International Journal on Applications in Engineering and Technology
Volume 9 : Issue 2 : April 2023, pp 14 – 18 www.aetsjournal.com ISSN (Online) : 2455 - 0523

DETECT PROFESSIONAL MALICIOUS USER WITH METRIC LEARNING IN RECOMMENDER SYSTEMS

M.HEMALATHA , M.SHANMUGA PRIYA

Abstract— In e-commerce, online retailers are usually suffering from professional malicious users (PMUs), who utilize negative reviews and low ratings to their consumed products on purpose to threaten the retailers for illegal profits. PMUs are difficult to be detected because they utilize masking strategies to disguise themselves as normal users. Specifically, there are three challenges for PMU detection: 1) professional malicious users do not conduct any abnormal or illegal interactions (they never concurrently leave too many negative reviews and low ratings at the same time), and they conduct masking strategies to disguise themselves. Therefore, conventional outlier detection methods are confused by their masking strategies. 2) the PMU detection model should take both ratings and reviews into consideration, which makes PMU detection a multi-modal problem. 3) there are no datasets with labels for professional malicious users in public, which makes PMU detection an unsupervised learning problem. To this end, we propose an unsupervised multi-modal learning model: MMD, which employs Metric learning for professional Malicious users Detection with both ratings and reviews. MMD first utilizes a modified RNN to project the informational review into a sentiment score, which jointly considers the ratings and reviews. Then professional malicious user profiling (MUP) is proposed to catch the sentiment gap between sentiment scores and ratings. MUP filters the users and builds a candidate PMU set. We apply a metric learning-based clustering to learn a proper metric matrix for PMU detection. Finally, we can utilize these metric and labeled users to detect PMUs. Specifically, we apply the attention mechanism in metric learning to improve the model's performance. The extensive experiments in four datasets demonstrate that our proposed method can solve this unsupervised detection problem. Moreover, the performance of the state-of-the-art recommender models is enhanced by taking MMD as a preprocessing stage.

M.Hemalatha , Assistant Professor , Department of Computer Applications , Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.
(Email : hemasenguthar92@gmail.com)

M.Shanmuga Priya , PG Scholar , Department of Computer Applications, Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.
(Email : priyamuthuvel574@gmail.com)

I. INTRODUCTION

E-COMMERCE giants, such as Amazon, Jingdong, and Alibaba, have been thriving with the development of Internet technology, where millions of electronic retailers produce great wealth through selling commodities on the websites [1]. For each day, billions of trades occur between retailers and consumers [2]. For the sake of improving the consumers' experience of online shopping, e-commerce websites usually allow consumers (we call them "users") to leave reviews and rank ratings on the commodities (we call them "items"). To trade off the interests between retailers and users, e-commerce websites punish the retailers who receive a high percentage of negative reviews and low ratings from users[3]. Being widely applied in almost all kinds of e-commerce websites, this feedback mechanism has been proved to be effective if all the users leave truthful and objective reviews or ratings.

However, in practice, there exist some malicious users (MU), who leverage this feedback mechanism to gain illegal profits [4, 5]. For example, these malicious users first purposefully leave negative reviews and low ratings of their consumed products without any consideration of the commodities' quality. Then they blackmail the electronic retailers to make illegal profits; otherwise, they would leave more negative feedbacks, cheating e-commerce websites to punish the electronic retailers and confuse the normal users about the items in recommendations. As a result, these malicious users undermine the fairness of e-commerce. Moreover, their negative feedbacks will confuse the recommender systems (collaborative filtering-based models [6] or content based models [7]), leading to a chaotic recommendation for normal users, which is also named as shilling attacks [8, 9].

To address the above issues, e-commerce companies usually employ statistic outlier detection or shilling attack detection models [10–12] to detect MUs, i.e., finding objective users who always give negative reviews or low ratings.

However, there are some restrictions for these detection models: first, these models only tackle this problem from a methodological perspective and ignore the real-world scenarios. For example, most detection models ignore that there are some professional malicious users (PMUs), who can utilize masking strategies to avoid detection; second, they usually focus on filtering either fake ratings to improve recommendation models, or negative reviews for content based models, which do not take both ratings and reviews into account. As a result, these models may be applied in limited application scenarios in recommender systems, but not proper for professional malicious user detections.

Different from malicious users, professional malicious users (PMU) typically adopt the following two masking strategies to avoid existing detections: 1) To avoid giving too many low ratings, they provide a high rating but a negativereview. In this way, they can mislead the potential consumer who is browsing this review to decide whether to buy this item. 2) To avoid giving too many negative reviews, they provide a low rating but a positive review. In this way, they can explain to the outlier detection that their interactions are "misoperations". By applying the above two strategies, alternately, professional malicious users can disguise themselves as normal users. As shown in Fig.1, we give an example to indicate how professional malicious users confuse potential consumers and undermine the fairness of online e-commerce.

In this paper, we focus on how to detect these PMUs with masking strategies in real-world scenarios by simultaneously analyzing their ratings and reviews.

To detect PMUs, there are three significant challenges in recommender systems: 1) PMUs adopt masking strategies to act like normal users, which is difficult to be detected. 2) Detecting PMUs needs to analyze both ratings and reviews, which makes it a multi-modal problem. 3) Existing public datasets do not contain the PMU label, which makes this detection an unsupervised learning problem. To this end, we propose an unsupervised multi-modal learning model: **MMD**, which applies metric learning [13–15] for professional malicious user detection with both ratings and reviews.The key to metric learning is utilizing different metrics (Euclidean distance or other metrics) to represent the relationships between entities [16, 17].MMDfirst utilizes Hierarchical Dual-Attention RNN (HDAN) [18] to do user profiling with reviews and ratings. By catching the sentiment gap between reviews and ratings, we build a candidate PMU set. Then we apply an unsupervised metric learning based clustering method to this candidate set to label professional malicious users. To be specific, we apply the attention mechanism in metric learning to enhance the model. We conduct experiments on four real-world datasets: Amazon, Yelp, Taobao, and Jingdong. The results demonstrate that our proposed method can solve this unsupervised malicious user detection problem. Moreover, their performance of the state-of-the-art recommender models can be enhanced by taking MMD as a preprocessing stage.

We summarize the main contributions as follows.

- ❖ This is the first work focusing on solving the professional malicious user detection issue utilizing both users' ratings and reviews to enhance the state-of the art recommender systems.
- ❖ A novel multi-modal unsupervised method-MMD-is proposed to detect professional malicious users with the modified RNN and attention metric learning based clustering.
- ❖ Extensive experiments are conducted on four real world e-commerce datasets to verify our proposed method. Moreover, by filtering professional malicious
- ❖ Users, some state-of-the-art models are enhanced.

II. EXISTING SYSTEM:

As we define professional malicious users in recommender systems, malicious user detection is a new problem, which is an issue with little attention

yet. However, we can treat this detection issue as a special case of abnormal user detection, and some existing works in this area can inspire us [35, 36]. In e-commerce, various abnormal users (spammers, shilling group, and frauds) have greatly damaged the systems, and some abnormal user detection models are proposed to tackle this issue. [37] proposed a hybrid model to detect the spammers through users' profile and relations. [38] explored spammer detection in big and sparse data. Shilling attacks harm the recommender system by injecting fake profile information of users and items. They cheat the recommendation model, such as Collaborative Filtering and Matrix Factorization [12]. [39] proposed this attack type and gave a basic supervised solution to tackle it. [12] proposed a convolutional neural network to solve shilling attacks and improved collaborative filtering. Frauds usually give fake reviews to hurt the profits of electronic retailers. [40, 41] also explored fraud detection in large-scale dataset and real scenarios.

Some researches of abnormal user detection utilize the machine learning model to find fake ratings or reviews [42, 43] and achieve an effective result. However, different from abnormal users above (spammers, shilling group, and fraud), professional malicious users are smarter and craftier. Shilling attacks inject fake ratings or reviews just before the recommendation process [44, 45], while for PMUs, all the actions that professional malicious users have taken are well-behaved by the rules of e-commerce websites (called masking strategies). They utilize the bug of abnormal detections, without leaving low ratings and negative feedback at the same time, to avoid detections.

Then they can make illegal profits and hurt the electronic retailers. Basically, they are "normal" users for the existing abnormal user detection models, which makes the professional malicious user detection a critical issue in the recommender system area.

Disadvantages

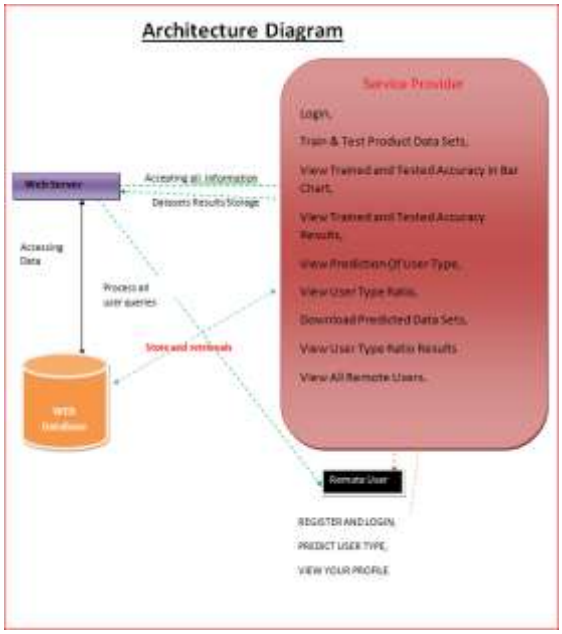
- The system not implemented Professional Malicious User Profiling (MUP) model.
- The system not implemented Attention Metric Learning for Clustering (MLC) and Hierarchical Dual-Attention RNN.

III. PROPOSED SYSTEM

- This is the first work focusing on solving the professional malicious user detection issue utilizing both users' ratings and reviews to enhance the state-of the- art recommender systems.
- A novel multi-modal unsupervised method-MMD-is proposed to detect professional malicious users with the modified RNN and attention metric learning based clustering.
- Extensive experiments are conducted on four real world e-commerce datasets to verify our proposed method. Moreover, by filtering professional malicious users, some state-of-the-art models are enhanced.

Advantages

- This is the first work focusing on solving the professional malicious user detection issue utilizing both
- users' ratings and reviews to enhance the state-ofthe- art recommender systems.
- A novel multi-modal unsupervised method-MMD-is proposed to detect professional malicious users with the modified RNN and attention metric learning based clustering.
- Extensive experiments are conducted on four real world e-commerce datasets to verify our proposed method. Moreover, by filtering professional malicious users, some state-of-the-art models are enhanced.



IV. MODULES

1) Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Train & Test Product Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of User Type, View User Type Ratio, Download Predicted Data Sets, View User Type Ratio Results, View All Remote Users.

2)View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

3)Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT USER TYPE, VIEW YOUR PROFILE.

V. CONCLUSION

In this work, we first defined the professional malicious users (PMUs), who give fake feedbacks to confuse the normal users, hurt the recommender systems, and make illegal profits. We noticed that the traditional outlier detections could not be applied in the recommender system area to detect these professional malicious users because of their professional masking strategies (never give negative reviews and low ratings at the same time). Also, supervised detection models could not work well on PMU detection for the lack of labels. To address the professional malicious user detection issue, we presented a new unsupervised multimodal learning model named MMD. By utilizing both reviews and ratings simultaneously, MMD obtained a proper metric to cluster users and detected professional malicious users. Extensive results on four real-world datasets demonstrated the effectiveness and strength of our method and the improvement by applying our method for recommender systems.

In essence, MMD is a generic solution, which can not only detect the professional malicious users that are explored in this paper but also serve as a general foundation for malicious user detections. With more data, such as image, video, or sound, the idea of MMD can be instructive to detect the sentiment gap between their title and content, which has a bright future to counter different masking strategies in different applications. Moreover, we will incorporate multimedia data into our model and consider the effect of contexts, such as consuming time, clicks, and other interactions. At last, we are very interested in building an online professional malicious user detection model that utilizes the recent advances in human-machine interactions.

VI. REFERENCES

[1] C. G. Traver and K. C. Laudon, E-commerce: business, technology, society. Pearson Prentice Hall/Pearson Education, 2008.

[2] B. Rutherford, A. Dagher, M. Wiseman, D. J. M. C. Paie, J.-P. E. Rans, F. Ates, and J.Wankmueller, "Customer authentication in e-commerce transactions,"Dec. 6 2016, uS Patent 9,514,458.

[3] S. Akter and S. F. Wamba, "Big data analytics in e-commerce: a systematic review and agenda for future research," Electronic Markets, vol. 26, no. 2, pp.173–194, 2016.

[4] M. Si and Q. Li, "Shilling attacks against collaborative recommender systems: a review," Artificial Intelligence Review, pp. 1–29, 2018.

[5] Y. Cai and D. Zhu, "Trustworthy and profit: A new value-based neighbor selection method in recommender systems under shilling attacks," Decision Support Systems, vol. 124, p. 113112, 2019.

[6] X. He, L. Liao, H. Zhang, L. Nie, X. Hu, and T.-S. Chua, "Neural collaborative filtering," in Proceedings of the 26th international conference on world wide web. International World Wide Web Conferences Steering Committee, 2017, pp. 173–182.

[7] J. Su, "Content based recommendation system," Jan. 5 2016, uS Patent 9,230,212.

[8] W. Zhou, J. Wen, Q. Xiong, M. Gao, and J. Zeng, "Svm-tia a shilling attack detection method based on svm and target item analysis in recommender systems," Neurocomputing, vol. 210, pp. 197–205, 2016.

[9] Y. Xu and F. Zhang, "Detecting shilling attacks in social recommender systems based on time series analysis and trust features," Knowledge-Based Systems, vol. 178, pp. 25–47, 2019.

[10] S. K. Kwak and J. H. Kim, "Statistical data preparation: management of missing values and outliers," Korean journal of anesthesiology, vol. 70, no. 4, p.407, 2017.

[11] R. A. Maronna, R. D. Martin, V. J. Yohai, and M. Salibi´an-Barrera, Robust statistics: theory and methods (with R). John Wiley & Sons, 2019.

[12] C. Tong, X. Yin, J. Li, T. Zhu, R. Lv, L. Sun, and J. J. Rodrigues, "A shilling attack detector based on convolutional neural network for collaborative recommender system in social aware network," The Computer Journal, vol. 61,no. 7, pp. 949–958, 2018.

[13] D. Wang and X. Tan, "Robust distance metric learning via bayesian inference," IEEE Transactions on Image Processing, vol. 27, no. 3, pp. 1542–1553, 2018.

[14] X. Sui, E. L. Xu, X. Qian, and T. Liu, "Convex clustering with metric learning," Pattern Recognition, vol. 81, 2018.

[15] W. Zuo, F. Wang, D. Zhang, L. Lin, Y. Huang, D. Meng, and L. Zhang,"Distance metric learning via iterated support vector machines," IEEE Transactions on Image Processing, vol. PP, no. 99, pp. 1–1, 2017.

[16] H. J. Ye, D. C. Zhan, and Y. Jiang, "Fast generalization rates for distance metric learning," Machine Learning, pp. 1–29, 2018.

[17] J. Li, A. J. Ma, and P. C. Yuen, "Semi-supervised region metric learning for person re-identification," International Journal of Computer Vision, vol. 126, no. 8, pp. 855–874, 2018.

[18] Y. Xu, Y. Yang, J. Han, E. Wang, F. Zhuang, J. Yang, and H. Xiong, "Neuo: Exploiting the sentimental bias between ratings and reviews with neural networks," Neural Networks, vol. 111, pp. 77–88, 2019.

[19] Y. Xu, Y. Yang, J. Han, E. Wang, J. Ming, and H. Xiong, "Slanderous user detection with modified recurrent neural networks in recommender system," Information Sciences, vol. 505, pp. 265–281, 2019.

[20] Z. Yang, D. Yang, C. Dyer, X. He, A. Smola, and E. Hovy, "Hierarchical attention networks for document classification," Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp. 1480–1489, 2016.

[21] E. P. Xing, M. I. Jordan, S. J. Russell, and A. Y. Ng, "Distance metric learning with application to clustering with side-information," in Advances in neural information processing systems, 2003, pp. 521–528

[22] X. He, H. Zhang, M.-Y. Kan, and T.-S. Chua, "Fast matrix factorization for online recommendation with implicit feedback," in Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval. ACM, 2016, pp. 549–558.

[23] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez,Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in Advances in neural information processing systems, 2017, pp. 5998–6008.

[24] M.-T. Luong, H. Pham, and C. D. Manning, "Effective approaches to attention-based neural machine translation," arXiv preprint arXiv:1508.04025,2015.

[25] X. He, J. Tang, X. Du, R. Hong, T. Ren, and T.-S. Chua, "Fast matrix factorization with nonuniform weights on missing data," IEEE transactions on neural networks and learning systems, 2019.