Trust Evaluation with Deep Learning in Online Social Networks: A State-of-the-Art Review

Zhiqi Li[1,2], Weidong Fang[1,2,3(✉)], Chunsheng Zhu[4], Wentao Chen[5], Tianpeng Hao[6], and Wuxiong Zhang[1,2]

[1] Science and Technology on Microsystem Laboratory, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 201899, China
{lizhiqi,weidong.fang,wuxiong.zhang}@mail.sim.ac.cn
[2] School of Electronic, Electrical, and Communication Engineering, University of Chinese Academy of Sciences, Beijing 100049, China
[3] Shanghai Research and Development Center for Micro-Nano Electronics, Shanghai 201210, China
[4] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
[5] State Grid Xinjiang Company Limited Electric Power Research Institute, Urumqi 830011, China
[6] Xinjiang Baiyang River Basin Administration, Urumqi 830000, China
yimengbingfeng@sina.com

Abstract. In the realm of online social networks (OSNs), it has become increasingly crucial to analyze user behavior, establish trustworthy relationships to mitigate social risks, enhance security, and safeguard privacy. Trust evaluation is widely acknowledged as an effective approach for detecting internal attacks and identifying compromised nodes, and deep learning technology can significantly enhance its performance. However, there remains a notable gap for a review paper focused on trust evaluation utilizing deep learning techniques within OSNs. Therefore, conducting a state-of-the-art review on this subject has become imperative. We analyze and compare some recent related research, summarizing prevalent challenges and open issues while proposing optimization strategies to address them. For instance, graph-based neural networks methods often grapple with exponentially increasing computational complexity as network size expands, and imbalanced datasets typically lead to reduced model accuracy and generalization. Lastly, it presents several promising avenues for future research in the field.

Keywords: Online Social Networks · Trust · Deep Learning · Cyber Security

1 Introduction

Social networks are intricate structures that arise from the interactions, connections, and collaborations among individuals using computer-based networked platforms, as highlighted in previous works [1]. For example, as of April 2024, Facebook and YouTube

D.-S. Huang et al. (Eds.): ICIC 2024, LNCS 14864, pp. 3–12, 2024.
https://doi.org/10.1007/978-981-97-5588-2_1

each have over 3 billion and 2.5 billion monthly active users, respectively[1]. This illustrates how online social networks have become essential tools in facilitating communication and connection between individuals, both with friends and strangers, in everyday human life. Nevertheless, online social networks remain vulnerable to a plethora of international threats, including Distributed Denial of Service (DDoS) attacks, phishing attempts, and malware threats. Traditional network security measures such as firewalls and intrusion detection systems frequently demonstrate inadequacies in safeguarding against specific internal network attacks. In addressing these security challenges, trust evaluation is widely recognized as a potent approach for detecting insider threats and identifying compromised nodes [2]. Trust is defined as the expectations and beliefs one party holds regarding another during interpersonal interactions, with these expectations subject to variation depending on the specific context [3].

Nevertheless, trust evaluation in OSNs, characterized by their ultra-large-scale nature, encounters a plethora of challenges. Utilizing traditional methods such as Bayesian probability and game theory can prove challenging in accurately assessing the trustworthiness of these new nodes. Fortunately, deep learning (DL) technology has shown promise in predicting future trust changes for nodes, effectively alleviating the cold start problem and enhancing accuracy and real-time performance [4]. Our contributions in this work are summarized as follows:

1. We conduct a thorough analysis and comparison of advanced works related to trust evaluation using deep learning techniques in OSNs.
2. We find that the GNN-based schemes encounter some formidable challenge of exponentially increasing computational complexity as network size expands. We delve into relevant literature focusing on other DL methods.
3. We summarize some prevalent challenges and open issues while proposing optimization strategies to address them.
4. We put forth a range of suggested future research directions to guide the academic and practitioner community in exploring novel solutions to these challenges.

The remaining structure of this paper is as follows. The analysis and comparison of some trust evaluation schemes are provided in Sect. 2. In Sect. 3, we analyze some open problems and challenges and propose some strategies to mitigate the issues. In Sect. 4, some suggested directions for future research are proposed. Finally, conclusion of this paper is drawn in Sect. 5.

2 Analysis and Comparison of Related Work

2.1 Graph-Based Neural Networks

The evaluation of node trustworthiness within a network has proven to be a valuable defense mechanism against internal attacks [5]. While DL technology has received extensive research attention in OSNs, most deep neural networks (DNNs) have been designed for Euclidean structured data, which doesn't fully leverage network topology. To address

[1] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users.

this limitation, some research has proposed graph-based DL methods for non-Euclidean structured data in recent years.

Graph Neural Networks (GNNs) have represented a significant advancement in deep learning, enhancing the efficiency of neural networks by extracting and analyzing potential dependencies through message passing and neighborhood aggregation. In their work, C. Huo et al. introduced an innovative GNN-based trust evaluation method named TrustGNN for social networks [6]. TrustGNN adeptly integrated the propagation and composability properties of trust graphs into a GNN framework, thereby enhancing trust evaluation processes. Besides, in OSNs, there has been a growing demand for user communication with strangers. However, when the network data was sparse, the accuracy of trust prediction could be greatly affected [7]. To tackle this challenge, S. Ghafari et al. leveraged and extended GraphSAGE [8], a method for computing node representations in an inductive manner, alongside the proposal of a deep context-aware trust prediction model called DCAT [9]. It targeted the analysis of textual information provided by users in comment-based OSNs. Additionally, X. Chen et al. putted forward a trust evaluation framework by categorizing user features into four distinct groups [10]. G. Liu et al. introduced a neural network (NN) called WalkNet within the NeuralWalk framework to simulate the process of single-hop trust propagation [11].

The problem of trust prediction could be approached through various methods, such as matrix factorization and propagated trust. However, there has been limited research considering the complementary nature of these methods. To address this gap, X. Gao et al. introduced a novel trust prediction scheme called iSim, which integrated three factors to evaluate user similarity [12]. iSim was a conventional approach for predicting trust typically rely on static graphs as input, disregarding the time-dependent nature of social interactions. W. Lin et al. proposed a model called Medley, which captured time-varying latent factors and predicts the evolution of social trust over time [13]. They utilized functional time encoding to capture continuous-time features and incorporates evolving topological structures to infer pairwise social trust from past interactions.

As discussed above, we compile and analyze these graph-based trust evaluation schemes in Table 1. They are categorized as direct experience (DE) and indirect experience (IE) based on the type of historical experience. Furthermore, the "Rep." represents the model's assessment of the node's reputation, the "Loc." signifies the evaluation of trust as local trust, and the "Glo." denotes the evaluation of trust as global trust, and A, P, R represent accuracy, precision, and recall, respectively.

2.2 Other Deep Learning Method

The scale of OSNs is vast, and graph-based trust evaluation schemes often encounter the challenge of exponentially increasing computational complexity. The graph-based methods can aid in identifying and building trust relationships between users, thereby identifying potential unreliable users or harmful information. Nevertheless, graph-based schemes often face limitations in identifying all trustworthy paths, which may necessitate the imposition of certain restrictions during the path-finding process.

Instead of relying solely on graph-based search algorithms, N. Fatehi et al. employed a distributed learning automata (DLA) to discover all trustworthy relationships [17]. It was proved that the flexibility and scalability of models can be improved [18]. Trust

Table 1. Summary of the Related Work on Trust Evaluation with Graph-Based Deep Learning Methods in OSNs

Scheme	DE	IE	Trust	Rep.	Loc.	Glo.	Dataset	Result	Advantage	Disadvantage
TrustGNN [6]	✓	✓	✓	×	✓	✓	Advogato, PGP, Ciao, Epinions	F1 = 74.4%, 87.2%, 72.8%, and 81.8%; MAE = 0.081, 0.083, 0.050, and 0.032	Compared to other benchmarks, it exhibits superior accuracy, minimal errors, and low time complexity	It is limited to static networks, and its modeling and computation processes are singular
DCAT [9]	✓	✓	✓	×	✓	✓	Ciao, Epinions	MAE = 0.36 and 0.4	Strong context-awareness ability	Weak ability to dynamically capture trust relationships
CHEN [10]	✓	✓	✓	×	×	✓	Twitter Dataset	A = 96%	High accuracy by analyzing the overlapping area of positive and negative feature distributions	Weak context-awareness ability for different scenarios and time
NeuralWalk [11]	–	–	✓	×	✓	✓	Advogato, PGP	F1 = 74.6% and 91.6%	It can accurately predict unknown trust relationships in an inductive manner	High time cost and computational consumption
iSim [12]	–	–	✓	×	✓	×	Advotago, RobotNet	MAE = 0.1473 and 0.1300	Low time complexity and strong context awareness-ability	Poor robustness and generalization performance
Medley [13]	×	✓	✓	×	✓	×	Bitcoin-Alpha	A = 73.3%	Obtaining time features and using attention mechanism to assign weights	High energy consumption and time cost
GATrust [14]	✓	✓	✓	–	✓	✓	Advogato, PGP	F1 = 0.773 and 0.913, MAE = 0.076 and 0.079	Improving the social trust evaluation performance of users and predict trust	Facing challenges related to the spatial and temporal dependencies

reasoning quality has heavily relied on trust propagation, which was influenced by various factors, such as the length of the path between users. For instance, DLATrust [19],

proposed by M. Ghavipour et al., aimed to identify reliable paths, and the trust network was treated as a static graph. However, the trust weights often change dynamically over time, prompting researchers to introduce a dynamic trust propagation algorithm called DyTrust [20]. To tackle challenges like the cold start problem and data sparsity, TrustDL [21] was proposed to integrate various information sources, including trust ratings, into the recommendation model.

However, the attributes of trust networks with directed edges and nodes with in-links and out-links could not be effectively captured by most existing networks with embedded solutions. A scheme proposed by Q. Wang et al., AtNE-Trust, was capable of capturing high-quality user embeddings and making accurate trust predictions [22]. Nevertheless, most trust prediction methods tend to focus on specific aspects of trust, lacking comprehensive research on the development of user trust. They introduced C-DeepTrust to fill this gap [23]. Furthermore, existing methods primarily aim to improve predictive performance by using more available information, but the influence of user information authenticity and user subjectivity was frequently disregarded in trust studies. S-DeepTrust [24] was proposed to address this gap by employing transfer learning to derive emotion labels from user review data, resulting in an emotion polarity matrix. This matrix was subsequently weighted to produce a revised rating matrix, enhancing the integration of emotional cues into the trust evaluation process.

We summarize the related work mentioned above in Table 2. Some abbreviations are the same as in Table 1 and "Tech." indicates the technique used by the model. From Table 2. It is evident that DL-based trust evaluation models exhibit a notable propensity for high time and energy consumption. This can be attributed to the inherent nature of DL, which necessitates extensive data processing and optimization tasks. Besides, there are several datasets commonly used for training models. For, example, the Trustlet[2] dataset from an online trust relationship network, including data from Epinions[2] and Ciao[3], two e-commerce websites. It encompasses social relationships between users, user ratings of products, and associations between products on these datasets.

3 Challenges and Open Problems

Despite the substantial contributions made by researchers in this field, numerous unresolved problems and challenges persist. Here, we outline several key problems and challenges pertaining to trust evaluation in OSNs.

Firstly, the applicability of some trust management models has been restricted because of the diverse range of network structures [10, 16]. There isn't a universally applicable trust model, and it's imperative to devise tailored protocols for each specific trust evaluation approach [25]. Trust evaluation configurations may vary across different network topologies or application contexts. The integration of adaptive mechanisms allows for flexible adjustment of parameters and strategies within the trust model, facilitating accommodation of diverse network structures and environmental conditions.

Secondly, in OSNs, trust evaluation models based on GNN may encounter the problem of exponentially increasing computational complexity, especially as the network

[2] http://trustlet.org/datasets/advogato.

[3] http://www.cse.msu.edu/~tangjili/trust.html.

Table 2. Summary of the Related Work on Trust Evaluation with Other Deep Learning Methods in OSNs

Scheme	DE	IE	Trust	Rep.	Loc.	Glo.	Tech.	Dataset	Result	Advantage	Disadvantage
DeciTrustNET [16]	✓	✓	✓	✓	×	✓	Graph-based	–	–	Evaluating trust in a more complete manner	Lacking context-awareness ability for different scenarios
FATEHI [17]	✓	✓	✓	×	×	✓	DLA	Epinions	A = 93.98%	The limitation of finding trusted paths	Long execution time
DLATrust [19]	×	✓	✓	×	✓	✓	DLA	Advogato	MAE = 0.1152; P = 96.32%, R = 97.38%	Identifying reliable trust paths with higher accuracy	It could not effectively predict dynamic trust
DyTrust [20]	×	✓	✓	×	✓	✓	DLA	Kaitiaki	MAE = 0.1152, P = 95.43%, R = 99.43%	Inferring dynamic trust accurately	High energy consumption and time cost
C-DeepTrust [23]	✓	✓	✓	×	✓	×	LSTM	Epinions, Ciao	F1 = 0.917 and 0.924	Achieving a high level of prediction accuracy	High time complexity
S-DeepTrust [24]	✓	✓	✓	×	✓	×	LSTM	Epinions, Ciao	F1 = 0.942 and 0.918	High predictive precision and robustness in dealing with the sparsity of data	It is complex, with high computational costs

size grows [6, 11–13]. This is because in a large-scale network, GNN need to handle a large number of nodes and edges, leading to a sharp increase in computational complexity. To mitigate this challenge, the random sampling techniques can be used to select a subset of nodes and edges for training. It can reduce the computational load, but may result in information loss. Besides, it can assist in selecting appropriate GNN structures and hyperparameters to optimize performance with learning automata.

Thirdly, the dependence of trust evaluation on historical data is emphasized. However, in large-scale social networks, interactions between nodes are often sparse [16, 19]. It presents a challenge in accurately assessing the initial trust of newly introduced nodes at the system's outset, a problem commonly known as the cold-start problem [26]. During the initial stage, lower accuracy in trust evaluation tends to result from

the limited availability of historical data. Consequently, accurately evaluating the initial trustworthiness in the early phases of the system proves challenging.

Lastly, the unequal distribution of samples among various classes or labels within a dataset is termed class imbalance [11, 20]. The performance of machine learning models is adversely affected, including reduced accuracy and generalization ability. To mitigate this issue, dataset balancing techniques are commonly employed. With dataset balancing techniques, the number of samples are augmented in the minority class and reduced in the majority class. Additionally, it often proves effective in handling imbalanced data by employing ensemble methods like random forests or gradient boosting trees, as they can amalgamate predictions from multiple models [27].

4 Research Direction

4.1 Trust Evaluation Based on Ensemble Learning with DNN in OSNs

Ensemble Learning (EL) is a powerful AI technique that combines multiple machine learning approaches to obtain the best possible solution. However, it is not without its drawbacks, which include long training hours and high computational overhead. In contrast, models based on deep neural networks show greater adaptability to the environment than traditional models. For these challenges, we propose to train a DNN-based selector to select a suitable set of classifiers. This DNN-based selector efficiently determines which ML method classifiers are appropriate for the specific problem at hand. This pre-screening process reduces training and computation overhead.

A selector model based on deep neural networks is constructed, which can effectively identify suitable machine learning methods based on input problem characteristics. The architecture of this selector may include CNNs, RNNs, Transformer, or other variants. Once the deep neural network selector model is trained, it can be applied to real-world scenarios. When faced with a new problem, its features are input into the selector model. The output of this model, a collection of applicable machine learning methods, helps with the initial screening. This screening process notably diminishes training and computational overhead, as it obviates the need to train and evaluate all potential methods, focusing instead on those recommended by the selector.

4.2 Cross-Origin Trust Evaluation Based on Deep Learning with a Hyperparameter Auto Optimizer in OSNs

Integrating a hyperparameter auto optimizer into cross-domain evaluation systems for OSNs is a promising approach because it could present a promising solution to the persistent challenge of effectively detecting a multitude of violations such as fraud and spam. The difficulty in achieving this effectiveness often arises from the constraints in selecting appropriate training datasets for these evaluation systems, rendering them inadequately equipped to adapt to the dynamic online landscape and the diverse range of violations encountered.

By incorporating a hyperparameter auto optimizer into these evaluation systems, researchers could enable the automatic selection of optimal detection subsystems and

hyperparameter configurations. The system is highly adaptable and can flexibly respond to the changing social network environment. Therefore, by deploying this model, various violations can be better detected, thus enhancing the security of the social network. In addition, the introduction of hyperparameter automatic optimizers brings several significant advantages to OSNs cross-domain evaluation systems. First, the adaptability of the system could be enhanced, because the model can automatically select the best configuration on different social networking platforms without manual adjustment. Second, by integrating multiple trained detection subsystems, violations more comprehensively can be identified, overcoming the limitations of relying on a single IDS.

Ultimately, through the proposed model, not only can the overall user experience be improved, but the credibility of the online platform can also be enhanced and the security of the social network can be improved. By making the social space safer and more conducive to positive interactions, the integration of hyperparametric automated optimizers into cross-domain evaluation systems represents a critical step in promoting trust and confidence in the digital realm.

5 Conclusion

We provide a review of research concerning trust evaluation employing deep learning within online social networks is presented. Trust evaluation has been proven to be a powerful method in mitigating internal attacks, while intrusion detection acts as a robust defense against external threats. Nonetheless, certain challenges arise with graph-based models due to their exponential computational complexity. Consequently, we delve into some other deep learning techniques and discuss the strategies to mitigate these challenges. Firstly, we conduct a comparison and analysis of the latest trust evaluation schemes, focusing on graph neural networks and other deep learning approaches. We emphasize the exponential increase in computational complexity associated with graph neural network methods as network scale expands. Subsequently, some possible solutions for the challenges and problems encountered in trust evaluation are proposed. These challenges include network structural diversity, high computational complexity, cold start problems, and sample imbalance. Then, we suggest corresponding optimization strategies to tackle these challenges effectively. Finally, we propose two future research directions, which include trust evaluation through ensemble learning and cross-source trust evaluation utilizing hyperparameter auto-optimization. In summary, it offers a review of deep learning-based trust evaluation in OSNs, highlighting its significant importance in enhancing understanding and improving trust evaluation within such networks.

Acknowledgments. This study was funded in part by the Key Research and Development Task Special Project of the Xinjiang Uygur Autonomous Region (grant number 2022B01009), in part by the Shanghai Science and Technology Innovation Action Plan (grant number 21DZ1200600), in part by the National Key Research and Development Program (grant number 2020YFB2104202), and in part by the Shanghai Natural Science Foundation (grant number 21ZR1461700).

References

1. Kumar, S., Revathy, S.: Review on social network trust with respect to big data analytics. In: 2020 4th International Conference on Trends in Electronics and Informatics, Tirunelveli, India, pp. 721–727. IEEE (2020)
2. Fang, W., Cui, N., Chen, W., Zhang, W., Chen, Y.: A trust-based security system for data collection in smart city. IEEE Trans. Ind. Inf. **17**(6), 4131–4140 (2021)
3. Li, Z., Fang, W., Zhu, C., Gao, Z., Zhang, W.: AI-enabled trust in distributed networks. IEEE Access **11**, 88116–88134 (2023)
4. Fang, W., Zhu, C., Yu, F.R., Wang, K., Zhang, W.: Towards energy-efficient and secure data transmission in AI-enabled software defined industrial networks. IEEE Trans. Ind. Inf. **18**(6), 4265–4274 (2022)
5. Niu, X., Liu, G., Yang, Q.: Trustworthy website detection based on social hyperlink network analysis. IEEE Trans. Netw. Sci. Eng. **7**(1), 54–65 (2018)
6. Huo, C., He, D., Liang, C., Jin, D., Qiu, T., Wu, L.: TrustGNN: graph neural network-based trust evaluation via learnable propagative and composable nature. IEEE Trans. Neural Netw. Learn. Syst., 1–13 (2023)
7. Fang, W., Zhu, C., Guizani, M., Rodrigues, J.J.P.C., Zhang, W.: HC-TUS: human cognition-based trust update scheme for AI-enabled VANET. IEEE Netw. https://doi.org/10.1109/MNET.2023.3320934
8. Hamilton, W., Ying, Z., Leskovec, J.: Inductive representation learning on large graphs. Adv. Neural. Inf. Process. Syst. **30**, 1024–1034 (2017)
9. Ghafari, S.M., Joshi, A., Beheshti, A., Paris, C., Yakhchi, S., Orgun, M.: DCAT: a deep context-aware trust prediction approach for online social networks. In: Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia, pp. 20–27. ACM (2019)
10. Chen, X., Yuan, Y., Lu, L., Yang, J.: A multidimensional trust evaluation framework for online social networks based on machine learning. IEEE Access **7**, 175499–175513 (2019)
11. Liu, G., Li, C., Yang, Q.: NeuralWalk: trust assessment in online social networks with neural networks. In: Proceedings of the IEEE Conference on Computer Communications, Paris, France, pp. 1999–2007. IEEE (2019)
12. Gao, X., Xu, W., Liao, M., Chen, G.: Trust prediction for online social networks with integrated time-aware similarity. ACM Trans. Knowl. Discov. Data **15**, 1–30 (2021)
13. Lin, W., Li, B.: Medley: predicting social trust in time-varying online social networks. In: Proceedings of the IEEE Conference on Computer Communications, Vancouver, BC, Canada, pp. 1–10. IEEE (2021)
14. Jiang, N., Jie, W., Li, J., Liu, X., Jin, D.: GATrust: a multi-aspect graph attention network model for trust assessment in OSNs. IEEE Trans. Knowl. Data Eng. **35**(6), 5865–5878 (2023)
15. Jain, L., Katarya, R., Sachdeva, S.: Opinion leaders for information diffusion using graph neural network in online social networks. ACM Trans. Web **17**(2), 1–37 (2023)
16. Ureña, R., Chiclana, F., Herrera-Viedma, E.: DeciTrustNET: a graph-based trust and reputation framework for social networks. Inf. Fus. **61**, 101–112 (2020)
17. Fatehi, N., Shahhoseini, H.S., Wei, J., Chang, C.T.: An automata algorithm for generating trusted graphs in online social networks. Appl. Soft Comput. **118**, Article no. 108475 (2022)
18. Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W., Yang, Y.: Trust management-based and energy-efficient hierarchical routing protocol in wireless sensor networks. Digit. Commun. Netw. **7**(5), 470–478 (2021)
19. Ghavipour, M., Meybodi, M.R.: Trust propagation algorithm based on learning automata for inferring local trust in online social networks. Knowl. Based Syst. **143**, 307–316 (2018)

20. Ghavipour, M., Meybodi, M.R.: A dynamic algorithm for stochastic trust propagation in online social networks: learning automata approach. Comput. Commun. **123**, 11–23 (2018)
21. Khaledian, N., Nazari, A., Khamforoosh, K., Abualigah, L., Javaheri, D.: TrustDL: use of trust-based dictionary learning to facilitate recommendation in social networks. Expert Syst. Appl. **228**, Article no. 120487 (2023)
22. Wang, Q., Zhao, W., Yang, J., Wu, J., Zhou, C., Xing, Q.: AtNE-trust: attributed trust network embedding for trust prediction in online social networks. In: Proceedings of the 2020 IEEE International Conference on Data Mining (ICDM), pp. 601–610. IEEE (2020)
23. Wang, Q., et al.: C-DeepTrust: a context-aware deep trust prediction model in online social networks. IEEE Trans. Neural Netw. Learn. Syst. **34**(6), 2767–2780 (2021)
24. Wang, Q., et al.: S-DeepTrust: a deep trust prediction method based on sentiment polarity perception. Inf. Sci. **633**, 104–121 (2023)
25. Ahvar, E., Fathy, M.: BEAR: a balanced energy-aware routing protocol for wireless sensor networks. Wirel. Sens. Netw. **2**(10), 793–800 (2010)
26. Siau, K., Wang, W.: Building trust in artificial intelligence, machine learning, and robotics. Cut. Bus. Technol. J. **31**(2), 47–53 (2018)
27. Fang, W., Zhu, C., Zhang, W.: Toward secure and lightweight data transmission for cloud–edge–terminal collaboration in artificial intelligence of things. IEEE Internet Things J. **11**(1), 105–113 (2024)