12-2021

Data fusion for trust evaluation

Zheng YAN

Qinghua ZHENG

Laurence T. YANG

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Editorial: Data Fusion for Trust Evaluation

Zheng Yan[ab] Qinghua Zheng[c] Laurence T. Yang[d] Robert H. Deng[e]

a State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, No. 2 South Taibai Road, 710071 Xi'an, China
b Department of Communications and Networking, Aalto University, Konemiehentie 2, P.O.Box 15400, Espoo 02150, Finland
c Xi'an Jiaotong University, China
d St Francis Xavier University, Canada
e Singapore Management University, Singapore

Published in Information Fusion, Volume 76, December 2021, Pages 187-188. DOI: 10.1016/j.inffus.2021.05.007

Trust evaluation is a process to quantify trust by analyzing the data related to the factors that affect trust [1]. It has been widely applied in many fields to facilitate decision making, system entity collaboration and security establishment. For example, in social networking, trust evaluation helps users make a social decision, reduce the risk of social interactions, and ensure the quality of a social networking environment [2,3]. In digital communications, trust evaluation can be applied to detect malicious nodes, filter unwanted traffic and improve communication security [4,5]. In e-commerce and cloud services, trust evaluation helps users selecting an appropriate product or service from a large number of candidates. In Peer-to-Peer (P2P) networking, trust evaluation supports identifying interactive objects, choosing friendly peers, and combating with malicious peers. Nowadays, trust evaluation has become a useful technique that has benefited many emerging areas by playing as a significant compensation to other security technologies.

With the rapid development of cyber systems and the huge volumes of data bursted in it, trust evaluation is evolving from simple mathematical calculation to data analytics through data fusion, e.g., machine learning [6,7]. Traditional trust evaluation methods are mostly based on direct and indirect interactions between a trustor and a trustee. They determine trust by aggregating trust factors through weighting and relevant calculations. However, these methods become infeasible when there are no interactions between the trustor and the trustee. Precisely determining the weights is actually difficult in practice, thus hard to guarantee evaluation accuracy. Data incompletion and fake data could further impact evaluation quality. In case of large amount of data with a complex structure, these traditional methods become infeasible and ineffective. In response to these problems, many researchers suggested using data fusion to make trust evaluation intelligent and accurate.

Comparing with the traditional trust evaluation methods, there are some irreplaceable advantages to use data fusion for trust evaluation [8,9]. First, trust evaluation based on data fusion, such as machine learning, can overcome the "cold start" and "zero knowledge" problems of traditional methods. By training a trust model with available trust-related data, trust evaluation can be performed even though some valuable data are missed. Second, the recent advance of data fusion can help evaluating trust in an accurate way, especially when facing enormous data with complex structure. Third, data fusion can precisely simulate human decision making with regard to trust evaluation, thus it is a proper technique to evaluate trust with clear explanation and easy human-being acceptance.

However, a number of new challenges are raised in data fusion for trust evaluation caused by practical demands and limitations of data fusion technologies [8,9,10]. First, a generic model for trust evaluation based on data fusion is still missed and hard to achieve. Data fusion works well for handling sparse data, complex data relationships and big data. Existing work only shows its effectiveness in some specific domains, e.g., social networking. The literature still lacks a generic model that can be applied into various fields. Second, trust evaluation requests a fine-grained evaluation result, which is hard to achieve with machine learning since it treats trust evaluation as a classification problem with two or a limited number of main categories such as trusted, neutral and distrusted. Such a coarser-grained representation cannot sufficiently reflect the subjectivity and uncertainty of trust. Third, the mothed of data labeling has not well explained or explored, which is obviously important in trust evaluation model training and may directly impact evaluation accuracy. Fourth, existing methods using data fusion for trust evaluation generally do not consider privacy protection on the data used for evaluation and seldom concern the robustness of evaluation. True data discovery and attack tracing are seldom studied. Last but not the least, most of the existing methods do not consider computational overhead, thus do not pay special attention to evaluation efficiency. This greatly impacts their applicability in practice.

This special issue aims to bring together researchers and practitioners to discuss various aspects of data fusion for trust evaluation, explore key theories and technologies, investigate technology enablers and innovate new solutions for overcoming major challenges in this research field. Through rigorous review, we selected six papers for publication, which are introduced as below.

The evolution of cyber-physical-social system (CPSS) changes the perspective of data science to focus on fusing data from multi-space information resources. One important issue should be concerned during the evolution is data privacy, which has been studied seriously in the literature, but lacks a thorough survey, especially on differential privacy based solutions. Gati et al. conducted a comprehensive review on differentially private data fusion and deep learning in CPSSs [11]. They also proposed a novel framework for differentially private data fusion and deep learning and indicated a number of promising directions to instruct future research.

In order to enable cold start and overcome data sparsity, Guo et al. [12] proposed T-MRGF, a trust-aware recommendation method based on heterogeneous multi-relational graphs fusion by considering both social trust relations and item-based knowledge. The authors fused a user-user trust relation graph, a user-item interaction graph and an item-item knowledge graph for feature propagation and model prediction in order to gain both high recommendation accuracy and sound training efficiency.

For overcoming the single point of failure of the control plane in Software-Defined Networking (SDN), Meng et al. [13] suggested integrating blockchain into SDN control plane and proposed BSDNFilter. BSDNFilter is an intrusion detection system enabled security mechanism to filter malicious traffic based on trust through traffic fusion and aggregation. Experimental test showed its effectiveness against flooding attacks.

In order to realize decentralized network trust evaluation and overcome the shortcomings of centralized solutions, blockchain's efficiency and security issues, and data privacy disclosure, Liu et al. [14] proposed SeDID, an SGX-enabled intrusion detection system for network trust evaluation. It offers incentives, preserves data privacy and solves the problems of blockchain by proposing a novel consensus mechanism named Poof-of-Detection. The Poof-of-Detection integrates intrusion detection and trust evaluation into block creation and rewards each node contributing to it. The authors constrained block creation with a threshold of the number of generated blocks. A miner with the fewest created blocks gains the smallest difficulty. Miners confirm a block winner to avoid forking based on a commonly agreed rule. For preserving data privacy, only authorized SGX enclaves hosted by miners can decrypt the data provided by collection nodes and exchange their obtained patterns with encryption protection. Analysis and simulations show the efficacy of SeDID with regard to incentive provision, privacy preservation, as well as its blockchain's efficiency and security.

In the context of cooperative vehicular safety applications for improving road safety, traffic efficiency, and driving comfort, Liu et al. focused their study on solving the conflict between trust evaluation and privacy preservation during distributed data fusion. They proposed a Lightweight Privacy-Preserving Trust Evaluation (LPPTE) scheme [15] that can achieve low data fusion overheads regarding computation, communication, and storage. Through theoretical analysis and simulation evaluation, they demonstrated the accuracy and advanced performance of the LPPTE scheme.

In order to overcome the shortcomings of cloud computing in Internet of Things (IoTs) and avoid forged data collection, Wang et al. [16] proposed a trust evaluation model based on trust transitivity on a chain assisted by mobile edge nodes to ensure sensor node reliability and mitigate attacks. They designed approaches to calculate the trust degrees of different trust chains and proposed an improved Dijkstra's algorithm for collecting trust information of sensor nodes by mobile edge nodes. Experimental results show that the proposed trust evaluation model can improve security and increase the throughput of IoTs.

Data fusion for trust evaluation is an emerging research topic that are worth special investigation. We would like to express our special appreciation to Professor Francisco Herrera, the Editor-in-Chief of Information Fusion for his support on this special issue edition. We also thank all authors and reviewers for their contributions. We hope this special issue can offer valuable perspective on trust evaluation and stimulate significant study in this field.

Declaration of Competing Interest

With regard to “Editorial: Data Fusion for Trust Evaluation”, there is no conflict of interest.

Acknowledgement

This work is supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Academy of Finland under Grant 308087 and Grant 335262; in part by the Shaanxi Innovation Team Project under Grant 2018TD-007; and in part by the 111 Project under Grant B16037, as well as Huawei Technologies Group Co., Ltd.

References

[1] Z. Yan, Trust Management in Mobile Environments – Usable and Autonomic Models, IGI Global, Hershey, Pennsylvania, USA, 2013.

[2] Z. Yan, L. Peng, W. Feng, L.T. Yang, Social-Chain: decentralized trust evaluation based on blockchain in pervasive social networking, ACM Transactions on Internet Technology 21 (1) (2021) 1–28.

[3] Z. Yan, Y. Chen, Y. Shen, A practical reputation system for pervasive social chatting, J. Comput. Syst. Sci. 79 (5) (2013) 556–572.

[4] L. Chen, Z. Yan, W.D. Zhang, R. Kantola, TruSMS: a trustworthy SMS spam control system based on trust management, Future Gen. Comput.Syst. 49 (2015) 77–93.

[5] L.F. Zhang, Z. Yan, R. Kantola, Privacy-preserving trust management for unwanted traffic control, Future Gen. Comput. Syst. 72 (2017) 305–318.

[6] J.W. Wang, X.Y. Jing, Z. Yan, Y.L. Fu, W. Pedrycz, L.T. Yang, A survey on trust evaluation based on machine learning, ACM Comput. Surv. 53 (5) (2020) 107, 36 pages.

[7] S.S. Liu, L.F. Zhang, Z. Yan, Predict pairwise trust based on machine learning in online social networks: a survey, IEEE Access 6 (1) (2018) 51297–51318.

[8] T. Meng, X.Y. Jing, Z. Yan, W. Pedrycz, A survey on machine learning for data fusion, Inf. Fusion 57 (2020) 115–129.

[9] W.X. Ding, X.Y. Jing, Z. Yan, L.T. Yang, A survey on data fusion in Internet of Things: towards secure and privacy-preserving fusion, Inf. Fusion 51 (2019) 129–144.

[10] D. Liu, Z. Yan, W.X. Ding, M. Atiquzzaman, A survey on secure data analytics in edge computing, IEEE Internet of Things J. 6 (3) (2019) 4946–4967.

[11] N.J. Gati, L.T. Yang, J. Feng, X. Nie, Z. Ren, S.K. Tarus, Differentially private data fusion and deep learning framework for cyber-physical-social systems: state-of-the-art and perspectives, Inf. Fusion (2021), https://doi.org/10.1016/j.inffus.2021.04.017.

[12] J. Guo, Y. Zhou, P. Zhang, B. Song, C. Chen, Trust-aware recommendation based on heterogeneous multi-relational graphs fusion, Inf. Fusion 74 (2021) 87–95.

[13] W.Z. Meng, W.J. Li, J.Y. Zhou, Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration, Inf. Fusion 70 (2021) 60–71.

[14] G. Liu, Z. Yan, W. Feng, X.Y. Jing, Y.X. Chen, M. Atiquzzaman, SeDID: an SGX-enabled decentralized intrusion detection framework for network trust evaluation, Inf. Fusion 70 (2021) 100–114.

[15] Z.Q. Liu, J.F. Ma, J. Weng, F.R. Huang, Y.D. Wu, L.F. Wei, Y.X. Li, LPPTE: a lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications, Inf. Fusion 73 (2021) 144–156.

[16] T. Wang, P. Wang, S.B. Cai, X. Zheng, Y. Mad, W.J. Jia, G.J. Wang, Mobile edge-enabled trust evaluation for the Internet of Things, Inf. Fusion 75 (2021) 90–100.