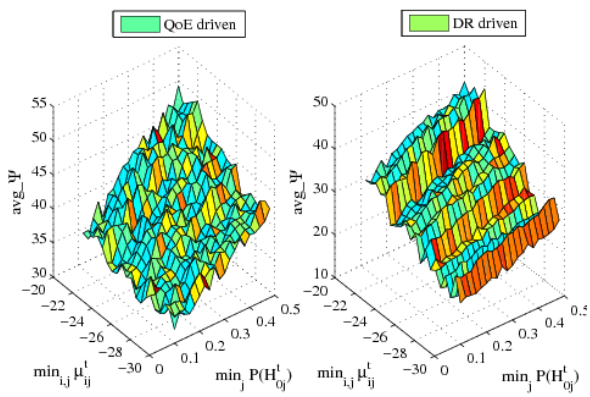


Fig. 2. Average MOS sum of the CUs over an entire GOP window vs. the minimum channel idle probability and the minimum SNR of CUs.

4. Conclusion

In this letter, we investigated the problem of QoE-aware video streaming over CRNs. The channel assignment problem was formulated as an IP and solved with the Hungarian Method to derive the optimal solution, where QoE is used as performance metric. We showed that the proposed algorithm achieves optimal solutions for channel access. The proposed scheme was validated with simulations.

ACKNOWLEDGMENT

This work was supported in part by the U.S. National Science Foundation under Grant CNS-1320664, and the Wireless Engineering Research and Education Center at Auburn University.

References

[1] Cisco, "Visual Networking Index (VNI)," Feb. 2014. [Online]. Available: http://www.cisco.com/.

[2] D. Hu, and S. Mao, "Streaming scalable videos over multi-hop cognitive radio networks," IEEE Trans. Wireless. Commun., vol.11, no.9, pp.3501– 3511, Nov. 2011.

[3] K. Yamagishi and T. Hayashi, "Opinion model using psychological factors for interactive multimodal services," IEICE Trans. Communication., E89-B(2):281–288, Feb. 2006.

[4] J. You, U. Reiter, M. Hannuksela, M, Gabbouj, and A. Perkis, "Perceptual-based quality assessment for audio-visual services: A survey," Signal Processing: Image Communication., vol.25, no.7, pp.482– 501, Aug. 2010.

[5] A. Khan, L. Sun, and E. Ifeachor, "Content clustering based video quality prediction model for MPEG4 video streaming over wireless networks," in Proc. IEEE ICC'09., Dresden, Germany, June 2009, pp.1– 5.

[6] A. Khan, L. Sun, and E. Ifeachor, "QoE prediction model and its application in video quality adaptation over UMTS networks," IEEE Trans. Multimedia, vol.14, no.2, pp.431–442, Apr. 2012.

[7] Y. Chen, Q. Zhao, and A. Swami, "Joint design and separation principle for opportunistic spectrum access in the presence of sensing errors," IEEE Trans. Inf. Theory, vol.54, no.5, pp.2053–2071, May 2008.

[8] Z. He, S. Mao, and S. Kompella, "Quality of Experience driven multi-user video streaming in cellular cognitive radio networks with single channel access," IEEE Trans. on Multimedia, vol.18, no.7, pp.1401-1413, July 2016.

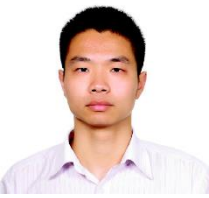
[9] Z. He, S. Mao, and S. Kompella, "QoE driven video streaming in cognitive radio networks: Case of single channel access," in Proc. IEEE GLOBECOM 2014, Austin, TX, Dec. 2014, pp.1388-1393.

[10] M. Feng, T. Jiang, D. Chen, and S. Mao, "Cooperative small cell networks: High capacity for hotspots with interference mitigation," IEEE Wireless Communications, vol. 21, no. 6, pp .108-116, Dec. 2014.

[11] K. Kar, L. Xiang, and S. Sarkar, "Throughput-optimal scheduling in multichannel access point networks under infrequent channel measurements," IEEE Trans. Wireless. Commun., vol. 7, no. 7, pp. 2619–2629, July 2008.

[12] M. Feng, S. Mao, and T. Jiang, "Joint duplex mode selection, channel allocation, and power control for full-duplex cognitive femtocell networks," Elsevier Digital Communications and Networks Journal, vol.1, no.1, pp.30-44, Feb. 2015.

[13] Y. Xu, G. Yue, and S. Mao, ``User grouping for Massive MIMO in FDD systems: New design methods and analysis," IEEE Access Journal, vol. 2, no. 1, pp. 947--959, Sept. 2014.



Mingjie Feng received his B.E. and M.E. degrees from Huazhong University of Science and Technology in 2010 and 2013, respectively, both in electrical engineering. He was a visiting student in the Department of Computer Science, Hong Kong University of Science and Technology, in 2013. He is currently a Ph.D. student in the Department of Electrical and Computer Engineering, Auburn University, AL. His research interests include cognitive radio networks, femtocell networks, massive MIMO and full-duplex communication. He is a recipient of Woltosz Fellowship at Auburn University.

Zhifeng He received the M.S. degree in Micro Electronics and Solid State Electronics from Beijing University of Posts and Telecommunications, Beijing, China, and the B.S. degree in Electronics Information Science and Technology from Shandong University of Technology, Zibo, China, in 2012 and 2009, respectively. Since 2012, he has been pursuing the Ph.D. degree in the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL, USA. His current research interests include cognitive radio, mmWave communications and networking, multimedia communications and optimization.

Shiwen Mao received Ph.D.in electrical and computer engineering from Polytechnic University, Brooklyn, NY. Currently, he is the Samuel Ginn Distinguished Professor in the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL. His research interests include wireless networks and multimedia communications. He is a Distinguished Lecturer of the IEEE Vehicular Technology Society. He is on the Editorial Board of IEEE Transactions on Multimedia, IEEE Internet of Things Journal, IEEE Multimedia, among others. He was a past Associate Editor of IEEE Transactions on Wireless Communications and IEEE Communications Surveys and Tutorials. He is the Chair of IEEE ComSoc Multimedia Communications Technical Committee. He received the 2015 IEEE ComSoC TC-CSR Distinguished Service Award, the 2013 IEEE ComSoc MMTC Outstanding Leadership Award, and the NSF CAREER Award in 2010. He is a co-recipient of the Best Paper Awards from IEEE GLOBECOM 2016, IEEE GLOBECOM 2015, IEEE WCNC 2015, and IEEE ICC 2013, and the 2004 IEEE Communications Society Leonard G. Abraham Prize in the Field of Communications Systems.

Data-driven QoE analysis in imbalanced dataset

Ruochen Huang, Xin Wei, Liang Zhou
College of Telecommunications and Information Engineering,
Nanjing University of Posts and Telecommunications, Nanjing, China, 210003
Email: huangruochen@outlook.com, {xwei, liang.zhou}@njupt.edu.cn

1. Introduction

The assessment of quality in multimedia is a topic of great interest to both service providers and developers. Quality of Experience (QoE) is proposed for evaluating the user's perception for service. There are many approaches to assess user QoE which can be categorized into three classes: subjective test, objective quality model and data-driven analysis [1].

Subjective test obtained from assessors' grading, such as Mean Opinion Score (MOS). The drawbacks are obvious: time-consuming and high cost. Objective quality models mainly focus on relationship between QoS (or other factors) and QoE. However, the validation of objective quality model needs the MOS from subjective test. So the objective quality models get same drawbacks. With the age of big data is coming, data-driven analysis gets serious attention and it can improve the drawbacks in both objective and subjective approaches. Firstly, in data-driven analysis, it always takes factors easily quantified as the measurement of user QoE. Secondly, the data-driven analysis can build QoE model with large-scale data in real scenario.

In data-driven analysis, machine learning are always used in building QoE model in big dataset than other methods [2][3].The big datasets from real-life system are always imbalanced because QoS parameters are remained within normal ranges in most cases. So the sample data that represent QoE at low level is small. However, imbalanced dataset will cause a lot of problems in data-driven analysis such as small disjuncts, dataset shift and so on [4]. In this work, we first give a typical evaluation process of data-driven QoE analysis in imbalanced dataset and then present our research in building QoE model over imbalanced dataset.

2. Data driven approach in imbalanced dataset

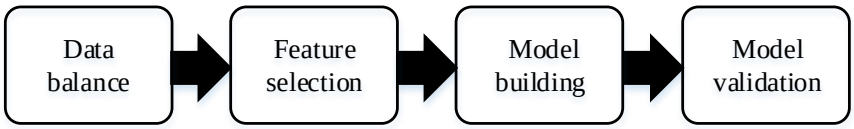


Fig. 1Procedure of data-driven QoE analysis in imbalanced dataset

The typical procedure of data-driven QoE analysis in imbalanced dataset is shown in Fig. 1, containing four main steps.

Data balance is one of key steps for handling imbalanced dataset. Many researchers try to balance the dataset by sampling methods which contain oversampling, under sampling and data cleaning [5].Oversampling methods try to balance dataset by creating new minority samples while under sampling methods decrease the number of majority samples. Data cleaning methods mainly remove the overlapping between majority class samples and minority class samples. The main achievements on this area contain synthetic minority over sampling technique (SMOTE), Tomek links, EasyEnsemble and so on.

Feature selection is used to select useful and key factors affecting QoE from the preprocessed dataset. When the feature selection step is finished, machine learning algorithms are often used to build QoE model and perform prediction. This step is another key step for data-driven QoE analysis in imbalanced dataset. In this step, cost-sensitive methods are always used to build QoE model by measuring costs of samples misclassified especially minority samples. Many typical models and algorithms have been improved for cost-sensitive such as Adaboost, neural networks, decision trees and so on. Finally, validation methods are used to validate precision and generalization of the designed model s and algorithms.

3. Our research on QoE in imbalanced data set

We get several datasets from telecom operators. The datasets contain KPI records from the IPTV set-top box and user-complaint records from operators. When a user makes a complaint call during a special period of time, his/her QoE is bad and vice versa.

In [6], we have improved the SMOTE algorithm to balance dataset. First, the minority class samples are split into two sets: "DANGER" and "SAFE" by number of minority class samples in nearest neighbors. The probability of

generating instances based on samples in "DANGER" set should be increased. Meanwhile, the probability of generating instances based on samples in "SAFE" set should be reduced. Considering this, a variable tis defined as follows:

$$t = \frac{n_{SAFE}}{n_{DANGER}} . \tag{1}$$

Moreover, a random number α which belongs from 0 to 1 is obtained. If $\alpha \in [0, t/t+1]$, a new minority sample is generated based on the "DANGER" set. Otherwise, the new sample is generated based on the "SAFE" set. The advantage of the proposed algorithm is that it can reduce calculation and make the boundary between majority class and minority class clearer. From Fig. 2, we can see that the G-mean of improved-SMOATE algorithm is higher than the original-SMOATE one in KNN and C4.5.

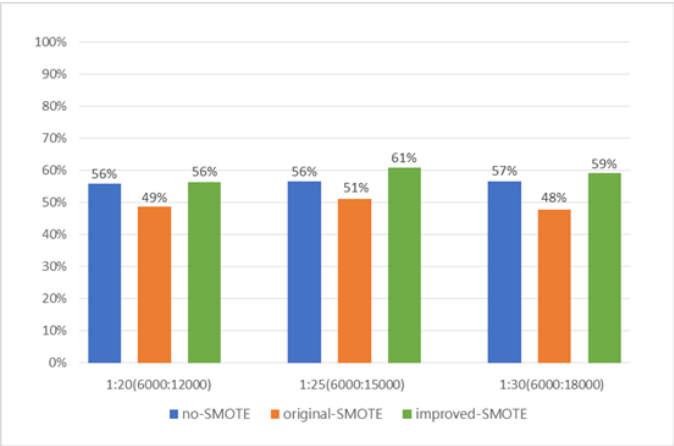


Fig. 2. G-mean comparison of no-SMOTE, original-SMOTE , improved-SMOATE in C4.5

Moreover, we also improve the cost-sensitive methods in [7][8]. In [7], Adaptive-Cost AdaBoost algorithm is proposed to predict QoE in imbalanced dataset. We modify the way of setting the initial weights of the samples and give higher coefficients to the minority class samples which are easily wrong classified. Compared with the AdaBoost, the proposed algorithm can obtain higher F-measure.

Considering decision tree can show decision-making process more clearly, we have proposed an improved algorithm based on decision tree for imbalanced dataset in [8].There are two main improvements of unbiased decision tree: Frist, we change the criteria used for selecting the best characteristic feature. The criteria considers the recall and precision of the minority class samples. Second, we add threshold T to leaf node of the decision tree. If the number of minority class samples is larger than threshold T, the leaf node represents minority class. Otherwise, traditional majority rule are used to determine the class of leaf node. The G-mean of unbiased decision tree is higher than classification and regression tree (CART).

4. Conclusion

Although the concept of QoE has been proposed for a period of time, there is no unified approach which can measure experience of user in the multi-scenario. The data-driven analysis provides a new way to solve this problem. In this paper, we give a typical procedure of data-driven QoE analysis in imbalanced dataset. Moreover, we introduce our research on this topic. In our ongoing work, we will try design a new billing model or traffic-aware routing approach based on the QoE analysis approaches.

References

[1] Y. Chen, K. Wu, and Q. Zhang, "From QoS to QoE: A tutorial on video quality assessment," IEEE Commun. Surv. Tutorials, vol. 17, no. 2, pp. 1126–1165, 2015.

[2] M. S. Mushtaq, B. Augustin, and A. Mellouk, "Empirical study based on machine learning approach to assess the QoS/QoE correlation," in Networks and Optical Communications (NOC), 2012 17th European Conference on, 2012, pp. 1–7.

[3] S. Aroussi and A. Mellouk, "Survey on machine learning-based QoE-QoS correlation models," in Computing, Management and Telecommunications (ComManTel), 2014 International Conference on, 2014, pp. 200–204.
[4] V. López, A. Fernández, S. García, V. Palade, and F. Herrera, "An insight into classification with imbalanced data: Empirical results and current trends on using data intrinsic characteristics," Inf. Sci. (Ny)., vol. 250, no. 11, pp. 113–141, 2013.
[5] H. He and E. A. Garcia, "Learning from imbalanced data," IEEE Trans. Knowl. Data Eng., vol. 21, no. 9, pp. 1263–1284, 2009.
[6] R. Liu, R. Huang, Y. Qian, X. Wei, and P. Lu, "Improving user's Quality of Experience in imbalanced dataset," in 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 2016, pp. 644–649.
[7] Q. Liu, X. Wei, R. Huang, H. Meng, and Y. Qian, "Improved AdaBoost model for user's QoE in imbalanced dataset," in 2016 8th International Conference on Wireless Communications Signal Processing (WCSP), 2016, pp. 1–5.
[8] L. Wang, J. Jin, R. Huang, X. Wei, and J. Chen, "Unbiased Decision Tree Model for User's QoE in Imbalanced Dataset," in International Conference on Cloud Computing Research and Innovations, 2016, pp. 114–119.

Ruochen Huang is currently a Ph.D. candidate in Nanjing University of Posts and Telecommunications. His research interest is on Quality of Experience (QoE) of multimedia delivery/distribution.

Xin Wei is an associate professor with College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include multimedia signal processing, machine learning, and pattern recognition.

Liang Zhou is professor in Nanjing University of Posts and Telecommunications. His research interests include multimedia communications and multimedia signal processing.

An EEG-Based Assessment of Integrated Video QoE

Xiaoming Tao[1], Xiwen Liu[2], Zhao Chen[3], Jie Liu[2] and Yifeng liu[2]
Department of Electronic Engineering, Tsinghua University, Beijing, China
[1]taoxm@tsinghua.edu.cn, [2]{liu-xw15, liu-jie13, liu-yf16}@mails.tsinghua.edu.cn,
[3]chenzhao1995@sina.com

1. Introduction

For several decades, quality of service (QoS) has been widely adopted as the primary measurement of the objective quality of wireless communications. It includes multiple network-level parameters, such as throughput, delay, jitter, error rate and so on. However, QoS is suffering an eclipse in recent years since it does not take user perception into account [1]. According to the report from Cisco [2], mobile video will generate more than three-quarters of mobile data traffic by 2021. This significant change calls for a usercentric evaluation method for mobile video communication. Pointedly, quality of experience (QoE), which is defined as the perceptual QoS from the users' perspective [3], is deemed to be a preferable index for the next generation of wireless multimedia communications.

The uppermost challenges of implementing QoE assessment are modeling and evaluation, since user experience is subjective and fluctuant with various environment. Traditionally, researchers conducted subjective test, in which participants were required to evaluated and scored the quality of tested video in specific environment, to obtain the firsthand QoE information, i.e. mean opinion score (MOS) [3]. Despite its high accuracy and credibility, MOS is not able to elicit any rational model. Therefore, such tests are not feasible beyond laboratory scenario due to its offline nature. Some researchers attempted to explore the relationship between QoE score and QoS parameters [1] [4], since QoS can be easily evaluated and monitored. Such QoS-based mapping method successfully avoids high cost and realizes real time monitoring of user QoE, however, at the cost of accuracy decline [5].

In view of the limitations of the two above-mentioned approaches, a complementary solution is inferring human's QoE through psychophysiological signals. Electroencephalogram (EEG), a system that records the scalp potentials from different electrodes at the frequency of 1000 to 2000Hz, has long been utilized in psychophysiology research and clinical diagnosis. It enables us to directly monitor human's pure brain activities almost in real time rather than conscious response with bias and intentions. For this reason, EEG is able to play an important role in evaluation and monitoring of user's QoE. In [6], the

authors creatively utilized EEG to directly measure the users' perception of video quality change and discovered users' unconscious responses to video quality change. This work is just a preliminary achievement for EEG-based video quality measurement. The multi-dimensional factors that affect users' QoE are complex. A more integrated QoE model including both internal factors and external factors, which correspond to video performance and environment needs to be further considered. In the rest of this paper, we are going to introduce the roadmap for further exploring the EEG's potential capability of measuring users' integrated QoE during watching videos.

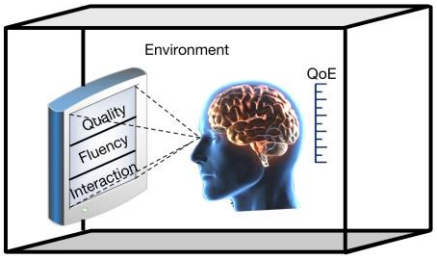


Fig. 1: An integrated QoE assesment model.

2. MODEL DESCRIPTION

We illustrate our integrated video QoE assessment framework in figure 1. The major factors that affect QoE are divided into two categories, internal ones and external ones, based on if they represent the quality of video transmission or not. For internal factors, we select three sorts of parameters, which relate to the quality of images (quality), the fluency of playing (stalling), and the interaction between the audience and devices (delay) respectively. For external factors, we select the watching environment, among which illumination affects most on the human's visual perception. Thus, our framework includes three internal factors and an external factor. When trying to

investigate their relationships with QoE, instruments of high temporal resolution is needed because we have to figure out how exactly the visual perception of an audience changes at an artefact. Therefore EEG, with a common temporal resolution of 1ms (1000Hz sample rate), is a perfect tool to put our framework of assessment into practice. We discuss our detailed approaches of researching into each sorts in the following sections.

2.1 Stalling

Online video degradations are either caused by a low bitrate or transmission errors, both of which can result in video stallings, i.e. video freezes [7]. Nowadays, stallings have become most common video artefacts, and its impact on QoE is related to its properties, e.g. its durations, number of occurrences, etc. EEG is an appropriate tool in investigating the impact of each of those properties, and is superior to other methods, e.g. MOS, because of its high time resolution. We justify this by giving our thinkings on one of the investigations, the impact of durations on QoE.

As the duration of a stalling increases, the audience's experience changes from being imperceptible to perceptible of the stalling, and from feeling not annoyed to annoyed at it. Mining into the enormous EEG data can help us find kinds of patterns which make it possible to quantify the "imperceptibility" and the "annoyance" of stallings of various durations.

For instance, to investigate its imperceptibility, the subject can be presented a series of video clips, each of which contains a stalling of different lengths randomly distributed in the middle. All the videos should be of the same content and without much meanings so that other properties of a stalling will not distort the results. The subject should be asked to find out if there is a stalling in each video, which helps him concentrate on the experiment. The EEG signals recorded can be analyzed to find out the common patterns during stallings of the same lengths.

2.2 Quality

Traditionally, if the distortion contained in a video is not noticeable, the video is deemed to be of no subjective quality degradation [8]. However, this viewpoint seems no longer reasonable if we consider human's physical perception and psychological response separately. In [6], the authors discovered users' unconscious brain activities to video quality changes that cannot be detected. Therefore, what the deep-seated influence of unnoticeable distortion on human's experience needs to be further investigated so that a fullrange measurement of subjective quality degradation can be obtained. The design of the experiment is briefly described as follows.

First, the threshold of just-noticeable distortion (JND) is determined for every participant. Then, for each participant, we produce a mass of stimulus videos, each of which contains randomly distributed distortions that are unnoticeable. Over the course of experiment, participants are presented numerous stimulus videos repeatedly and their brain activities are recorded in the form of EEG waves. After collecting enough data, we will find out whether there exists a specific pattern of signal distinguishing a participant's experience related to unnoticeable distortion from other cases, i.e., no distortion and noticeable distortion. If it is in that circumstance, using such a signal pattern to quantify human's experience of unnoticeable distortion is another significant work.

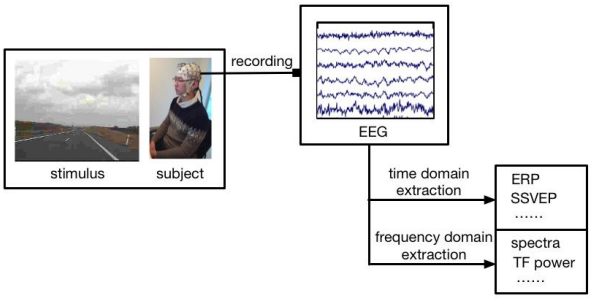


Fig. 2: Our proposed procedures of QoE assessment.

1）Delay

We often encounter problems when watching videos that the start delay is too long, which is caused by pre-buffer of player. Concerning the limit to human perception, we are aiming at finding the threshold of pre-buffer time. Once the pre-buffer time is below the threshold, subject will not realize the existence of start delay.

Here we briefly describe how to use EEG to measure the threshold of start delay. First we need a series of test

videos based on different pre-buffering time as experimental stimulus. For example, a pre-buffer time of 500 means test video will be delayed by 0.5 second when the subject press the play button. Then their EEG signals will be recorded and processed, from which we can analyze whether they realize the start delay and the pre-buffering threshold can be set.

2）Environment

While video playback quality is determined by source encoding parameters and network state, viewing quality may also be affected by environment factors. In other words, we should take viewing conditions into account when conducting subjective video quality assessment, since it is closely pertinent to viewing quality. Specifically, luminance is acknowledged as a prominent environment factor influencing viewing quality, which is neurophysiologically reasonable. Present work on the issue tends to track the correspondence between visibility and quality for an extended range of luminance conditions, and it is based on subjective measurements of contrast sensitivity function (CSF) and mean opinion score (MOS) [9].

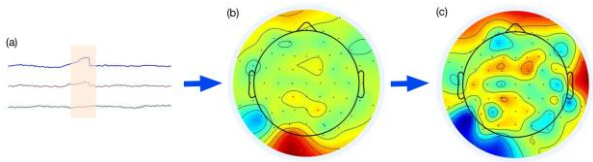


Fig. 3: A method of extracting P300 features.

The fact that thresholds for subjects to detect video quality distortion will shift with changing luminance level lays a foundation for our EEG-based research. The subject should be presented a sequence of video clips with different degradation levels and be asked to decide whether the distortion is perceived. The same practice is then conducted under different luminance levels, with EEG signals recorded respectively. Employing event-related potentials (ERPs) oriented feature extraction and classification, we can have a command of perceptual thresholds of distortion under different luminance conditions, which allows us to have a glimpse into the effect of luminance on video quality perception. Other environment factors like viewing angle can be studied as well using this method.

3. FEATURE EXTRACTION

Among the chaotic EEG signals, some features need to be extracted from the raw EEG signals for further analysis and QoE measurement (seen figure 2). According to the property of the stimulus and human's response, we search for the expected features from time domain or frequency domain. Time domain features are directly related to the waveforms, and they usually reflect human's simultaneous reaction to a specific event. For example, in [6] some features characterizing an ERP are discovered. With such features, the "imperceptibility" of an impairment can be determined. Frequency domain features, on the other hand, are extracted from the spectra of the signals, and can be used to measure human's mental state over a period of time, e.g., the annoyance of impairments occurring in a video. In the following sections, we briefly summarize and propose some useful approaches to extract those features.

1) From time domain

Basically, abrupt changes of video quality lead to a typical pattern in the EEG, a positive voltage in the time interval 250-500 ms post-stimulus (the P300 component). Its amplitude peaks over central-parietal brain regions and correlates positively with the magnitude of the video quality change.

Among several categories of ERPs with their particular scalp topographies and latencies, P300 has been the most exploited ERP component in video quality assessment on an empirical and practical basis. Methods to extract these features and to exploit P300 nature have been explored in figure 3. First, discriminative time intervals should be selected between undistorted trials and trials with highest distortion (a). Spatial distribution of class difference values are subsequently calculated for the selected time interval (b). Second, the LDA filter is computed and is utilized as a spatial filter of original EEG signals, which projects all channels data to a single virtual channel (c). The prefiltered data is presumed to be P300-dominant since we expect P300 component for lower quality changes has a similar spatial distribution to that of highest distortion, thus suitable for LDA classification [6].

Potentials other than P300 have been investigated to get an alternative for EEG-based measurement of perceived video quality, e.g. Steady state visual evoked potentials (SSVEPs) [14].

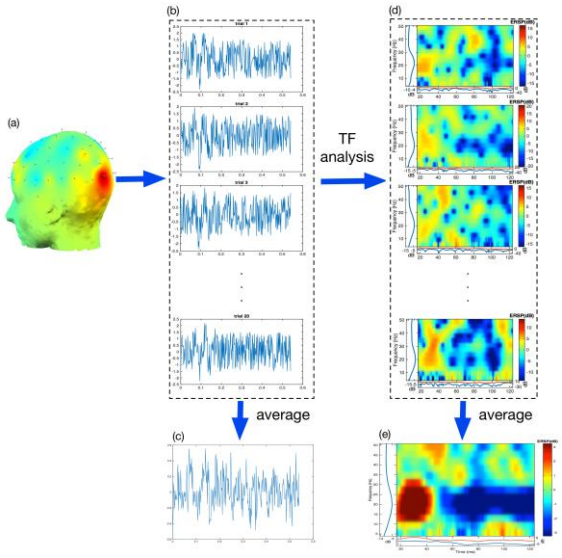


Fig. 4: ERP(c) and mean spectra changes (e) of 20 trial runs (b).

2) From frequency domain

EEG power is commonly divided into 5 frequency bands, which are delta (1-3Hz), theta (4-7Hz), alpha (8-13Hz), beta (14-30Hz) and gamma(31-50Hz), and the average power of each band has been found highly correlated with emotions. In [10], for instance, the correlations between frontal power asymmetry and emotional responding are confirmed. Other studies use the power spectral density (PSD) of EEG signals as features for emotion recognition [11]. They use either power from some electrodes or the differences of some symmetric pairs as features.

When it comes to short time impairment, e.g. stallings, PSD cannot yield satisfying results since the audience's emotions only change transiently. However, time-frequency (TF) analysis helps us to figure out the spectral changes in time domain [12], and the changes of QoE can be explored in this way. When the brain activities, e.g. reactions to a kind of video degradation, are not accurately "phase-locked", averaging spectra yield better results than ERPs [13], as shown in figure 4. Figure 5 illustrates the mean spectral changes of EEG signals of electrode P7 during the perceptions of several video clips each with a 2-second freeze. The power of beta band and delta band increases significantly during the stalling, and may serve as a feature of quantifying the effects of stallings on QoE.

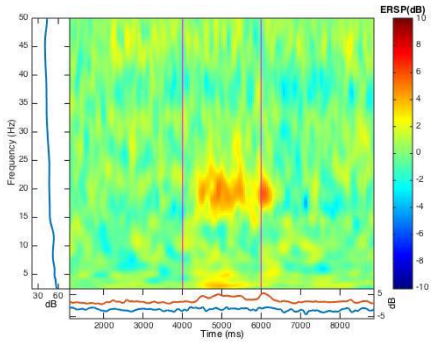


Fig. 5: Mean spectral change of EEG signals of P7 electrode. The two vertical lines denote the start and the end of the stalling respectively.

4. Conclusion

An integrated EEG-based video QoE model is proposed where both internal and external factors are considered. The subject is presented a stimulus while his EEG signals being recorded. The stimulus-related features of EEG are extracted, either from time domain or from frequency domain, to be further analyzed and quantified into QoE scores.

ACKNOWLEDGMENT

This work was supported by the National Basic Research Project of China (973)(2013CB329006) and National Natural Science Foundation of China (NSFC, 61622110, 61471220, 91538107).

References

[1] M. Venkataraman and M. Chatterjee, "Inferring video QoE in real time," IEEE Network, vol. 25, no. 1, pp. 4-13, January-February 2011.

[2] Cisco, Cisco Visual Networking Index, "Global mobile data traffic forecast update, 2013-2018," Cisco White Paper, Feb. 2014.

[3] R. C. Streijl, S. Winkler, D. S. Hands. "Mean opinion score (MOS) revisited: methods and applications, limitations and alternatives," Multimedia Systems, vol. 22, no. 2, pp. 213-227, 2016.

[4] M. Fiedler, T. Hossfeld and P. Tran-Gia, "A generic quantitative relationship between quality of experience and quality of service," IEEE Network, vol. 24, no. 2, pp. 36-41, March-April 2010.

[5] A. Khan, L. Sun, E. Jammeh and E. Ifeachor, "Quality of experiencedriven adaptation scheme for video applications over wireless networks," IET Communications, vol. 4, no. 11, pp. 1337-1347, July 23, 2010.

[6] S. Scholler, S. Bosse, M. S. Treder, B. Blankertz, G. Curio, K. Mller, and T. Wiegand, "Toward a Direct Measure of Video Quality Perception Using EEG," Image Processing, IEEE Transaction on, vol. 20, no.5, pp. 2619-2629, May 2012.

[7] H. Quan, G. Mohammed, "No-reference Temporal Quality Metric for Video Impaired by Frame Freezing Artefacts," in Image Processing, International Conference on, 2009.

[8] N. Jayant, J. Johnston and R. Safranek, "Signal compression based on models of human perception" in Proceedings of the IEEE, vol. 81, no. 10, pp. 1385-1422, Oct 1993.

[9] R. Mantiuk, K. J. Kim , A. G. Rempel, W. Heidrich, "HDR-VDP-2:a calibrated visual metric for visibility and quality predictions in all luminance conditions," ACM Transactions on Graphics (TOG), vol. 30, no. 4, pp. 1-14, July 2011.

[10] J. A. Coan, J.J.B. Allen, "Frontal EEG Asymmetry as a Moderator and Mediator of Emotion," Biological Psychology, vol. 67, no. 1-2, pp. 7-49, March 2004.

[11] M. Soleymani, S. Asghariesfeden, M. Pantic, and Y. Fu, "Continuous Emotion Detection using EEG Signals and Facial Expressions," in Multimedia and Expo, IEEE International Conference on, 2014.

[12] S. K. Hadjidimitriou and L. J. Hadjileontiadis, "Toward an EEGBased Recognition of Music Liking Using Time-Frequency Analysis," Biomedical Engineering, IEEE Transactions on, vol. 59, no. 12, pp. 3498-3510, December 2012.

[13] S. Makeig, S. Debener, J. Onton, and A. Delorme, "Mining Event-related Brain Dynamics," TRENDS in Cognitive Sciences, vol. 8, no. 5, pp. 204-210, May 2004.

[14] L. Acqualagna, S. Bosse, A. K. Porbadnigk, G. Curio, K. Muller, T. Wiegand and B. Blankertz, "EEG-based classification of video quality perception using steady state visual evoked potentials (SSVEPs)," Neural Engineering, Journal of, vol. 12, no. 2, pp. 1-16, 2015.

XIAOMING TAO (M'11) received the B.S. degree from Xidian University, Xi'an, China, in 2003, and the Ph.D. degree from Tsinghua University, Beijing, China, in 2008. From 2008 to 2009, she was a Researcher with Orange-France Telecom Group Beijing, Beijing, China. From 2009-2011, she was a Post-Doctoral Research Fellow with the Department of Electrical Engineering, Tsinghua University. From 2011 to 2014, she was an Assistant Professor with Tsinghua University, where she is currently an Associate Professor. Her research interests include wireless communication and networking, as well as multimedia signal processing.

XIWEN LIU received the B.E. degree from Huazhong University of Science and Technology (HUST) , Wuhan, China in 2012 where he also received the M.E. degree in communication and information system in 2015. He is currently pursuing the Ph.D. degree in the Wireless Multimedia Communication Laboratory, Tsinghua University. His research focuses on understanding of the human visual system and the quality of experience for multimedia.

ZHAO CHEN is currently an undergraduate student from Dalian University of Technology (DUT) . He will be pursuing his M.E. degree in the Wireless Multimedia Communication Laboratory, Tsinghua University in 2017. His research interests include QoE modeing.

JIE LIU is currently an undergraduate student majoring in the Bachelor's Degree of Electronic Information at Tsinghua University. He has been in the Wireless Multimedia Communication Lab since 2016. His research interests include QoE modeling in wireless networks and human visual perception.

YIFENG LIU received the B.E. degree in electronic engineering from Tsinghua University(THU) in 2016. He is currently pursuing the M.E. degree with THU. His research areas include QoE modeling in wireless networks and human visual perception.

QoE-aware on-demand content delivery through device-to-device communications

Hao Zhu, Jing Ren, Yang Cao
School of Electronic Information and Communications,
Huazhong University of Science and Technology, Wuhan, 430074, China
{zhuhao, jingren, ycao}@hust.edu.cn

1. Introduction

Recently, Device-to-Device (D2D) communication, defined as the direct communication between two adjacent mobile users without data routing through the base station (BS), has been proposed as a promising technique to enhance the capacity of cellular networks. If some user devices (UEs) have cached a few popular on-demand contents, other interested neighbor UEs can reuse these contents through D2D communications. Hereby, the BS would only transmit contents which are not locally available instead of transmitting the same popular contents multiple times. The traffic of the BSs is thus significantly offloaded. Moreover, the spectral and energy efficiency can be improved with the short communication distance [1][2].

Quality of Experience (QoE) evaluates the quality of service from the users' perspective [3]. While controlling Quality of Service (QoS) parameters in D2D networks is important for providing good content services, it is more crucial to design novel D2D content delivery mechanisms from the viewpoint of QoE. This is due to the fact that current mobile networks are still facing poor user experience even though the bandwidth and data rate increase.

Our research aims at making a better use of available resources such as the bandwidth and energy of D2D networks to cater to user experience, based on QoE-aware D2D content delivery mechanisms. In this letter, we give an overview of a D2D content delivery process which contains four steps: content caching, pair matching, resource allocation and content transmission. Additionally, we introduce our research on a pair-matching mechanism from users' perspective and a specific example of QoE-aware resource allocation mechanism when the delivered content type is adaptive video stream.

2. Content delivery through D2D communications

The process of content delivery through D2D communications is shown in Fig. 1, containing four main steps.

Content caching is a process to cache popular on-demand contents in the local memory of UEs. It is the premise of D2D content delivery to guarantee that the content requested by the receiver has been cached on the transmitter. The key problem in this process is to decide cache which contents into the limited storage of UEs, considering the characteristics of D2D communications such as mobility and collaboration distance, in the aim of maximizing cache hit radio, cellular network throughput and so on [4][5].

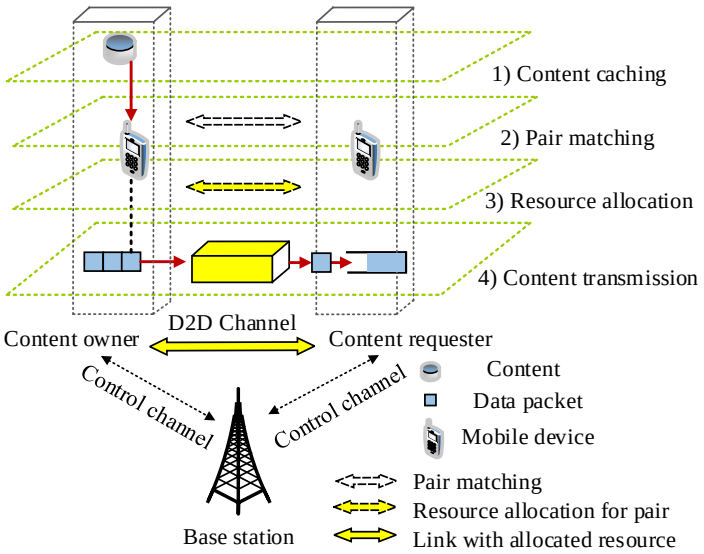


Fig. 1 Process of content delivery through D2D communications

Pair matching solves the problem of selecting an appropriate user from multiple content owners to act as the transmitter for the user who requests a content. Pairing a content requester with a content owner can be done with or without the help of the BS, which may consider factors such as geographic location, social relationship to improve the system performance, and/or communication link quality [6].

Resource allocation is a process to allocate the limited radio resources to multiple D2D pairs that have been matched via the previous step [1]. With the allocated resources, D2D pairs can establish D2D communication links for transmitting content data. When data are transmitted over D2D links, application-level adaptation can be adopted for enhancing QoE. For example, bit rate adaptation for video streams can be deployed to enable a tradeoff between video qualities and play interruptions under the variable conditions of D2D channels [8].

3. Our research on QoE-aware D2D content delivery

To cater to user experience in D2D content delivery with the limited radio resources and UEs' battery energy, we design mechanisms for pair matching and resource allocation from the perspective of QoE.

In [7], we have proposed a user-centric pair matching mechanism which pairs content requesters with content owners while considering the fact that D2D users' motivations are greatly affected by the transmission energy consumption. In the proposed mechanism, UEs can form mutually disjoint collaborative groups. In each group, every UE is obligated to be the transmitter for providing contents to other UEs. Simultaneously, every UE also has the right to be the receiver for obtaining contents from other UEs. The utility function of UE i which joins group S^i is defined as

$$u_i = \sum_{j \in S^i} g_{ij} - \alpha_i \cdot \sum_{j \in S^i} (g_{ji} \cdot E_{ji}) . \tag{1}$$

where g_{ji} denotes the number of contents transmitted from UE i to UE j, and E_{ji} denotes the energy for transmitting a content from UE i to UE j. The value of $1/\alpha_i$ means the upper bound of the ratio of transmission energy consumption to the number of received contents allowed by UE i, for achieving a positive utility.

Since users are selfish and rational in practice, every user aims to join a group which can maximize its utility. From this perspective, we utilize the concept of coalition formation game to solve this problem. A D2D group formation algorithm has been proposed based on the merge-and-split rule combined with the Pareto order. The advantage of the proposed mechanism is that all pairing users are guaranteed to achieve positive utilities with performance gains on the mean and variance of user utilities.

Moreover, we also have proposed a QoE-aware resource allocation mechanism for D2D content delivery when the specific content type is adaptive video stream in [8]. The target of this mechanism is to minimize the time-averaged total quality loss of all video streams, while controlling the long-term play interruption for every stream. The problem can be represented as follows,

$$\begin{aligned} &\min \ \lim_{t \to \infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_i E[L_i(\tau)] \\ &\text{s.t.} \quad Q_i(\tau) \ \text{ is stable for every user} \end{aligned} \tag{2}$$

where $Q_i(t)$ is defined as a virtual queue for user i at the beginning of slot t in order to depict the long-term fluency of the video stream. The input of the queue equals to the length of a slot and the output of the queue is the playing time of the data transmitted to user i at slot t. We leverage the Lyapunov drift-plus-penalty method to solve this problem.

As shown in Fig. 2, the proposed mechanism can achieve a better performance than the QoE-oblivious resource allocation mechanism when the bandwidth is relatively abundant for smooth playback in adaptive video streaming.

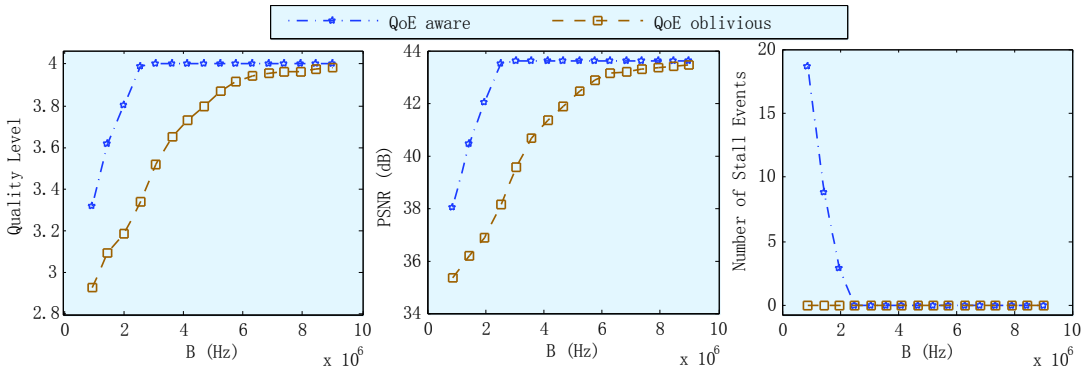


Fig. 2 Performances comparison with different bandwidth B

4. Conclusion

Recently, D2D on-demand content delivery has been proposed to enhance the cellular network capacity. Note that it is significant to understand and design D2D networks from users' perspective. In this letter, we give a typical process of content delivery thorough D2D communications, followed by our research on this topic from the viewpoint of QoE. In future work, we will attempt to design novel QoE-aware mechanisms for on-demand content caching.

Reference

[1] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-Device Communication in LTE-Advanced Networks: A Survey", IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 1923–1940, 2015.

[2] M. Sheng, Y. Li, X. Wang, J. Li, and Y. Shi, "Energy Efficiency and Delay Tradeoff in Device-to-Device Communications Underlaying Cellular Networks", IEEE Journal on Selected Areas in Communications, vol. 34, no. 1, pp. 92-106, Jan. 2016.

[3] Y. Chen, K. Wu, and Q. Zhang, "From QoS to QoE: A tutorial on video quality assessment", IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1126–1165, Secondquarter 2015.

[4] N. Golrezaei, A. G. Dimakis, and A. F. Molisch, "Scaling behavior for device-to-device communications with distributed caching", IEEE Transactions on Information Theory, vol. 60, no. 7, pp. 4286-4298, July 2014.

[5] H. J. Kang, K. Y. Park, K. Cho, and C. G. Kang, "Mobile caching policies for device-to-device (D2D) content delivery networking", in Proc. IEEE INFOCOM WKSHPS, Apr. 2014.

[6] Y. Cao, T. Jiang, X. Chen, and J. Zhang, "Social-aware video multicast based on device-to-device communications", IEEE Transactions on Mobile Computing, vol. 15, no. 6, pp. 1528-1539, Jun. 2016.

[7] H. Zhu, Y. Cao, B. Liu, and T. Jiang, "Energy-aware incentive mechanism for content sharing through device-to-device communications", in Proc. IEEE GLOBECOM, Dec. 2016.

[8] H. Zhu, Y. Cao, W. Wang, B. Liu, and T. Jiang, "QoE-aware resource allocation for adaptive device-to-device video streaming", IEEE Network, vol. 29, no. 6, pp. 6-12, Nov.-Dec. 2015.

Hao Zhu is currently a Ph.D student in the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, P.R. China. His current research interests include device-to-device communication, multimedia communications and optimization.

Jing Ren is currently a M.S. student in the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, P.R. China. Her research interest is wireless edge caching and computing.

Yang Cao is currently an assistant professor in the School of Electronic Information and Communications, Huazhong University of Science and Technology. His research interests include resource allocation for cellular D2D communications and fog/edge computing. He was awarded CHINACOM Best Paper Award in 2010 and a Microsoft Research Fellowship in 2011.

SPECIAL ISSUE ON Security and Privacy of Cloud Computing

Guest Editors: Zheng Chang, University of Jyväskylä, Finland
Zheng Yan, Xidian University, China
zheng.chang@jyu.fi, zyan@xidian.edu.cn

Cloud computing is an emerging technology aimed to provide various computing and storage services over the Internet. It generally incorporates infrastructure, platform, and software as services. For multimedia applications and services over the Internet and mobile wireless networks, there are also strong demands for cloud computing because of the significant amount of computation tasks required for serving millions of Internet and/or mobile users. With cloud computing, users store and process their multimedia application data in the cloud in an efficient manner, eliminating full installation of the media application software on the users' device and thus alleviating the burden of software maintenance and storage , upgrade as well as sparing the computation of user devices and saving the battery of mobile devices. Meanwhile, due to its inherent nature of delivering and sharing in the cloud computing, security and privacy issues are essentially significant to ensure the wide usage of cloud. Specially, security and privacy of big data and data transmission, including those generated by large number of multimedia applications and devices, is a serious issue. However, it is challenging to achieve, as technology is changing at rapid speed and our systems turn into ever more complex. Therefore, the wide spread of cloud computing and the explosion of data volume have jointly created unprecedented opportunities and fundamental security and privacy challenges.

The 5 papers included in this special issue on security and privacy issues of cloud computing aim to address a number of noteworthy challenges and present the corresponding solutions and suggestions. These contributions are made by authors who are renowned researchers in the field, and the audience will find in these papers the research advances for enhanced cloud computing platform for the multimedia services in terms of better efficiency and security, among many other metrics. Each of these 5 papers is briefly introduced in the following paragraphs.

As one of the most common measures, intrusion detection systems are always
introduced in the cloud computing systems to protect the cloud services and provide valuable clues when the systems are under attack. In contribution, "Towards Better Anomaly Interpretation of Intrusion Detection in Cloud Computing Systems", Chengqiang Huang, Zhengxin Yu, Geyong Min, Yuan Zuo, Ke Pei, Zuochang Xiang, Jia Hu, Yulei Wu propose a way of achieving interpretable anomaly detection that is accurate and, at the same time, capable of distinguishing contextual anomalies from typical/point anomalies, to overcome the current limitations. From the simulation results, it can be seen that the utilization of the method in intrusion detection systems will largely benefit the underlying decision-making systems in choosing the proper reaction when an anomaly is witnessed.

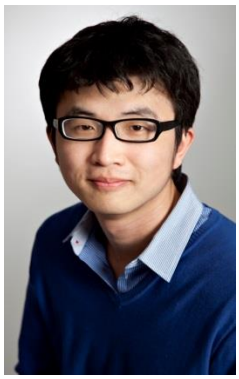
The criticality of the data exchanged through the cloud by companies and regular customers, and the pivotal role of the cloud in critical infrastructures imposes the respect of stringent security and privacy required by cloud platforms. To this aim, the available marketed cloud platforms have been equipped with traditional security and privacy enhancement solutions such as cryptographic primitives, access control or security audit. The cloud computing is also subject to peculiar and unseen requirements, such as data sovereignty and interoperable access control, which have not been yet properly treat. "Geolocation-aware Cryptography and Interoperable Access Control for Secure Cloud Computing Environments for Systems Integration" presents the contribution made by Christian Esposito, where the author have briefly introduced these new challenging issues and the promising solutions in order to deal with aforementioned challenges.

In the cloud storage, data duplication causes cloud service providers (CSPs) too much time and space for data processing. Aiming to address such a problem, a deduplication scheme based on the game theory was proposed by Xueqin Liang and Zheng Yan to handle encrypted cloud data especially big data, in their contribution "Cloud Data Deduplication Scheme Based on Game Theory". Particularly, the existence of collusion between malicious CSPs and dis-honest data users makes data holders lose high profits, which causes more and more data holders refuse to adopt this deduplication scheme. Public goods dilemma happens when the deduplication rate of the Internet environment decreasing with the existence of malicious activities. To solve this dilemma, they analyze the utilities of all players based on a mechanism that can adjust the utilities to arouse their willingness to make contributions to the system, based on the game theoretical method.

In contribution, “Securing DNS-Based CDN Request Routing”, Zhe Wang, Scott Rose and Jun Wang presented a secure DNS-based content distribution network (CDN) requesting scheme to address the trust gap issue raised by the limited Domain Name System Security Extensions (DNSSEC) deployment. The scheme allows a CDN domain in an island of trust to be securely linked with a secure site zone. Besides, the individual-domain-based signing proposed in this work may significantly lessen the cryptographic work by the conventional zone-based DNSSEC signing. The simulation results also show that, as a flexible and scalable extension to DNSSEC, the technique is promising in securing CDNs.

Data explosion is becoming an irresistible trend in the cloud computing system, as the era of big data has arrived. Data-intensive file systems are the key component of any cloud-scale data processing middleware. Hadoop Distributed File System (HDFS), one of the most popular open source data-intensive file systems, has been successfully used by many industrial companies. In HDFS, write and read (WR) performance has a significant impact on the performance of cloud and big data platform, which should be carefully treated. In the contribution, “Empirical Measurement and Analysis of HDFS Write and Read Performance”, Bo Dong, Jianfei Duan, and Qinghua Zheng, have presented comprehensive empirical measurement and analysis of HDFS WR performance, and we propose a derivation method to achieve probability distribution calculation based on HDFS WR mechanism. From the experimental results, the effectiveness of the proposed method can be observed.

The guest editors would like to give our special thanks to all the authors for making contribution to this special issue. We are also thankful to the MMTC Communications–Frontier Board for providing helpful support.



Zheng Chang received the B.Eng. degree from Jilin University, Changchun, China in 2007, M.Sc. (Tech.) degree from Helsinki University of Technology (Now Aalto University), Espoo, Finland in 2009 and Ph.D degree from the University of Jyväskylä, Jyväskylä, Finland in 2013. Since 2008, he has held various research positions at Helsinki University of Technology, University of Jyväskylä and Magister Solutions Ltd in Finland. He was a visiting researcher at Tsinghua University, China, from June to August in 2013, and at University of Houston, TX, during from April to May in 2015. He has been awarded by the Ulla Tuominen Foundation, the Nokia Foundation and the Riitta and Jorma J. Takanen Foundation for his research work. Currently he is working as a Assistant professor with University of Jyväskylä and his research interests include cloud/edge computing, radio resource allocation, and green communications. He is an Editor of Wireless Network and MMTC communication Frontier, and a guest editor of IEEE Access. He serves as a TPC member for numerous IEEE conferences, such as INFOCOM, ICC and Globecom, and reviewer for major IEEE Journals, such as IEEE TVT, TWC, JSAC, TMC, ToN etc.

Zheng Yan received the B. Eng in electrical engineering and M. Eng in computer science and engineering from Xi’an Jiaotong University in 1994 and 1997. She received a second M. Eng in information security from National University of Singapore in 2000. She received the Licentiate of Science and the Doctor of Science in Technology in electrical engineering from Helsinki University of Technology in 2005 and 2007. She is currently a professor at the Xidian University, Xi'an, China and a docent/visiting professor in Aalto University, Finland. She joined the Nokia Research Center, Helsinki in 2000, working as a senior researcher until 2011. She authored more than 150 publications (90% first or corresponding author) and solely authored 2 books. She is the inventor of 11 patents and 38 PCT patent applications, 26 of which were solely invented. She was invited to offer more than 10 talks or keynotes in international conferences or universities. Her research interests are in trust, security and privacy; mobile applications and services; social networking; cloud computing, pervasive computing, and data mining. Prof. Yan is an associate editor of Information Sciences, IEEE Access, IEEE IoT Journal, JNCA, Security and Communication Networks, etc., a special issue leading guest editor of more than 20 journals, such as ACM TOMM, information fusion, IEEE Systems Journal, Future Generation Computer Systems, Computers & Security, IJCS, ACM/Springer MONET, and IET Information Security, etc., and acts as a reviewer for many top journals. She is the organizer of IEEE TrustCom/BigDataSE/ISPA-2015, EAI MobiMedia2016, IEEE CIT2014/2017, CSS2014, ICA3PP2017, NSS2017, etc. She serves as a steering committee or organization committee member for more than 30

conferences and a TPC member for more than 50 conferences, e.g., GlobeCom, ICSOC, ACM MobileHCI, ACM SAC, etc. She is a senior member of the IEEE.

Towards Better Anomaly Interpretation of Intrusion Detection in Cloud Computing Systems

Chengqiang Huang, Zhengxin Yu*, Geyong Min*, Yuan Zuo*, Ke Pei†, Zuochang Xiang†, Jia Hu*, Yulei Wu**
**Department of Computer Science, University of Exeter, Exeter, UK*
†2012 Lab, Huawei Technologies Co., Ltd., China
**{ch544,zy246,G.Min,yz506,J.Hu,Y.L.Wu}@exeter.ac.uk, †{peike,xiangzuochang}@huawei.com*

1. Introduction

The past decade has witnessed a tremendous development of cloud computing technologies, which have infiltrated into diverse aspects of our daily lives. Applications, such as Dropbox, Google App Engine, and Amazon Web Services, all heavily rely on the underlying cloud computing systems, whose availability and reliability have significant impacts on the performance of the applications and the overall user experience. Among many factors, security is one of the most critical aspects in ensuring the normal operation of the cloud computing systems. Therefore, many efforts have been made by cloud service providers and researchers in enhancing the security of the cloud computing systems. As one of the common measures, intrusion detection systems [4] are always introduced in the cloud computing systems to protect the cloud services and provide valuable clues when the systems are under attack.

Intrusion detection systems usually implement a set of anomaly detection methods. These methods monitor the user and system behaviors, model the normal operations, and report anomalies whenever a significant deviation from the expected status of the system or actions of the user is witnessed. For most anomaly detection methods, e.g., box-plot method [2], conventional Support Vector Data Description (SVDD) [5], Replicator Neural Network (RNN) [1], they solely focus on detecting the anomalies, yet, provide little information within the method for interpreting the anomalies, such as a further classification of the detected anomalies or the potential reasons that cause the anomalies. Consequently, in this work, we propose a way of achieving interpretable anomaly detection that is accurate and, at the same time, capable of distinguishing contextual anomalies from typical/point anomalies. The practical application of this method will largely benefit the intrusion detection systems where contextual information plays a vital role in anomaly detection.

As a concrete example of anomaly interpretation, let's consider the situation in Fig. 1, where a time series of Internet traffic is recorded with marked anomalies. In the depicted time series, the metric has two types of anomalies, which are point anomaly and contextual anomaly. The definition of contextual anomaly typically depends on the context. In Fig. 1, the time series has a clear periodic pattern, i.e., a single period contains 5 high peaks followed by 2 low peaks. Considering the periodic pattern as the contextual information, the contextual anomalies in the time series are the data points that are normal in terms of their data value, but abnormal because they do not follow the periodic pattern. A better anomaly interpretation is possible if the differences of the anomalies are identified within the anomaly detection method. To this end, this article is to introduce an anomaly detection method with the capability of distinguishing different anomalies.

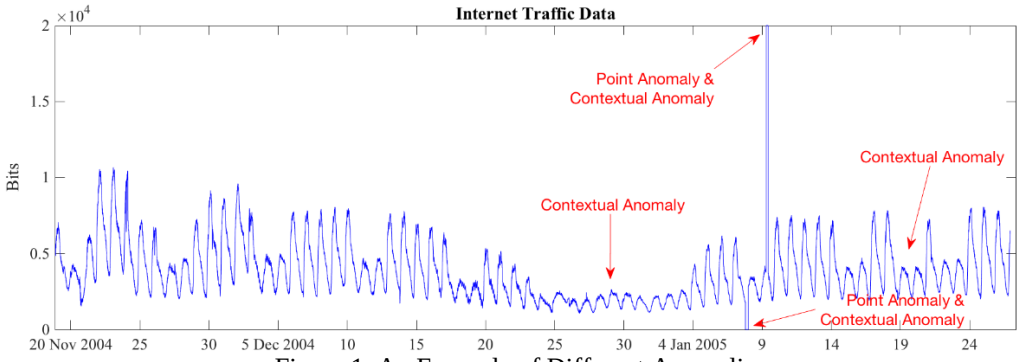


Figure 1. An Example of Different Anomalies

2. Support Vector Data Description with Contextual Information

To provide detailed information about the reported anomalies, i.e., whether the anomalies relate intensively to their contexts, this article proposes to use support vector data description (SVDD) with selected contextual information [6] to supply intrusion detection systems with more flexibility of reporting anomalies. The formulation of the anomaly detection method over a set of data instances $X = \{x_1, x_2, \cdots, x_N\}$ with their contextual information $X^* = \{x_1^*, x_2^*, \cdots, x_N^*\}$ is as follows:

$$\min_{\alpha,b,\alpha^*,b^*} \sum_i \left(\left(\sum_j \alpha_j K(x_i, x_j) + b \right) + \lambda \cdot \left(\sum_j \alpha_j^* K(x_i^*, x_j^*) + b^* \right) \right), \tag{1}$$

$$\text{s.t. } \forall i, \left(\left(\sum_j \alpha_j K(x_i, x_j) + b \right) + \lambda \cdot \left(\sum_j \alpha_j^* K(x_i^*, x_j^*) + b^* \right) \right) \geq 0, \tag{2}$$

$$\forall i, \quad \sum_j \alpha_j^* K(x_i^*, x_j^*) + b^* \geq 0, \tag{3}$$

$$\sum_j \alpha_j = 1, \quad \sum_j \alpha_j^* = 1, \qquad \forall j, \alpha_j \geq 0, \alpha_j^* \geq 0, \tag{4}$$

where $x_i, x_j \in \mathbb{R}^D$ is D-dimensional data with index $i, j \in \{1, 2, \cdots, \mathrm{N}\}$; $x_i^*, x_j^* \in \mathbb{R}^{D^*}$ is D^*-dimensional data with the same index; N is the number of data instances; λ is a hyper-parameter. Function $K(\cdot)$ denotes the famous kernel function that enables the mapping of a data instance to a high- dimensional space for better generalization of the method. In this article, the Gaussian kernel is selected as the kernel function for the experiments, i.e.,

$$K(x_i, x_j) = e^{\frac{-\|x_i - x_j\|^2}{\sigma^2}}. \tag{5}$$

Essentially, the formulation tries to integrate two linear programming SVDDs for training two types of information concerning the same object. The solution of the formulation leads to a description of the dataset that is helpful in anomaly detection. However, different from typical SVDD, this formulation gains two discriminants that are capable of detecting different types of anomalies. As has been mentioned, X is set as the main data information and X^* is the contextual information. Therefore, Eq. (3) mainly concerns the identification of the contextual anomalies, while Eq. (2) is applicable in detecting the overall normality of a data instance. To be more specific, the discriminant of whether a new data x_{new} with contextual information x_{new}^* has contextual anomaly is:

$$\sum_j \alpha_j^* K(x_{new}^*, x_j^*) + b^* \geq \min_i \sum_j \alpha_j^* K(x_i^*, x_j^*) + b^*, \tag{6}$$

while the overall normality of the data is determined by:

$$\left(\left(\sum_j \alpha_j K(x_{new}, x_j) + b \right) + \lambda \cdot \left(\sum_j \alpha_j^* K(x_{new}^*, x_j^*) + b^* \right) \right) \geq 0. \tag{7}$$

From the above two discriminants, a third one is possible considering the enforcement of the constraints in Eqs. (2) and (3). This third discriminant, i.e.,

$$\sum_j \alpha_j K(x_{new}, x_j) + b \geq \min_i \sum_j \alpha_j K(x_i, x_j) + b, \tag{8}$$

demonstrates a practical way of detecting the anomalies from the very origin information of the data instances, i.e., X.

As a result, the new formulation introduces three different discriminants for identifying different types of anomalies. This novel capability enables the anomaly detection method to supply strong interpretations of the detected anomalies. In other words, the anomaly detection method can provide more details about the reason why a data instance is detected as anomalous. Through leveraging this anomaly detection method, intrusion detection systems would be able to tell the contextual anomalies from other anomalies, and response actions could be initiated correspondingly. To illustrate a concrete example, let's consider a set of web servers that will attract billions of requests on a particular day of the year, e.g., the Double 11 Festival (11.11) in Taobao. The high-rocketing number of the requests from the very beginning of the day would trigger lots of alarms in a typical intrusion detection system, indicating that the network performance indicators have shown abnormal behaviour that could be considered as suffering a large-scale DDoS attack. With the help of the contextual information, which tells the intrusion detection system that the abnormal request rate is normal on the day, the false alarms of the intrusion system will be

significantly reduced.

3. Performance Evaluation

This section presents the detailed results of the experiments conducted to evaluate the proposed approach. As a benchmark dataset, the A3Benchmark from Yahoo computing datasets [7] is selected for time series anomaly detection. More specifically, forty time series are randomly picked from the datasets for validation. To construct multi-dimensional data instances, time series embedding [3] is utilized and the contextual information of a data instance is set as its increment over the data instance that is one period ahead (the period of each dataset is known).

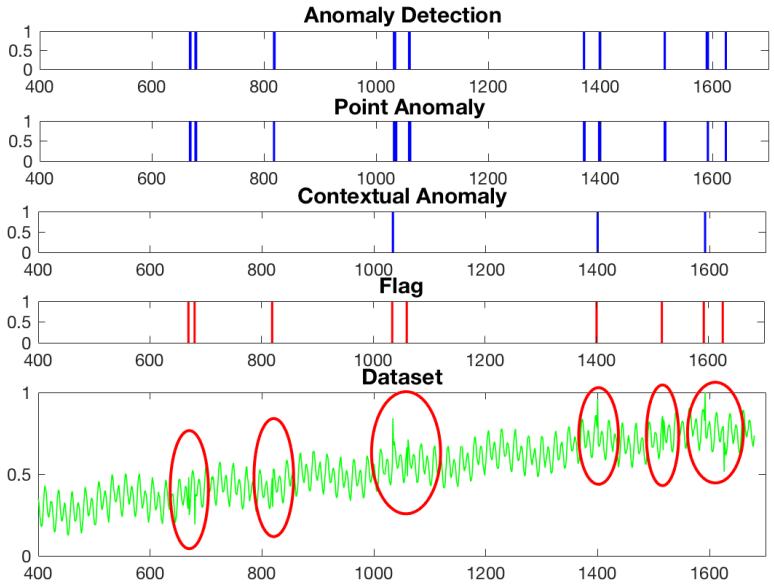


Figure 2. An Example of Experiments

Figure 2 shows an example of the experiments. In the 5th subfigure on the bottom, the original time series is demonstrated with manually marked anomalies, which is also depicted in the 4th subfigure. From the 1st subfigure on the top, it is clear that all the anomalies are detected without false alarms. The results in the 1st subfigure are obtained through checking Eq. (7), while the results in the 3rd and 2nd subfigures are generated with the discriminant functions in Eqs. (6) and (8) respectively. Note that the 2nd subfigure also identifies all the anomalies, but further interpret them as point anomalies. This is because these anomalies show strange patterns, e.g., an abnormal combination of data instances or an abrupt spike. On the other hand, the results in the 3rd subfigure identify 3 contextual anomalies, stressing that the abnormality of the corresponding data is also due to their anomalous contextual information, i.e., the abrupt increment. With the identification of the point anomalies and the contextual anomalies, the anomaly detection process provides more informative details about why a data is marked as anomalous. Consequently, one would be able to treat anomalies differently according to the additional information.

The experiments over the selected forty time series obtain an average F-score of 0.93 and also demonstrate similar results as that in Fig. 2, which reflects the effectiveness of the proposed method in further interpreting the anomalies. More specifically, according to the experiment

results, the proposed method is effective for distinguishing the contextual anomalies from the typical point anomaly and, therefore, achieves better anomaly interpretation for intrusion detection systems.

4. Conclusion

In this paper, an anomaly detection method, which can distinguish different anomalies, is proposed to provide more information for interpreting the anomalies. The method is based on integrating two linear programming SVDDs to support the training of two different types of information. Experimental results on forty time series datasets in Yahoo benchmark datasets demonstrate that the proposed method is capable of identifying different anomalies and thus enables better interpretation of the anomalies. As a result, the utilization of the method in intrusion detection systems will largely benefit the underlying decision-making systems in choosing the proper reaction when an anomaly is witnessed.

References

[1] S. Hawkins, H. He, G. Williams, R. Baxter, Outlier detection using replicator neural networks, *International Conference on Data Warehousing and Knowledge Discovery*, pp. 170-180, 2002.

[2] J. L. Hintze, R. D. Nelson, Violin plots: a box plot-density trace synergism, *The American Statistician*, vol. 52, no. 2, pp. 181-184, 1998.

[3] J. Ma, S. Perkins, Time-series Novelty Detection Using One-class Support Vector Machines, *IJCNN*, vol. 3, pp. 1741-1745, 2003.

[4] C. Manikopoulos, S. Papavassiliou, Network intrusion and fault detection: a statistical anomaly approach, *Communications Magazine*, vol. 40, no. 10, pp. 7682, 2002.

[5] D. M. J. Tax, R. P. W. Duin, Support Vector Data Description, *Machine Learning*, vol. 54, no. 1, pp. 45-66, 2004.

[6] V. Vapnik, A. Vashist, A new learning paradigm: Learning using privileged information, Neural Networks, vol. 22, no. 5, pp. 544-557, 2009.

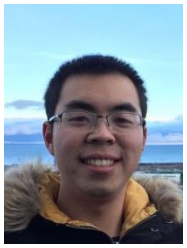
[7] Yahoo, S5-A Labeled Anomaly Detection Dataset, version 1.0, http://webscope.sandbox.yahoo.com/catalog. php?datatype=s&did=70, 2015.

Chengqiang Huang is currently a Ph.D. candidate in the Department of Mathematics and Computer Science, University of Exeter, United Kingdom. He received his master degree and the bachelor degree in Computer Science from Xidian University, China, in 2014 and 2011, respectively. His recent research mainly focuses on machine learning methods for anomaly detection and network management.

Zhengxin Yu is currently a Ph.D. candidate in the Department of Mathematics and Computer Science, University of Exeter, United Kingdom. She received her master degree in Information Technology Management for Business from University of Exeter, United Kingdom, in 2016 and bachelor degree in Information Management and Information System (English and Japanese Bilingual Extension) from Dalian University of Foreign Languages, China, in 2015. Her recent research mainly focuses on distributed

machine learning technologies.

Geyong Min is a Professor of High-Performance Computing and Networking in the Department of Computer Science within the College of Engineering, Mathematics and Physical Sciences at the University of Exeter, United Kingdom. He received the Ph.D. degree in Computing Science from the University of Glasgow, United Kingdom, in 2003, and the B.Sc. degree in Computer Science from Huazhong University of Science and Technology, China, in 1995. His research interests include Future Internet, Computer Networks, Wireless Communications, Multimedia Systems, Information Security, High-Performance Computing, Ubiquitous Computing, Modelling, and Performance Engineering.



Yuan Zuo is currently a Ph.D. candidate in the Department of Mathematics and Computer Science, University of Exeter, United Kingdom. He received his Bachelor degree in the University of Electronic Science and Technology of China, and Master degree in the National University of Defence Technology, China, in 2012 and 2014, respectively. His current research mainly focuses on machine learning and text data analysis for network management.

Ke Pei is currently a technical expert in RAS department of Huawei 2012Lab. He was a DMTS of lucent bell-labs and received his PhD degree from the Xidian university. His research rests on intelligent fault predictive and localization techniques based on AI/ML/data mining.

Zuochang Xiang is a senior software architect in Huawei Co. Ltd. He has more than 10 years' experience in developing software systems. His research interests include developing high-performance software systems with high reliability and general topics concerning the re- liability, availability, and serviceability (RAS) of software systems.

Geolocation-aware Cryptography and Interoperable Access Control for Secure Cloud Computing Environments for Systems Integration

Christian Esposito
Department of Computer Science, University of Salerno
esposito@unisa.it

1. Introduction

The cloud computing [1] consists in the elastic provisioning of computing and storing resources accessible throughout thanks to the Internet, by assuming an on-demand payment scheme. At the beginning, cloud computing was proposed as a solution for delivering computation as a public utility, and its usage was limited to companies in order to resolve their problems in owning and managing data centers. However, with the progressive increase of the bandwidth offered by the Internet, cloud computing has met a tremendous proliferation and acceptance by the masses, which started to extensively use it to rent computers on which to run their own applications, and/or to have a remote data storage usable from anywhere. This prolific usage of the cloud by both ICT professionals and common people is the cause of the evolution of the provided service models. At the origins, the cloud computing was limited to the Infrastructure as a Service (IaaS), where the cloud consists in a virtual infrastructure that mimics and makes accessible over the Internet the traditional physical computing hardware. Later on, we have witnessed the advent of more advanced higher-level models forming the so-called Cloud Computing Stack: Platform as a Service (PaaS), built on top of IaaS, represents the model of delivering hardware and software tools over the Internet, and Software as a Service (SaaS), built on PaaS, allows having applications hosted in the cloud and available to customers over the Internet. The widespread availability of the Internet connection due to the next generation of cellular and wireless networking, and the existence of cloud platforms with a massive amount of computing resources (which can be further enlarged thanks to the possibility of seamlessly federating multiple clouds [2]) is currently paving the way of a radical rethinking of multiple traditional ICT systems, where the cloud plays the crucial role, such as the sensory networks, the critical infrastructures for healthcare-related data management, or the manufacturing processes, just to cite the most prominent ones.

The technological advancement in the hardware miniaturization paved the way in the nineties to the advent of sensory networks, consisting in tiny sensing devices deployed within an area of interest, such as a forest, within a building or along a motorway, in order to measure certain environmental factors, such as temperature, humidity, vibrations, pollution and so on. Such devices are characterized by short-range wireless communication means so that they can exchange messages with special nodes, called base stations. These special nodes, thanks to stable wired communication means, are able to interact with a centralized remote server in charge of collecting all the data and performing complex analytics on them and exposing them by means of proper visualization means to a human operator. The lower costs of the hardware are making possible to tag everyday object with these sensing devices, so as to progressively increase the size of these sensory networks, and to let the amount of data exchanged with the centralized server, and the complexity of the analytics required to be conducted on such data, growing exponentially. Such a novel class of sensory networks is known in the literature as the Internet of Things (IoT) [6], where the big data flowing from the sensing part of the network has rapidly overwhelming the capacity of a traditional computing commodity and calling for more elastic provisioning of computing and storing capabilities. For this scope, the cloud computing, which has virtually unlimited capabilities, has started to being used within the context of sensory networks, so as to cope with the demands of dynamic and adaptable resource provisioning. Moreover, the current sensing devices are starting to have networking chips able to realize longer range communications and to directly communicate with the centralized cloud-based server. This allows the tiny sensing devices to expose themselves as a service, and having the cloud to be more than a mere means to satisfy its technological demands in terms of storage and processing, but to also serve the overall IoT as a way to realize IoT application by letting developers to manage and composite IoT devices as services. In fact, the cloud plays the role of an intermediate layer between the sensing devices and the applications, by hiding all the details for communicating with the sensing devices and the complexity to implement the application. Currently, the role of the cloud computing within the IoT is further evolving in more structured and complex architectures, so as to augment the provided scalability and flexibility [3].

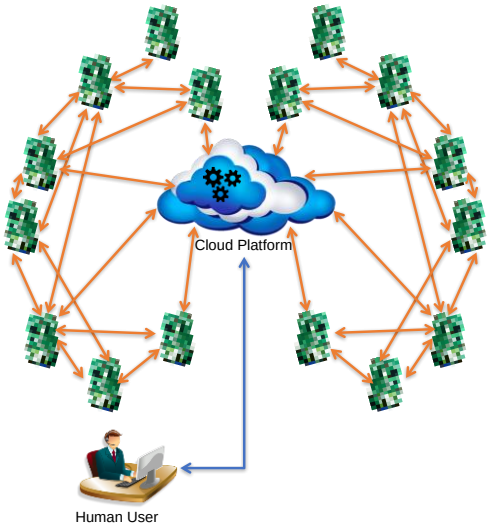


Fig. 1: Integration of sensory networks and the cloud computing, leading to the so-called Internet of Things.

Healthcare is a data intensive application domain, where the personnel of healthcare providers needs updated information on the patients so as to offer them the best care. The progressive dematerialization of the healthcare documents, such as test results, referrals or hospital dismissal letters, is causing the problem of having healthcare providers to own and manage proper data centers of the storage of the electronic healthcare documents, which implies considerable costs of acquiring and maintaining such ICT commodities. Moreover, the recent phenomenon of patient mobility, where patients receives healthcare services far from their residence area due to tourism or economic and quality reasons, is calling for suitable means to share electronic healthcare documents among providers within a given country or even across a country boundary. Cloud computing is starting to be considered a winning solution for these two problems, since it is able to provide data management capabilities to healthcare providers without implying in the enormous costs of a physical data center, and to offer an Internet-based ubiquitous accessibility that is required for the healthcare data sharing among providers within a country and across multiple countries [4]. As illustrated in the Fig. 2, a cloud-based infrastructure, both a private or a public one, can be used in order to deal with all the data management challenges that a healthcare provider exhibits in order to deal with all the electronic documents produced during the provided healthcare services, from hospitalization to medical tests, and to keep the identities of the staff authorized to access to certain hosted documents. In order to treat patient mobility, the different cloud-based solutions can be federated by means of an inter-cloud solution [2], so as to allow the efficient and effective share of healthcare data among providers through their cloud solution without the users being aware of where the data resides (locally within the healthcare provider or remotely at the premises of another provider).

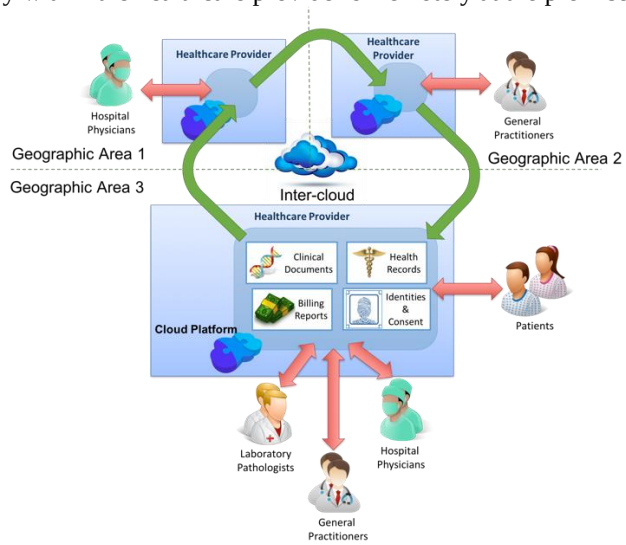


Fig. 2: Cloud-based medical data management within a healthcare provider and among different providers.

The manufacturing domain is characterized by a great pressure on the companies to rapidly respond to the market needs, which is extremely volatile and globalized, targeting multiple potential customers around the world, and cutting the production costs and time by keeping a high-quality of the manufactured products. To address such challenges, a networked organization of the manufacturing firms emerged so as to interconnect multiple production sites and allow the exchange products, services and knowledge to improve company flexibility, productivity and competitiveness at the international level. Such a collaborative approach can be implemented within a firm, but has been recently adopted also among firms so that multiple companies can join their forces so as to overcome their limits. The cloud computing has started to be adopted in order to support such a vision, leading to the so-called Cloud Manufacturing [5], illustrated in Fig. 3. Specifically, each firm has its management applications hosted within a cloud platform, which can be private of public, such clouds can be interconnected by means of a network so that data exchange is possible in a seamless manner. Apart from this naïve use of the cloud computing, the cloud manufacturing consists in virtualizing and offering the manufacturing resources of each firm as a cloud service hosted in a centralized cloud, as illustrated in the figure. Such services can be used by users to realize complex manufacturing business by properly composing, scheduling, monitoring and controlling such services.

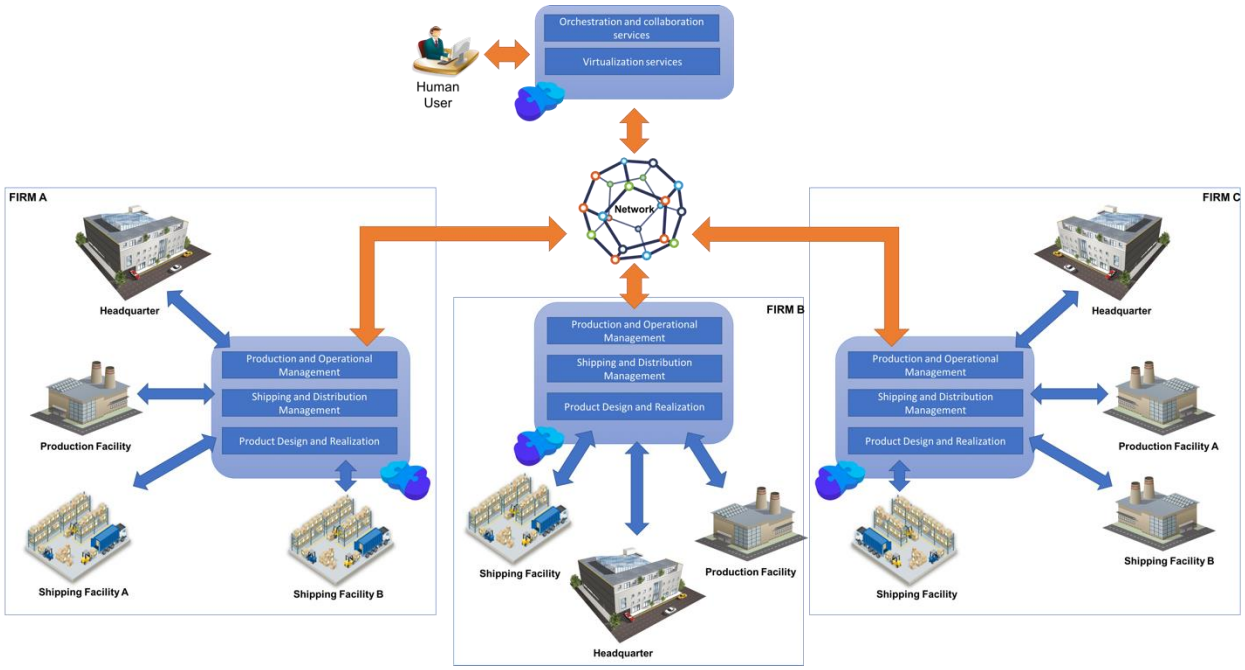


Fig. 3: Collaborative manufacturing approach among multiple firms realized by means of cloud computing.

2. Security and Privacy Issues in Cloud Computing

As above mentioned, cloud computing is extensively used in many ICT contexts and domains, and most of them consists in using the cloud computing for collaboration, exchange and processing of data that is characterized to be critical, both because contain sensitive information on the users and/or companies, or because the data is valuable for the achievement of the mission of the applications running within the cloud. As a concrete example, healthcare data can contain private information on patients, such as HIV test outcomes, psychological profiles or social security number, whose exposure can compromise the reputation and/or life of the patients. Cloud manufacturing vehicles business critical data of the interconnected firms, such as confidential and copyrighted information on a particular manufacturing design, production plan or commercialization strategy, that malicious employees may use for blackmailing their employers, or competitors may be willing to obtain in order to copy innovative upcoming products or improve their own product to the detriment of the competitor's product. Last, the sensing data may reveal habits of the users so as to let thefts to plan a house burgled. In addition to the protection of the data confidentiality, our daily activities are tightly coupled with the successful behavior of the cloud platforms, that must be protected against possible cyber-attacks aiming at compromise their availability and/or their correct behavior. As a practical example a Denial of Service attach can target a cloud platform hosting the management services of a healthcare provider, making them unavailable so that doctors are not able to retrieve their patients' documents for a

certain time window, or a solution of cloud manufacturing may be compromised causing a sudden stop of the production and shipping activities of the affected firms. Another kind of example is the injection of false data or the tampering of real sensing data so that the application running within the IoT may take the wrong decisions, with the effect of causing losses of human lives, of money and the application reputation. Therefore, security and privacy of the cloud computing is starting to be demanding since the data hosted in the cloud is sensitive and the cloud is itself important for the successful execution of several critical processes.

The terms governing the relationship between the cloud service provider (CSP) and its customers are contained in the Service Level Agreement (SLA) [11], which is a contractual obligation for the quality of the services provided by the CSP and codifies the specific parameters and minimum quality levels required for the provided service, such as how ensuring data security. Traditionally, the typical security requirements that a communication infrastructure must satisfy encompass data confidentiality and integrity, and attack protection. Specifically, the data outsourced to the cloud and stored in it should be protected from stealing, tampering or falsification done either by external attacks perpetrated by malicious adversaries trying to get access from the cloud front-end, and by internal attacks conducted by the staff employed at the cloud provider. The confidentiality of data is crucial, so that the available cloud solutions have been be enforced by running proper access control policies [8] so that data can be retrieved only by authorized entities, and by using encryption for data at rest [9] so that malicious insiders are not able to retrieve understandable information from the cloud. Moreover, data may be modified without its owner being notified, which can use the modified data to make critical decisions. The integrity of outsourced data is important and must be guaranteed; therefore, most of the marketed cloud platforms are equipped with proper integrity schemes [10], such as Provable Data Possession (PDP), Compact Proofs of Retrievability (CPOR), or Dynamic Provable Data Possession(DPDP). In addition to the traditional security challenges exhibited by the communication systems when used in critical scenarios, the cloud computing presents novel and peculiar challenges due to its Internet-based accessibility, the multi-tenant environments, and the elastic resource provisioning.

On the one hand, data location is uncertain when using cloud computing, especially in the case of cloud federation. In fact, the elastic provisioning of storage and the guarantying of Quality-of-Service properties, such as availability or timeliness, can cause the replication and the migration of the outsourced data across multiple machines of the cloud infrastructure without the data owner being aware of such movements and where exactly his/her data has been placed and how many replicas exist. This negatively impacts the data privacy and can also have serious legal consequences [12], since data may reside in different legislative domains, where some may have with less stringent guarantees on privacy protection and data disclosure. As a concrete example, the European Union (EU) Data Protection Directive states that any personal data generated within the EU is subject to the European law, can be shared with third parties if its owner is notified and cannot leave the EU unless it goes to a country that provides an adequate level of protection. On the contrary, in the United States (US), the Patriot Act allows US intelligence agencies to access personal data managed by US companies without notifying data owners, so as to enhance domestic security against terrorism by surveying suspected terrorists. The mentioned EU directive and the US Patriot Act are in conflict regarding to the disclosure requirements, and this arises serious issues: if EU citizens' data, hold by a data center owned or operated by a US company, has to be released under the US Patriot Act, there will be a violation of the EU Data Protection Directive. Moreover, there is also the case of countries aiming at protecting the data related to its critical infrastructures from enemy aliens, which are any natives, citizens, or organizations of any foreign nation or government with which a government is in conflict with. As a concrete example, the data related to critical infrastructures in the US should not be stored or made available to anyone located in the US Office of Foreign Assets Control (OFAC) sanctioned countries.

In the SLA negotiated between the CSP and the customer, there may not be indicated the exact geographic location where outsourced data may reside, raising disputes in the case of particular sensitive data that are not allowed to be stored away from the US, or the export of personal data from the EU. But, even in the case this is stated, the customer cannot solely rely on such contractual agreements in order to protect its data from a legislative context with soften privacy protection rules. It is needed a way to take control over the possible data replication and movements, called as data sovereignty, so that the above-mentioned issues are limited and/or nullified.

On the other hand, the cloud is typically used by multiple disparate organizations as an integration and collaboration means (as seen in the healthcare and manufacturing domains), each characterized by proper access control models and policies, which must coexist and interoperate in order to achieve a collaboration among the organizations. It is impossible to impose a single access control model, such as a role-based or an attribute-based one. This is mainly

due to the fact that there is no agreement on the most suitable and effective access model when integrating multiple organizations, but also because it will consist in rethinking the internal access control rules of the integrated organizations and is not reasonable or profitable to undergo. Even if a common model may be possible to determine, each organization can assume a proper syntax and semantics to formulate its own set of access control polies, which differ from the ones adopted by the others. Therefore, it is strongly desirable to have a flexible authorization solution that can welcome any given access control model with which a particular entity is confident, and to overcome possible syntactical and semantic divergences in an automatic manner.

3. Data Sovereignty and Semantic Access Control in the Cloud Computing

The naive solution to achieve data sovereignty within the context of cloud computing has been so far to limit the movements of the outsourced data by letting them staying with a precise geographical region respecting precise legislation awareness policies, according to the obligations within the negotiated SLA [14]. The verification of these geo-location and legislation awareness policies is conducted in order to have proofs of the compliance and respect of these contractual obligations when storing data in a cloud infrastructure [15]. Such a solution has twofold drawbacks:

- on the one hand, it limits the elastic and adaptive resource provisioning feature that characterizes the success of cloud computing, since the CSP is not able to perform its internal data management strategies in order to achieve effective and efficient resource usage;
- on the other hand, the users do not have guarantees that data is not replicated and the replicas moved to other locations so as to avoid the SLA verification and violate the SLA obligations.

Such solution impose that the user must have faith in the CSP to always do the right thing and behave according the SLA. However, this is a bind trust for the users that make them and their data vulnerable to possible security threats of a malicious or corrupted insider or CSP. The data sovereignty is not limited to the possible data flows within the cloud solution, but has a wider context. In fact, the cloud is used to share access to outsourced data with other consumers or organizations, as long as they have an Internet connectivity, even if they are located in a different geographic location, which may have a different data protection legislature. Realizing data sovereignty consists also in avoiding data to be shared through the cloud with users in conflicting legal frameworks or enemy aliens with respect to the data owner. This last issue may be approach with a proper access control solution, by integrating the location attribute as part of the credential to be acquired and verifying in order to allow or deny an access to the cloud, but this does not allow to have control if the data retrieved from the cloud may be sent toward un-allowed geographic areas.

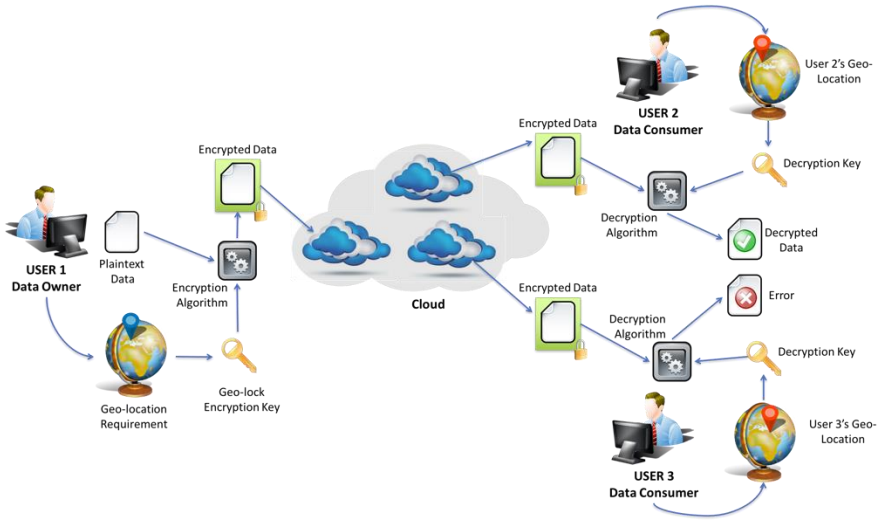


Fig. 4: Schematic view of an encryption-based solution for data sovereignty in the cloud computing.

We posit that geo-location and legislation-aware data restrictions, coupled with SLA verification and access control, are not effective to achieve data sovereignty within the cloud computing, even if federated, and that a more suitable approach can be to exploit a geolocation-aware cryptographic scheme, which can be constructed based on the

widely-known Attribute Based Encryption (ABE) [16], by using the available cryptographic primitives offered by the available CSP or adopting an additional encryption layer on top of the available one. Such a solution has three beneficial effects: (i) removing the blind trust in the CSP for respecting and enforcing the respect of location requirements expressed in the SLA, (ii) avoiding to have the outsourced data being subject to foreign law with less guarantees than the one of the data owner, since CSPs cannot be forced to provide data to which it has no access and (iii) neglecting the case of data obtained from the cloud to be distributed within a forbidden geographical area by a malicious user. A tentative location-aware cryptographic solution is illustrated in Fig. 4, where the data owner, indicated as user 1 in the figure, selects a desired geographic area where his/her data can be understandable, and obtains a suitable encryption key, built on top of the selected geographic attribute. Therefore, the data can be encrypted by the user and outsourced to the cloud, which can add its own encryption scheme, with the relative key management strategy. The data hosted within the cloud can be accessible by two kinds of users: one within the allowed area, namely the user 2 in the figure, and the ones with of a forbidden location, i.e. user 3 in the figure. Both users must estimate their own solution and obtain a decryption key from their current location, which is further used in order to decrypt the obtained data, but only the user 2 is able to achieve the plaintext of the retrieved data, while the other one fails.

The issue of having an interoperable access control solution when the cloud computing integrate multiple organizations with heterogeneous authorization policies and models can be approach only by formally describing the access control model to make interoperable, so as to semi-automatically resolve the differences and match the different models. This consists in exploiting an ontological representation of the access control models, where the subjects, their attributes and any other elements of the access control policies are precisely described as elements within an ontology. Such ontological representation is able to cope with the case of divergence in the adopted class of affinity, e.g., Role-Based or Policy-Based Access Control models, but also the case of term heterogeneity and mismatch. In fact, an ontology is able to relate terms that are syntactical different but share the same semantic. By adopting a semantic access control, the allowing or denying decisions are taken based on rules formalized as queries expressed in the SPARQL language, able to retrieve and manipulate data stored in the Resource Description Framework (RDF) format of an ontology.

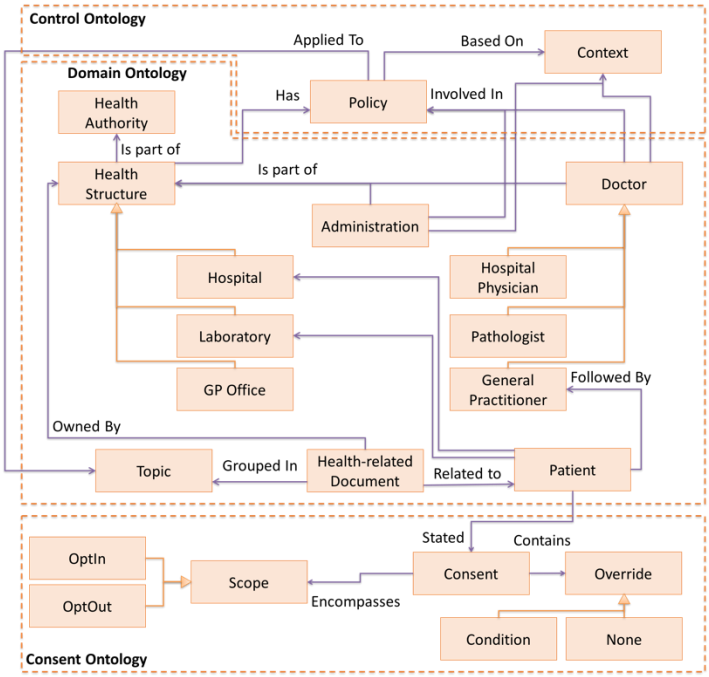


Fig. 5: Example of the ontological formalization of an access control model for the healthcare domain.

Fig. 5 provides an example on how to model the set of authorization policies for the cloud computing when used to interconnect healthcare providers, where the overall ontology is structured in three distinct parts:

- The first part is called the Domain Ontology, and models the context of usage of the cloud platform, and in the figure, we have modelled all the entities involved in the application domain of interest, specifically the

healthcare one in the figure. Specifically, all the potential users of the cloud solution for the healthcare data exchange has been identified, their possible employing healthcare providers have been identified and the dependencies of the users with these providers have been determine, and the relation of the data with these entities has been formalized.

- The second part is named as Control Ontology and formalizes the set of security policies and restrictions agreed by an organization, based on a specific access control model. In the figure, a Policy-Based Access Control approach has been described, with the indication of context-aware security policies and their relations with the entities of the Domain Ontology so as to determine the allowed accesses that each subject can obtain.
- The last part is the Consent Ontology, and describes the user consent to share its own sensitive data through the cloud, and in the figure, we have considered the semantic modeling of patient consent in [17], based on the study described in [18] to express specific conditions for controlling accesses to the electronic healthcare information of a patient.

The provided example is just explicative and do not means that such an approach is applicable to a given domain, access control model, or consent approach, but they can be selected at pleasure. The decision to allow or deny an access request to the cloud can be taken by considering the security claims provided by the requestor and running a series of SPARQL predicates, whose parameters are valued with attributed in the received claim, on the ontology populated with real data gathered on the healthcare providers' real employees and patients. Considering the syntax of SPARQL, in our work we have used the ASK form forms as a means to express access rules. The Boolean return of the ASK queries are intended as a permission to access the requested resource or not.
When the cloud interconnect multiple heterogeneous organizations, more than one ontologies are present and must be matched among themselves. Matching diverse ontologies is still an open issue in the current literature and a survey on this topic is available in [19]. In our work, we have adopted a simple approach based on the semantic similarity of the terms composing two diverse ontologies, and the graph similarity of the dependencies among similar terms. After such a mapping is applied, the requests from an organization can be transformed by using the mapped terms of the receiving organization and verified on this organization's ontology. To this aim, there is no difference if such a request is received by a user belonging to the same organization of the controller or by a remote one, whose access control has joined the one that has received the request.

5. Conclusion

The progressive success of cloud computing made it pervasive within our society and available to professional and/or regular customer. In addition, the cloud has imposed itself as a powerful integration means in order to interconnect several legacy systems and let them exchange data among its self and among different companies' staff. The criticality of the data exchanged through the cloud by companies and regular customers, and the pivotal role of the cloud in critical infrastructures imposes the respect of stringent security and privacy required by cloud platforms. To this aim, the available marketed cloud platforms have been equipped with traditional security and privacy enhancement solutions such as cryptographic primitives, access control or security audit. However, the cloud computing is also subject to peculiar and unseen requirements, such as data sovereignty and interoperable access control, which have not been treat, yet. In this paper, we have briefly introduced such novel challenges and the promising solutions we are investigating in order to deal with them.

References

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7-8, May 2010.
[2] N. Grozev, and R. Buyya, "Inter-Cloud architectures and application brokering: taxonomy and survey", Software Practice Experience, vol. 44, no. 3, pp. 369-390, March 2014.
[3] C. Esposito, A. Castiglione, F. Pop, and K.-K. R. Choo, "Connecting Edge and Cloud Computing: A Security and Forensic Perspective", In Press at the IEEE Cloud Computing, 2017.
[4] V. Casola, A. Castiglione, K.-K. R. Choo, and C. Esposito, "Healthcare-Related Data in the Cloud: Challenges and Opportunities", IEEE Cloud Computing, vol. 3, no. 6, pp. 10-14, November-December 2016.
[5] C. Esposito, A. Castiglione, B. Martini, and K.-K. R. Choo, "Cloud Manufacturing: Security, Privacy, and Forensic Concerns", IEEE Cloud Computing, vol. 3, no. 4, pp. 16-22, July-August 2016.
[6] L. Atzori, A. Iera, and Giacomo Morabito, "The Internet of Things: A survey", Computer Networks, vol. 54, no. 15, pp. 2787-2805, October 2010.

[7] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey", Future Generation Computer Systems, vol. 56, pp. 684-700, March 2016.
[8] M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions", Journal of Systems and Software, vol. 86, no. 9, pp. 2263-2268, September 2013.
[9] M. Y. Shabir, A. Iqbal, Z. Mahmood, and A. Ghafoor, "Analysis of classical encryption techniques in cloud computing", Tsinghua Science and Technology, vol. 21, no. 1, pp. 102-113, February 2016
[10] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, N. Javed, M. Alam, and F. Jamil, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends", Computers & Security, vol. 65, pp. 29-49, March 2017.
[11] Q. Zhang, L. Cheng, R. Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7-18, May 2010.
[12] C. Esposito, A. Castiglione, and K.-K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated Clouds", IEEE Cloud Computing, vol. 3, no. 1, pp. 12-17, January-February 2016.
[13] C. Esposito, A. Castiglione, and Francesco Palmieri, "Interoperable Access Control by Means of a Semantic Approach", Proceedings of the AINA Workshops, pp. 280-285, May 2016.
[14] N. Paladi, M. Aslam, and C. Gehrmann. Trusted geolocation-aware data placement in infrastructure clouds. Proceedings of the IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 352-360, 2014.
[15] D. L. Fu, X.G. Peng, and Y.L. Yang. Trusted validation for geolocation of cloud data. The Computer Journal, 2014.
[16] J. Hur, and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
[17] A. Khan, H. Chen, and I. McKillop, "A semantic approach to secure electronic patient information exchange in distributed environments", Proceedings of the Annual Conference of the Northeast Decision Sciences Institute (NEDSI), 2011.
[18] E. Coiera, and R. Clarke, "e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment", Journal of the American Medical Informatics Association, vol. 11, no. 2, pp. 129-140, 2004.
[19] E. Rahm, and P. Bernstein, "A survey of approaches to automatic schema matching", The VLDB Journal, vol. 10, no. 4, pp. 334-350, 2001.

Christian Esposito received the M.S. degree in computer engineering from the University of Napoli "Federico II" in Italy in 2006, and Ph.D. degree in computer and automation engineering from the same university, in 2009. He is now an adjunct professor at the University of Napoli "Federico II", and at the University of Salerno, where he is also a research fellow, respectively since 2014 and 2016. His main interests include mobile computing, benchmarking, aspects of publish/subscribe services, and security and reliability strategies for data dissemination in large-scale critical systems. He regularly serves as a reviewer in international journals and conferences in the field of Distributed, Secure and Dependable Systems.
Contact him at christian.esposito@unina.it or esposito@unisa.it.

Cloud Data Deduplication Scheme Based on Game Theory

Xueqin Liang[1], Zheng Yan[1, 2]
[1]State Key Lab of Integrated Networks Services, School of Cyber Engineering, Xidian University, Xi'an, China
[2]Department of Communications and Networking, Aalto University, Espoo, Finland
Dearliangxq@126.com, zyan@xidian.edu.cn

1. Introduction

Cloud computing is a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources [1]. Lots of cloud storage service providers (CSPs) emerge in accordance with the needs of the times and have been widely used by lots of people all over the world.

Some security problems arise due to the rapid development of data analysis technologies and are worked out by storing encrypted data only. What's more, with tremendous number of users, there also comes another problem, duplicated storage. Existing deduplication schemes either cannot handle encrypted data [2] or are processed at client side [3] that cannot ensure efficiency. An encrypted cloud data deduplication scheme based on data ownership challenge and Proxy Re-encryption (PRE) [4] was proposed. Its performance has been verified theoretically.

However, the existence of collusion between malicious CSPs and dis-honest data users makes data holders lose high profits, which causes more and more data holders refuse to adopt this deduplication scheme. Public goods dilemma happens when the deduplication rate of the Internet environment decreasing with the existence of malicious activities. To solve this dilemma, we need to analyze the utilities of all players based on a mechanism that can adjust the utilities to arouse their willingness to make contributions to the system, based on the game theoretical method that has been widely used to remove social problems in the practical deployment of schemes [5, 6].

2. System model and payoff analysis

The details of this data deduplication scheme can be found in [4]. Incentive mechanism which can be used to punish the dishonest actions of CSPs and users and make compensation to data holders whose data has been disclosed is needed to improve its practice. We assume the dishonest actions can be detected by Authorized Party (AP) and the punishment fee is related to the number of data owners whose data have been disclosed and Insurance fee of CSP is related to the number of data stored in it.

We set up an economic model to help analyze the acceptance of the target deduplication scheme. The utility functions of all entities are specified based on the interactions of data holders and CSPs.

If a data holder has no faith in this scheme will choose to store locally and we represent its utility as $cf_h(t)$. If it stores data at CSP can obtain benefit $b_h^c(t)$ and access fee $af_h^c(t)$ from data users, storage fee $sf_h^c(t)$ should be paid to CSP as well. When the CSP it stores at is malicious, it may suffer loss $l_h^u(t)$ for data leakage. With incentive mechanism, it can get compensations $Cf_{AP}^{h,u}(t)$ from AP when data leakage happens. Note that if the CSP adopts deduplication scheme, the storage fee can be adjusted by a parameter α.

CSP can obtain storage fee from all the data holders who choose to store at it and download fee $df_u^c(t)$ from data users. Providing storage services also need cost $oc_C^c(t)$ which is proportional to the number of data. If CSP colludes with dishonest users can get extra malicious fee $m_u^c(t)$ as well. While a CSP adopting the deduplication scheme should pay yearly fee $yf_c^{AP}(t)$ and insurance fee $If_c^{AP}(t)$ to AP.

Honest data user can get profit $w_u^h(t)$ by accessing data holder's data while it should pay download fee and access fee as well. If the data user is dishonest, by paying malicious fee and download fee to malicious CSP, it can obtain profit $w_u^h(t)$ and illegal benefit $ib_u^h(t)$. While with the incentive mechanism, his dishonest action will be detected and will be punished by AP with punishment fee $Pf_u^{AP,h}(t)$.

Based on the above analysis, we can see that AP only makes profits when all entities accept the deduplication scheme. And its utility contains yearly fee and insurance fee from all CSPs, punishment fee paid by dishonest entities and compensation fee paid to data holders. It needs to pay a cost $OC_{AP}(t)$ to provide service as well.

3. Public goods based deduplication game

We will discuss the acceptance of different system entities on the deduplication scheme and how the social dilemma is mitigated after a number of time generations in this part.

Table 1. the utilities of data holder with different strategies

Strategies	Utility functions
Store locally	$cf_h(t)$
Store at honest CSP without deduplication	$b_h^c(t) - sf_h^c(t) + af_h(t)$
Store at dishonest CSP without deduplication	$b_h^c(t) - sf_h^c(t) - l_h(t)$
Store at honest CSP with deduplication	$b_h^c(t) - \alpha \times sf_h^c(t) + af_h(t)$
Store at dishonest CSP with deduplication	$b_h^c(t) - \alpha \times sf_h^c(t) + Cf_{AP}^h(t) - l_h(t)$

The rapid development of the Internet and the fast improvement of cloud services make the cost of CSPs lower and lower. Therefore, we make a reasonable assumption that $b_h^c(t) - sf_h^c(t) > cf_h(t)$for each data holder. We can set $Cf_{AP}^h(t) \approx l_h(t)$ to make sure data holder will not suffer a big loss due to data leakage. The deduplication scheme offering compensation can benefit the data holders if their data is stored at honest CSPs and can make the loss of the data holders that store data at dishonest CSPs lower. Overall, applying the deduplication scheme with compensation can encourage data storage at the cloud with the acceptance of data holders.

Table 2. the utilities of CSP with different strategies

Strategies	Utility functions
Honest CSP without deduplication	$sf_c(t) + df_c(t) - oc_c(t)$
Dishonest CSP without deduplication	$sf_c(t) + df_c(t) + mf_c(t) - oc_c(t)$
Honest CSP with deduplication	$\alpha \times sf_c(t) - If_c^{AP}(t) - yf_c^{AP}(t) + df_c(t) - oc_c(t)$
Dishonest CSP with deduplication	$\alpha \times sf_c(t) - If_c^{AP}(t) - yf_c^{AP}(t) + df_c(t) + mf_c(t) - oc_c(t)$

In the short run, no matter a CSP choose deduplication or not, be dishonest can bring it a higher reward. However, data leakage will make data holder who stores at dishonest CSP without deduplication have no confidence in cloud storage and bring it larger insurance fee which is proportional to the number of its malicious actions. Through proper parameters setting, the utility of dishonest CSP is less than that of honest from a long-term perspective. Through the above analysis, we can obtain that deduplication scheme can increase the utility of CSP and the introduction of compensation mechanism can suppress the dishonest actions of CSP and improve the deduplication rate of the network.

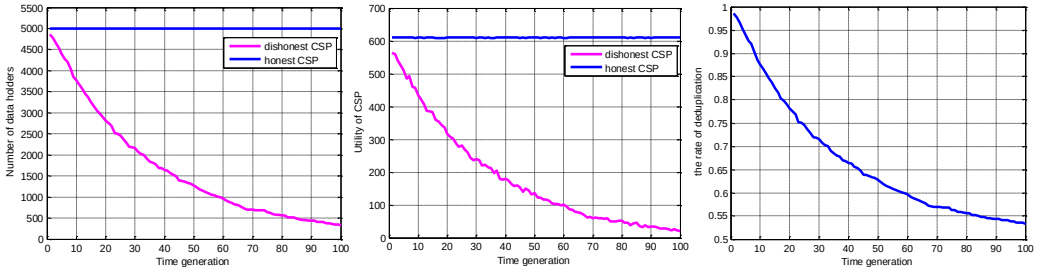
4. Evaluation: simulation results and analysis

We also conduct some experiments to show the effectiveness of our proposed model. In our simulations, we designed an environment with 10000 unit data needed to store and 70% of them can be deduplicated. There are two CSPs, each of which can store 10000 unit data. Parameters settings can be seen from Table 3. The price of storage-related fee was set based on [5], and the other parameters were set to ensure the utility of each entity is nonnegative.

Table 3. simulation settings

Symbols	Values	Symbols	Values	Symbols	Values
$sf_h^c(t)$	0.165	$df_u^c(t)$	0.1	$ib_u^h(t)$	1.5
$b_h^c(t)$	2.165	$yf_c^{AP}(t)$	20.0	If	0.05
$cf_h(t)$	0.9	$OC_{AP}(t)$	20.0	$Pf_u^{AP,h}(t)$	1.5
$af_h(t)$	1.0	$m_u^c(t)$	1.2	α	0.8
$l_h(t)$	1.0	$w_u^h(t)$	1.5	oc	0.05

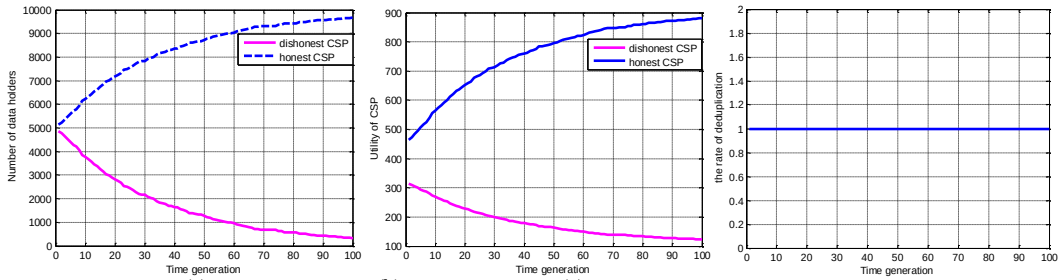
In the first experiment, we assume there are two CSPs, one is honest that will not collude with data users and the other can be easily allured to act dishonestly by dishonest data users. Punishment and compensation mechanism has not been applied either. All these 10000 unit data are equally stored at these two CSPs initially. There are 100 data users require to access data in each time generation as well. Once data leakage happens, data holder would start to store data locally because of the high data transfer costs. The first graph in Fig. 1 shows the number of data holders at honest CSP stays stable while that of data holders at dishonest CSP drops gradually. And the decline of the number of data holders causes great loss to CSP even if it can gain malicious fee from data users. The deduplication rate decreases and stays around 0.5 after 100 game times.



(a) (b) (c)

Fig.1 the number of data holders, the utilities of CSPs and the rate of deduplication in different time generations

In the second experiment, the general settings are the same as those in the first experiment, except that incentive mechanisms are introduced here. The compensation mechanism will make data holders still have faith in cloud storage and the compensation fee can support them to change to another honest CSP. Fig. 2 illustrates data holders in dishonest CSP will gradually transfer their data to the honest one, and the honest CSP will gain more profit due to the increase of data holders. What's more, no matter how data holders transfer their data from one CSP to another, their data are still deduplicated stored at cloud.



(a) (b) (c)

Fig.2 the number of data holders, the utilities of CSPs and the rate of deduplication in different time generations

5. Conclusion

Data duplication causes CSP too much time and space in processing. A deduplication scheme was proposed to handle encrypted cloud data especially big data. Its accuracy and security have been testified, but as we stated before, whether this scheme can be implemented successfully depends on the acceptance and behavior of all the participants. The dishonest actions of data users and CSPs driven by the natural of self-interest make data holders disappointed at cloud storage environment and repulsive to store data at cloud. Not to mention adopting deduplication scheme. Data users and CSPs cannot gain more interests in the long term, which is how the social dilemma emerges. We considered the deduplication rate of the environment as public goods and proposed public goods based deduplication game to analyze the acceptance of this scheme. Theoretical analysis and practical experiments have proven the effectiveness of this scheme in raising the deduplication rate of the system when data users have not been considered. Incentive mechanisms are introduced to suppress the malicious behaviors of data users and CSPs. Our study can work as a concrete confirmation of our previous work [5] and show the practical business model for successful deployment.

Acknowledgement

This work is sponsored by the National Key Research and Development Program of China (grant 2016YFB0800704), the NSFC (grants 61672410 and U1536202), the 111 project (grants B08038 and B16037), the Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), and Aalto University.

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology: U.S. Department of Commerce*, Special Publication 800-145, 2011.

[2] W.K. Ng, Y. Wen, and H. Zhu, "Private Data Deduplication Protocols in Cloud Storage," *Proc. 27th Ann. Acm Symp. Applied Computing (SAC'12)*, pp. 441-446, 2012.

[3] X.L. Xu and Q. Tu, "Data Deduplication Mechanism for Cloud Storage Systems," *International Conf. Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 286-294, 2015.
[4] Z. Yan, W.X. Ding, X.X. Yu, H.Q. Zhu, and R. H. Deng, "Deduplication on Encrypted Big Data in Cloud," *IEEE Trans. Big Data*, vol. *2*, no. 2, pp. 138-150, 2016.
[5] L.J. Gao, Z. Yan, and L.T. Yang, "Game Theoretical Analysis on Acceptance of a Cloud Data Access Control System Based on Reputation," *IEEE Trans. Cloud Computing*, vol. PP, no. 99, 2016.
[6] Y. Shen, Z. Yan, and R. Kantola, "Analysis on the Acceptance of Global Trust Management for Unwanted Traffic Control Based on Game Theory," *J. Computers and Security*, vol. 47, no. C, pp. 3-25, 2014.

Xueqin Liang received the B.Sc. degree on Applied Mathematics from Anhui University, Anhui, China, 2015. She is currently working for her PhD degree in Cyberspace Security at Xidian University, Xi'an, China. Her research interests are in game theory based security solutions, cloud computing security and trust, and IoT security.

Zheng Yan (M'06, SM'14) received the BEng degree in electrical engineering and the MEng degree in computer science and engineering from the Xi'an Jiaotong University, Xi'an, China in 1994 and 1997, respectively, the second MEng degree in information security from the National University of Singapore, Singapore in 2000, and the Licentiate of Science and the Doctor of Science in Technology in electrical engineering from Helsinki University of Technology, Helsinki, Finland in 2005 and 2007. She is currently a professor at the Xidian University, Xi'an, China and a visiting professor at the Aalto University, Espoo, Finland. She authored more than 150 peer-reviewed publications and solely authored two books. She is the inventor and co-inventor of about 60 patents and PCT patent applications. Her research interests are in trust, security and privacy, social networking, cloud computing, networking systems, and data mining. Prof. Yan serves as an associate editor of Information Sciences, Information Fusion, IEEE Internet of Things Journal, IEEE Access Journal, JNCA, Security and Communication Networks, etc. She is a leading guest editor of many reputable journals including ACM TOMM, FGCS, IEEE Systems Journal, MONET, etc. She served as a steering, organization and program committee member for over 70 international conferences. She is a senior member of the IEEE.

Securing DNS-Based CDN Request Routing

Zheng Wang[1], Scott Rose[1], Jun Huang[2]
[1]National Institute of Standards and Technology
[2]Chongqing Univ of Posts and Telecom, Chongqing, China
zhengwang98@gmail.com, scott.rose@nist.gov, xiaoniuadmin@gmail.com

1. Introduction

Content Distribution Networks (CDNs) have emerged and evolved for CDN providers to deliver content over the Internet for their CDN customers in an efficient, scalable, and secure manner. CDN request routing techniques are generally used to direct a client request to a suitable surrogate server that best serves the request. Most commercial CDN providers make use of DNS-based request routing mechanism because of the universal availability of the DNS infrastructure. In a typical version of that mechanism, the DNS requests for the site domain owned by the CDN customer are redirected to the CDN domain owned by the CDN provider, which then returns the request routing by resolving the CDN domain [1], [2]. As a security feature of DNS, DNSSEC (Domain Name System Security Extensions) was designed to provide source authentication and data integrity by digitally signing DNS resource records (RRs) [3]. By building the chain of trust and verifying the digital signature, DNS clients can validate the authenticity of DNS responses. In the past decade, the deployment and usage of DNSSEC is growing but still relatively low, due to complexity and lack of support. So a trust gap emerges when the CDN customer secures its site domain using DNSSEC but the CDN provider leaves its CDN domain insecure. As the validating resolver fails to build a chain of trust from a pre-configured trust anchor (usually the root) to the request routing, the request routing is still vulnerable in spite of the DNSSEC support from the CDN customer. Some prior work focused on the certificate security of HTTPS-based CDNs [4], [5] which is an issue in parallel with the trust gap problem addressed by our work. In this letter, we propose an extension for the DNSSEC chain of trust. The extension secures DNS-Based CDN request routing through bridging the trust gap between site domain (CDN customer) and CDN domain (CDN provider).

2. Trust Gap and Solution

DNSSEC authenticates DNS data by establishing a chain of trust along the DNS hierarchy. When validating the DNS data, a validating resolver attempts to build a chain of trust from the trust anchor to the data. The DNS root is usually configured as the default trust anchor by validating resolvers. A chain of trust consists of a set of zones, of which the parent zone offers a signed delegation to the child zone. In Fig. 1, the site zone foo.com operated by CDN customer is secure because there exists a chain of trust from the root through com to foo.com, but the CDN zone cdn.net operated by CDN provider is insecure because it is not linked to a chain of trust. The site zone returns a CNAME record to redirect name resolution of the site domain www.foo.com to the CDN domain www.cdn.net. As the chain of trust between the root and the CDN zone does not exist, a validating resolver will find the validation path of www.foo.com is insecure (see the upper subfigure of Fig. 1). That means the resolution path from the root to www.foo.com is vulnerable to DNS spoofing attacks [6], [7].

In order to link an island of trust to a chain of trust, our DNSSEC extension allows a secured redirection connecting the CDN domain with the site domain (see the lower subfigure of Fig. 1). In the extension, a new RR resides only at the CDN customer and only in accompany with the corresponding CDN redirection. It is used to identify the key(s) that the CDN provider uses to self-sign the CDN request routing targeted by the CDN redirection. Validating resolvers use the presence of the new RR and its corresponding signature (RRSIG) to authenticate the trust link between the CDN customer and the CDN provider. And they use a new signature RR to authenticate the CDN request routing by the trustworthy CDN provider.

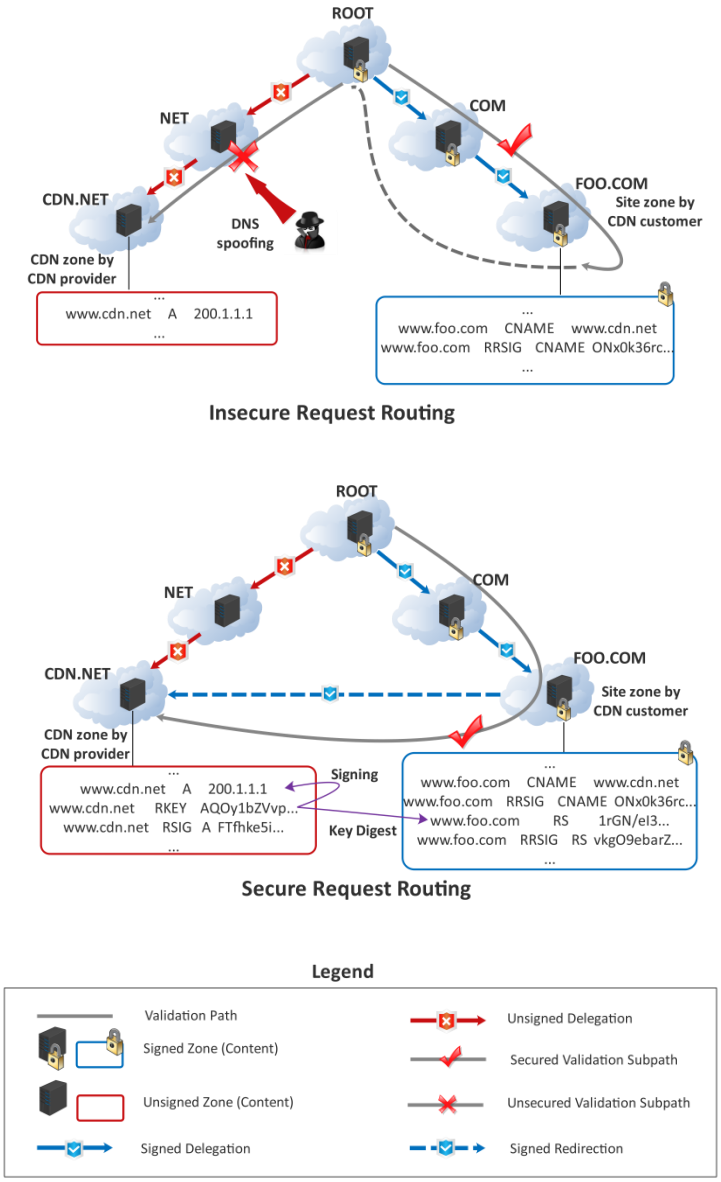


Fig. 1. Insecure and secure request routing.

CDN customer. CDN customer uses a digest of the CDN provider's public key to accompany the CDN redirection. As part of the zone, the digest is signed using the zone signing key of the site zone. The digest along with its verifiable signature provides a signed CDN redirection towards the CDN provider. The digest is stored in RS (Redirection Signer) RR. The digest is calculated by applying the digest algorithm to a string, which is obtained by concatenating the canonical form of the fully qualified owner name of the RKEY (Redirection KEY) RR with the RKEY RDATA:

digest = digest_algorithm(RKEY owner name | RKEY RDATA)

CDN provider. CDN provider uses public key cryptography to sign the CDN request routing, namely the IP address of the CDN server indicated by the A/AAAA RR. The public key is stored in RKEY RR. In the CDN zone, CDN provider signs its CDN request routing by using a private key and stores the corresponding public key in a RKEY RR. The signature covering the CDN request routing is stored in RSIG (Redirection SIGnature) RR. The cryptographic signature covers the RSIG RDATA (excluding the Signature field) and the CNAME RRset specified by the RSIG owner name and RSIG class:

signature = sign(RSIG_RDATA | RR(1) | RR(2) ...)

where the CNAME RRset in canonical order is listed as RR(1), ..., RR(n).

Validating resolver. An extended-security-aware resolver must not only support the signature verification specified in the conventional DNSSEC but also support the signature verification specified in our proposed extension. So it faces two approaches of validating CDN request routing: the conventional DNSSEC validation and the extended validation proposed in this work. The former should be tried first. If the former returns a secure or bogus result, the final validation result is so; if the former returns an insecure result, the latter should be attempted and its result is the final validation result.

3. Message Flow

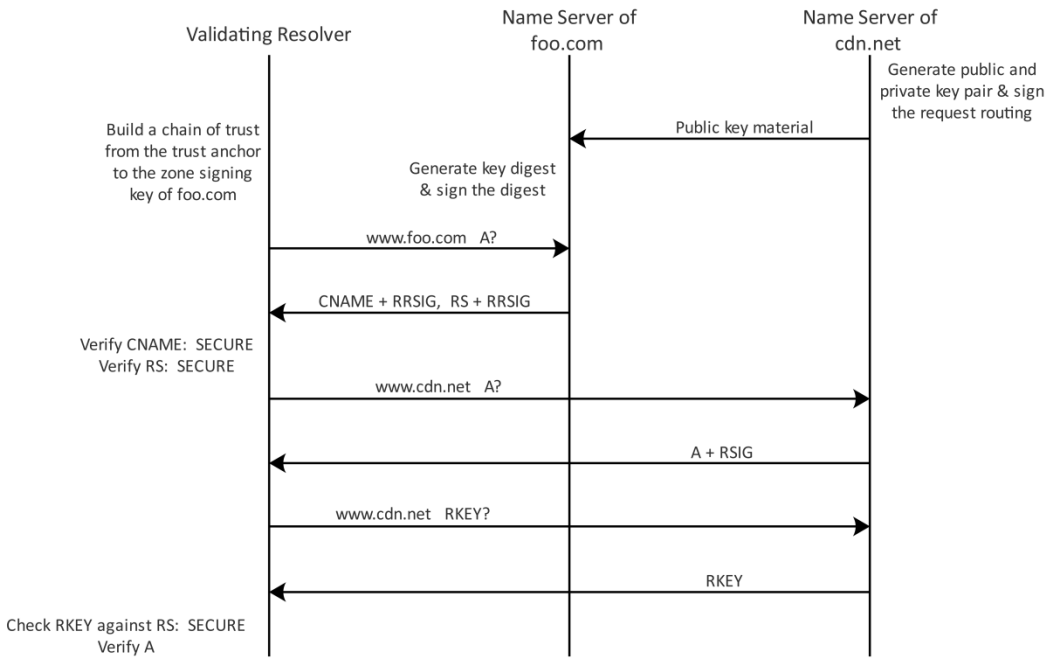


Fig. 2. Message flow of secure DNS-based CDN requesting.

In accordance with Fig.1, we illustrate the message flow of secure DNS-based CDN requesting in Fig. 2. As the bootstrapping work, validating resolver should build a chain of trust to the zone signing key of foo.com; the name server of cdn.net should generate the public and private key pair and sign the requesting routing before submitting the public key material to name server of foo.com; then the name server of foo.com should generate the key digest of the public key and sign the digest using its zone signing key. At the beginning, validating resolver sends a request for www.foo.com to the name server of foo.com, and the response includes the CNAME RR and its signature as well as the RS RRset of its signature. Validating resolver learns that www.foo.com is an alias of www.cdn.net. Validating resolver should verify the CNAME RR and the RS RRset using the zone signing key. If they are both secure, validating resolver proceeds with requesting the name server of cdn.net for www.cdn.net. The response includes the request routing along with its signature. The RSIG RR implies that the cdn.net zone is not signed since otherwise RRSIG RR should be present. So validating resolver doesn't need to try the conventional DNSSEC validation. The last query is for the RKEY of www.cdn.net. Once the RKEY is identified as secure by being checked against the RS RR, it is used to verify the requesting routing (the A RR).

4. Measurement

We built a measurement tool to actively probe the top 50,000 domains in the Alexa ranking. To measure the presence of insecure CDN request routing, we only examined each individual domain which satisfies all the following: it is a signed DNS zone; it has a site domain with a "www" prefix; its site domain sustains an insecure CDN request routing. Among those domains, we identified four major CDN domains: akadns.net, edgekey.net,

amazonaws.com, and edgesuite.net. About 62.7% of insecure CDN requesting routing were found to fall into the four CDN domains, and edgekey.net alone accounts for 32.9% of insecure CDN requesting routing.

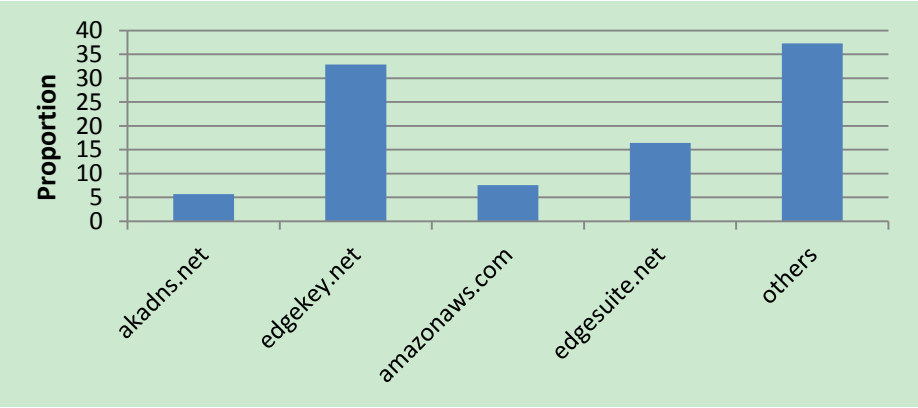


Fig. 3. Distribution of insecure CDN requesting routing under different CDN domains.

5. Conclusion

In this letter, we have presented a secure DNS-based CDN requesting scheme to address the trust gap issue raised by the limited DNSSEC deployment. The scheme allows a CDN domain in an island of trust to be securely linked with a secure site zone. Besides, the individual-domain-based signing proposed in this work may significantly lessen the cryptographic work by the conventional zone-based DNSSEC signing. As a flexible and scalable extension to DNSSEC, the technique is promising in securing CDNs.

References

[1] W. Benchaita, S. G. Doudane, and S. Tixeuil, “Stability and optimization of DNS-based request redirection in CDNs”, in Proc. of ICDCN'16, Article 11 , 10 pages, 2016.

[2] M. Taha, “A novel CDN testbed for fast deploying HTTP adaptive video streaming”, in Proc. of MobiMedia '16, pp. 65-71, 2016.

[3] R. Arends, et. al., “Protocol modifications for the DNS security extensions”, RFC 4035, Mar. 2005.

[4] F. Cangialosi, et al., “Measurement and analysis of private key sharing in the HTTPS ecosystem”, in Proc. of CCS '16, pp. 628-640, 2016.

[5] J. Liang, et al., “When HTTPS meets CDN: A case of authentication in delegated service”, in Proc. of SP'14, pp. 67-82, 2014.

[6] Z. Wang, “POSTER: On the capability of DNS cache poisoning attacks”, in Proc. of CCS'14, pp. 1523-1525, 2014.

[7] Z. Wang, “A revisit of DNS Kaminsky cache poisoning attacks”, in Proc. of GLOBECOM'15, pp. 1-6, 2015.

Zheng Wang received his Ph.D. degree from Computer Network Information Center, Chinese Academy of Sciences, Beijing, China, in 2010. His research interests include Internet naming and addressing, network security, cloud computing, and network measurement.

Scott Rose works as a computer scientist at the National Institute for Standards and Technology (NIST). He was on the editor team that produced the DNS Security Extensions (DNSSEC). Scott received his BA in Computer Science from The College of Wooster and his MS from University of Maryland, Baltimore County.

Jun Huang received his Ph.D. degree from Beijing University of Posts and Telecom, Beijing, China, in 2012. His research interests include Internet of Things, Cloud computing, and next generation Internet. He is currently a full professor at Chongqing University of Posts and Telecom.

Empirical Measurement and Analysis of HDFS Write and Read Performance

Bo Dong, Jianfei Ruan, Qinghua Zheng
MOE Key Lab for Intelligent Networks and Network Security, Xian Jiaotong University
Email: dong.bo@xjtu.edu.cn

1. Introduction

Data explosion is becoming an irresistible trend, and the era of Big Data has arrived [1, 2]. Data-intensive file systems are the key component of any cloud-scale data processing middleware [3, 4]. Hadoop Distributed File System (HDFS), one of the most popular open source data-intensive file systems, has been successfully used by many companies, such as Yahoo!, Amazon, Facebook, AOL and New York Times [5, 6].

HDFS write and read (WR) performance has a significant impact on the performance of Big Data platform, and has received increasing attention recently, including researches on performance evaluating, modeling and optimizing [7–10]. Specially, in the field of evaluating HDFS performance, a typical approach is through experiments; thus, it is mainly based on the analysis of experiment results [10]. The commonly used statistical methods are to calculate mean values [9, 10] or median values [6] of the execution times/throughputs of repeated operations, which yield the average level of HDFS WR performance.

However, few studies have investigated the distribution of HDFS WR performance. Normally, if the performance is not stable, its distribution could be of great importance to the analysis of experiment results and discovering performance feature. On the one hand, both mean value and median value contain much less information, whereas knowledge on the distribution of performance may even be crucial, such as in time-critical systems which often relied upon the tail of distribution. On the other hand, choosing an appropriate statistical method still requires to verify the distribution of experiment results, such as the case when the distribution is skewed the mean value is not appropriate. Therefore, exploiting the distribution of HDFS WR performance and discovering its corresponding features are the pre-requisite for HDFS performance evaluation.

In this paper, we study the instability and distribution of HDFS WR performance through empirical measurement and analysis. First, we discover that HDFS WR performance is not stable for a given file size even in the same condition, and analyze the reasons. Then, we use Kolmogorov-Smirnov (K-S) test to determine that HDFS WR performance does not follow any common distributions. Lastly, we propose a derivation method based on HDFS WR mechanism to testify that HDFS WR performance follows a certain distribution for a file size. Our work can provide a premise of studying distribution features of HDFS WR performance.

2. Specially Designed Experiments

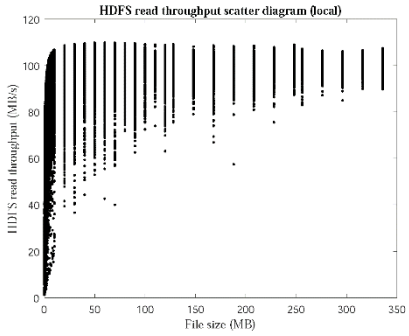
Special measurement experiments are designed to study the stability and distribution characteristics of HDFS WR performance. The methodology of the measurement experiments includes:

- All the measurement experiments are performed in the same condition, that is (1) only one HDFS client writes or reads a file at one moment; (2) the experimental environment including machines, disks, and network, is exclusive to the experiments, and there are no other operations to contend for resources; (3) HDFS configuration parameters used are the same as the default setting.
- A set of representative file sizes should be sampled to study the dynamic changes of the stability and distribution characteristics in the file size dimensionality. For a given file size, a certain number of HDFS write or read operations are sequentially performed and the throughput of each operation is obtained.

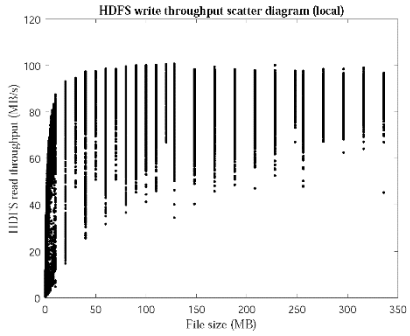
In the experiments, 50 datasets are sampled, each of which contains 1000 files with a same size. For each dataset, sequential HDFS WR operations are performed in two clusters: a large cluster on EC2 (Amazon Elastic Compute Cloud) and a local cluster having physical nodes. First, sequentially upload each file of the dataset to HDFS using a HDFS client; the execution time of uploading each file is measured, and the throughput of each write operation is calculated. Then, sequentially download 500 files from HDFS using a HDFS client; the execution time of downloading each file is measured, and the throughput of each read operation is calculated.

3. Instability of HDFS WR Performance

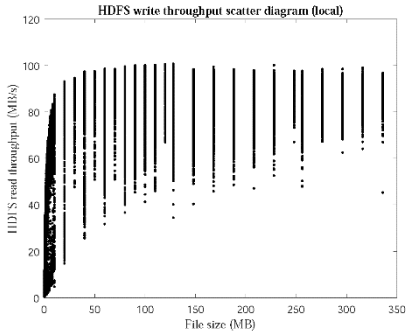
In order to illustrate the performance variability of HDFS WR operations intuitively, scatter diagrams of the measurement results are shown as Fig. 1. Horizontal axes show file size (in unit of MB), and vertical axes show throughput (in unit of MB/s).



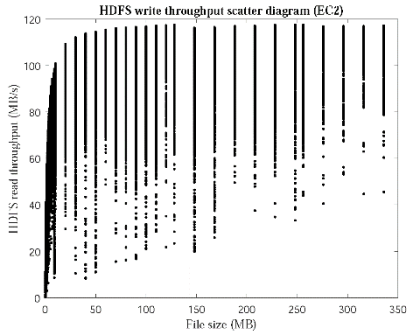
(a) HDFS read throughput in local environment



(b) HDFS write throughput in local environment



(c) HDFS read throughput in EC2 environment



(d) HDFS write throughput in EC2 environment

Fig. 1. Scatter diagrams of the measurement results

As shown in Fig. 1, each file size on the horizontal axis corresponds to a significant number of different points on the vertical axis, which describes the throughput variability of HDFS WR operations for a given file size. For small file sizes, taken HDFS write operations as an example, the drastically unstable HDFS write throughput is observed, which is distributed between close to 0 and near 100 MB/s. When file size becomes larger, the gap between the minimum and maximum throughput is not as huge as the case of small file sizes, while still reaches the range of 15 to 90 MB/s. Thus, it is concluded that HDFS WR performance is not stable for a given file size even in the same condition.

The instability of HDFS WR performance does not occur coincidentally, but is caused by the internal mechanism of HDFS WR operations. HDFS WR performance is influenced by a range of factors such as network traffic, disk I/O, and HDFS configuration parameters [11]. We learn from literature the performance of network traffic and disk I/O is not stable in practice. For example, the throughput of network traffic is not stable and follows specific distribution described by kurtosis and skewness [12], and the seek and rotation delays of disk I/O vary even for the same transfer [13]. Thus, affected by the performance instability of underlying network and disk I/O, it is theoretically inferred that HDFS WR performance is not stable. In addition, HDFS involves certain mechanisms with performance enhancing features such as pipelines and load balancing, which further increase the performance variability [14].

4. Distribution of HDFS WR Performance

4.1 Does HDFS WR Performance Follow any Common Distribution for a File Size?

To study the distribution of HDFS WR performance, an intuitive first step is to consider whether HDFS WR performance follows some common distributions. In the literature review, eight probability are commonly researched and used, including Normal, Gamma, Poisson, Exponential, Rayleigh, Lognormal, Weibull and Extreme Value distribution [15]. Here, K-S test [16] is applied to determine whether HDFS WR performance follows any of the above eight common distributions.

For each file size, each p-value of K-S test using the measurement results is far less than the selected significance level (i.e., 0.05), even close to zero. Thus, based on the judgment of K-S test, it can be concluded that HDFS WR performance does not follow any of the common distributions referred.

4.2 Does HDFS WR Performance Follow a Certain Distribution for a File Size?

Since we have no knowledge of HDFS WR performance fitting any common distribution, a subsequent question arises as to whether HDFS WR performance follows a certain probability distribution for a given file size, which is a premise of studying distribution features of HDFS WR performance.

In this paper, we propose an approach to solve this question which distinguishes between the intervals (0, *BS*] and (*BS*, ∞) (Here *BS* is equal to 128 MB).

- Friedman test based on the measurement results for file sizes on the finite interval (0, *BS*];
- A derivation method based on HDFS WR mechanism for file sizes on the infinite interval (*BS*, ∞).

4.2.1 On the finite interval (0, *BS*]

Friedman test, one of the non-parametric statistical test methods, is applied to verify whether HDFS WR performance for a given file size follows a certain probability distribution on the interval (0, *BS*].

The measurement experiments of HDFS WR operations stated in Section 2 are performed three times, and the treatments are the throughputs of the three experiments. For both the local cluster and EC2 cluster, the *p*-values are all far larger than the selected significance level (i.e., 0.05). Thus, based on the judgment of Friedman test, it could be concluded that HDFS WR performance follows a certain distribution for each given file size on the interval (0, *BS*].

4.2.2 On the infinite interval (BS, ∞)

If a statistical test method based on the measurement results, such as Friedman test, is adopted on the interval (BS, ∞), infinite number of file sizes would need to be sampled. In this case, the cost of measurement experiments is too great to bear. Consequently, a derivation method based on HDFS WR mechanism is introduced for file sizes on the infinite interval (BS, ∞).

Taking HDFS read operation for instance, the derivation process is illustrated as follows.

A. Formulation of the execution time of HDFS read operation

According to the mechanism of HDFS read operation, the execution time of HDFS read operation for a file is equal to the sum of metadata operation time and the time of reading each block. Then, the problem of verification on the interval (BS, ∞) can be transformed into a problem of deriving the distribution followed by the time addition of metadata operation and reading each block.

Assume a file (in size of *S* and *S* >*BS*) is chopped up into *n* blocks, whose lengths are denoted by $BS_1, BS_2, \ldots, BS_n$, and the corresponding execution times of HDFS reading these blocks are denoted by $T_{BS_1}, T_{BS_2}, \ldots, T_{BS_n}$, respectively. Moreover, the metadata operation time is denoted by T_{md}. Then, the execution time of HDFS read operation for the given file size *S*, denoted by T_S, can be represented as follows.

$$T_S = T_{BS_1} + T_{BS_2} + \ldots + T_{BS_n} + T_{md} \quad (1)$$

When network condition does not cause the messages piled up in the NameNode (i.e., the metadata server of HDFS) side, the response time of HDFS metadata operation can be set constant [10]. Thus, T_{md} can be treated as a constant denoted by C. Then, T_S is represented as follows.

$$T_S = T_{BS_1} + T_{BS_2} + \ldots + T_{BS_n} + C \quad (2)$$

B. Replace the execution time of block reading by that of file reading

As the execution times of HDFS reading blocks $T_{BS_1}, T_{BS_2}, \ldots, T_{BS_n}$ are difficult for measurement, it is still infeasible to obtain the execution time of HDFS file reading T_S. Then, could the execution time of each block reading be taken place by or calculated from that of file reading with the same length respectively?

It can be learned from HDFS read mechanism, for a file with the length on the interval (0, *BS*], the execution time of HDFS read operation can be represented by the sum of metadata operation time and the time of reading its block which own the same length as the file. Then, the expression can be formulated as follows.

$$T_{FS_k} = T_{BS_k} + C, \quad k = 1, 2, \ldots, n \quad (3)$$

Where, FS_k denotes the *k*-th file length, which is equal to the corresponding block length BS_k. T_{FS_k} denotes the execution time of HDFS file reading operation for the given file size FS_k.

Then, T_{BS_k} can be represented by $T_{FS_k} - C$. Based on this, T_S can be reformulated as follows.

$$T_S = T_{FS_1} + T_{FS_2} + \ldots + T_{FS_n} - (n-1) \times C \quad (4)$$

C. Distribution transforms from "throughput-oriented" to "time-oriented"

As file sizes $FS_1, FS_2, \ldots, FS_n$ are on the interval $(0, BS]$, the throughput of HDFS file reading operation follows a certain distribution according to the conclusion drawn from Section 4.2.1.

Let $TR_{FS_1}, TR_{FS_2}, \ldots, TR_{FS_n}$ be HDFS read throughput for the given file sizes $FS_1, FS_2, \ldots, FS_n$, respectively. Then, each of $TR_{FS_1}, TR_{FS_2}, \ldots, TR_{FS_n}$ can be taken as a random variable which obeys a certain probability distribution as follows.

$$TR_{FS_k} \sim f_{TR_{FS_k}}(tr), \quad k = 1, 2, \ldots, n \quad (5)$$

Where, the ~ (tilde) used in that way means "is distributed as". $f_{TR_{FS_k}}(tr)$ represents the probability distribution function followed by TR_{FS_k}.

As HDFS read throughput is the average flow rate per file read from HDFS during a read operation, its computational formula is equal to:

$$TR_{FS_k} = \frac{FS_k}{T_{FS_k}}, \quad k = 1, 2, \ldots, n \quad (6)$$

For each obtainable value of *k*, the execution time of HDFS read operation can be taken as a random variable, which obeys a certain probability distribution as follows.

$$T_{FS_k} \sim f_{T_{FS_k}}(t) = f_{TR_{FS_k}}\left(\frac{FS_k}{t}\right), \quad k = 1, 2, \ldots, n \quad (7)$$

Where, FS_k stay constant for each selected *k*.

D. Probability distribution calculation based on convolution

The probability distribution of the sum of two or more independent random variables is the convolution of their individual distributions [17]. Since $T_{FS_1}, T_{FS_2}, \ldots, T_{FS_n}$ are the execution time of independent HDFS read

operations, the sum of $T_{FS_1}, T_{FS_2}, \ldots, T_{FS_n}$ is given by a certain probability distribution, which can be denoted as follows.

$$T_{FS_1} + T_{FS_2} + \ldots + T_{FS_n} \sim f_{T_{FS_1}+T_{FS_2}+\ldots+T_{FS_n}}(t) = T_{FS_1}(t) * T_{FS_2}(t) * \ldots * T_{FS_n}(t) \quad (8)$$

Where, the asterisks $*$ denotes the operation of convolution.

In order to simplify the theoretical expression, $T_{FS_1} + T_{FS_2} + \ldots + T_{FS_n}$ is represented as $T_{S'}$, and $f_{T_{FS_1}+T_{FS_2}+\ldots+T_{FS_n}}(t)$ is represented as $f_{T_{S'}}(t)$. Thus, the above expression is reformulated as follows.

$$T_{S'} \sim f_{T_{S'}}(t) = T_{FS_1}(t) * T_{FS_2}(t) * \ldots * T_{FS_n}(t) \quad (9)$$

Meanwhile, Eq. 4 can be simplified as $T_S = T_{S'} - (n-1) \times C$, which represents a linear transformation with a constant $-(n-1) \times C$ added to every possible value of the random variable $T_{S'}$. Thus, the probability distribution of T_S can be denoted as follows.

$$T_S \sim f_{T_S}(t) = f_{T_{S'}}(t + (n-1) \times C) \quad (10)$$

Let TR_S be HDFS read throughput for the given file size S. Then, the probability distribution of TR_S can be denoted as follows.

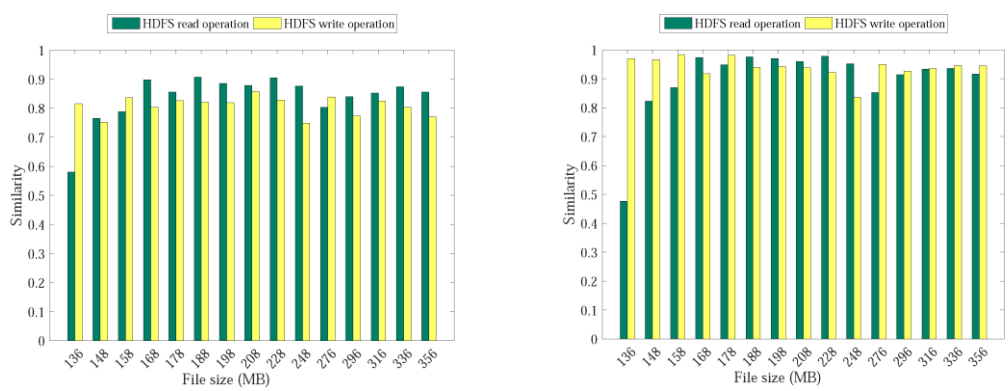
$$TR_S \sim f_{TR_S}(tr) = f_{T_S}\left(\frac{S}{tr}\right) = f_{T_{S'}}\left(\frac{S}{tr} + (n-1) \times C\right) \quad (11)$$

Therefore, HDFS read throughput belongs to a certain probability distribution for a file size on the interval (BS, ∞).

The process of HDFS write operation is relatively complex, but the time of HDFS write operation for a given file is also equal to the sum of metadata operation time and the time of writing each block. Similarly, HDFS write performance belongs to a certain probability distribution for a file size on the interval (BS, ∞).

E. Preliminary Experimental Evaluation

Preliminary experiments for simulating HDFS WR performance on the infinite interval (BS, ∞) are carried out by taking 15 files. Correlation coefficient is used to compare the similarities between actual distributions of HDFS WR performance and estimated ones by our proposed method. The results are shown as Figure. 2.



(a) Local environment (b) EC2 environment

Fig. 2. Similarities between the actual distributions and the estimated ones

5. Conclusion

The distribution of HDFS WR performance is crucial for the analysis of experiment results. In this paper we discover that HDFS WR performance follows a certain distribution for a file size. Especially, we propose a derivation method to achieve probability distribution calculation based on HDFS WR mechanism.

ACKNOWLEDGMENT

This work is supported by "The Fundamental Theory and Applications of Big Data with Knowledge Engineering" under the National Key Research and Development Program of China with grant number 2016YFB1000903, the National Science Foundation of China under Grant Nos. 61502379, 61472317, 61532015, and Project of China Knowledge Centre for Engineering Science and Technology.

References

[1] A. Labrinidis and H. V. Jagadish, "Challenges and opportunities with big data," in Proceedings of the VLDB Endowment, vol. 5, no. 12, pp. 2032–2033, 2012.
[2] X.Wu, X. Zhu, G.-Q.Wu, andW. Ding, "Data mining with big data," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97–107, 2014.
[3] B. Fan, W. Tantisiriroj, L. Xiao, and G. Gibson, "Diskreduce: Raid for data-intensive scalable computing," in Proceedings of the 4th Annual Workshop on Petascale Data Storage. ACM, 2009, pp. 6–10.
[4] S. Sehrish, G. Mackey, P. Shang, J. Wang, and J. Bent, "Supporting HPC analytics applications with access patterns using data restructuring and data-centric scheduling techniques in MapReduce," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 158–169, 2013.
[5] Y. Luo, S. Luo, J. Guan, and S. Zhou, "A ramcloud storage system based on HDFS: Architecture, implementation and evaluation," Journal of Systems and Software, vol. 86, no. 3, pp. 744–750, 2013.
[6] F. Tian, T. Ma, B. Dong, and Q. Zheng, "PWLM^3-based automatic performance model estimation method for HDFS write and read operations," Future Generation Computer Systems, vol. 50, pp. 127–139, 2015.
[7] J. Shafer, S. Rixner, and A. L. Cox, "The Hadoop Distributed Filesystem: Balancing portability and performance," in Proceedings of 2010 IEEE International Symposium on Performance Analysis of Systems & Software, IEEE, 2010, pp. 122–133.
[8] B. Dong, Q. Zheng, F. Tian, K.-M. Chao, R. Ma, and R. Anane, "An optimized approach for storing and accessing small files on cloud storage," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1847–1862, 2012.
[9] B. Dong, Q. Zheng, F. Tian, K.-M. Chao, N. Godwin, T. Ma, and H. Xu, "Performance models and dynamic characteristics analysis for hdfs write and read operations: A systematic view," Journal of Systems and Software, vol. 93, pp. 132–151, 2014.
[10] Y. Wu, F. Ye, K. Chen, and W. Zheng, "Modeling of distributed file systems for practical performance analysis," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 156–166, 2014.
[11] N. S. Islam, X. Lu, M. Wasi-ur Rahman, J. Jose, and D. K. D. Panda, "A micro-benchmark suite for evaluating HDFS operations on modern clusters," in Specifying Big Data Benchmarks. Springer, 2014, pp. 129–147.
[12] P. Cˇ isar and S. M. Cˇ isar, "Skewness and kurtosis in function of selection of network traffic distribution," Acta Polytechnica Hungarica, vol. 7, no. 2, pp. 95–106, 2010.
[13] K. Salem and H. Garcia-Molina, "Disk striping," in Proceedings of IEEE Second International Conference on Data Engineering, IEEE, 1986, pp. 336–342.
[14] V. Puranik, T. Mitra, and Y. Srikant, "Probabilistic modeling of data cache behavior," in Proceedings of the seventh ACM International Conference on Embedded software. ACM, 2009, pp. 255–264.
[15] C. Walck, "Handbook on statistical distributions for experimentalists," 2007.
[16] W. J. Conover and W. J. Conover, "Practical nonparametric statistics," 1980.
[17] M. P. Kaminskiy, Reliability models for engineers and scientists. CRC Press, 2012.

Bo Dong received his Ph.D. degree in computer science and technology from Xi'an Jiaotong University in 2014. He is currently a postdoctoral researcher in the MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University. His research interests focus on performance modeling and evaluation, big data processing and analytics, and cloud computing.

Jianfei Ruan received his B.S. degree in automation from Xi'an Jiaotong University in 2014. He is currently a Ph.D. student in the MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University. His research interests include performance modeling and evaluation, and cloud computing.

Qinghua Zheng received his B.S. and M.S. degrees in computer science and technology from Xi'an Jiaotong University in 1990 and 1993, respectively, and his Ph.D. degree in systems engineering from the same university in 1997. He was a postdoctoral researcher at Harvard University in 2002. He is a professor with the Department of Computer Science and Technology at Xi'an Jiaotong University. His research interests include intelligent e-Learning and software reliability evaluation.

MMTC OFFICERS (Term 2016 — 2018)

CHAIR

Shiwen Mao
Auburn University
USA

STEERING COMMITTEE CHAIR

Zhu Li
University of Missouri
USA

VICE CHAIRS

Sanjeev Mehrotra (North America)
Microsoft
USA

Fen Hou (Asia)
University of Macau
China

Christian Timmerer (Europe)
Alpen-Adria-Universität Klagenfurt
Austria

Honggang Wang (Letters&Member Communications)
UMass Dartmouth
USA

SECRETARY

Wanqing Li
University of Wollongong
Australia

STANDARDS LIAISON

Liang Zhou
Nanjing Univ. of Posts & Telecommunications
China

MMTC Communication-Frontier BOARD MEMBERS (Term 2016—2018)

Guosen Yue	Director	Huawei R&D USA	USA
Danda Rawat	Co-Director	Howard University	USA
Hantao Liu	Co-Director	Cardiff University	UK
Dalei Wu	Co-Director	University of Tennessee	USA
Zheng Chang	Editor	University of Jyväskylä	Finland
Lei Chen	Editor	Georgia Southern University	USA
Tasos Dagiuklas	Editor	London South Bank University	UK
Melike Erol-Kantarci	Editor	Clarkson University	USA
Kejie Lu	Editor	University of Puerto Rico at Mayagüez	Puerto Rico
Nathalie Mitton	Editor	Inria Lille-Nord Europe	France
Shaoen Wu	Editor	Ball State University	USA
Kan Zheng	Editor	Beijing University of Posts & Telecommunications	China