MSPLD: Shilling Attack Detection Model Based on Meta Self-Paced Learning

Yanjing Yang[1], Min Gao[1,*], Yuerang Li[1], Fan Wu[1], Jia Wang[1], Quanwu Zhao[2,3]
[1]School of Big Data and Software Engineering, Chongqing University, Chongqing, China, 400044
[2]School of Economics and Business Administration, Chongqing University, Chongqing,China, 400033
[3]Chongqing Key Laboratory of Logistics, Chongqing University, Chongqing,China, 400033
{yangyj, gaomin, liyr, wufan, jiawang, zhaoquanwumx}@cqu.edu.cn

***Abstract*—With the dramatic rise of recommendation systems, more and more companies use them to improve users' experience. However, the openness of the recommender systems makes them vulnerable to shilling attacks, which causes a bad impact on user satisfaction. Existing shilling attack detection models usually have problems in solving the noise of samples and labels. To this end, this paper proposes a shilling attack detection model based on meta self-paced learning, named MSPLD. Meta self-paced learning can make the model select samples from easy to difficult in the learning process, which can alleviate the problem that the model parameters are difficult to optimize due to the outliers or noises in the samples. Specifically, MSPLD adopts some methods to get the extraction of potential feature embedding vectors first. Second, metadata is selected adaptively by a regression method. Then, it uses the embedding vectors of malicious users and metadata as input data. Third, it optimizes the age loss function and the loss function of the classifier itself with bilateral optimization. The relationship between age and sample loss of the classifier will determine the weight of sample selection. Finally, using the tendency of the age gradually to select training samples from easy to difficult can improve the generalization ability of the models. Compared with the state-of-the-art detection models, the experimental results on two public datasets show that MSPLD can achieve better detection performance. Besides, we illustrate the training process of MSPLD to analyze the reason for the superiority of the model.**

Keywords—shilling attack detection, meta self-paced learning, visual theoretical reliability analysis.

I. INTRODUCTION

With the constantly rising of the internet industry, such as the e-commerce Taobao and Amazon, video streaming TikTok and YouTube have gradually become the primary means of daily shopping and news information acquisition for the public. The dramatic development of these platforms depends on the recommendation system [1]. Accurate and reliable recommendation not only optimizes the experience of customers but also maintains healthy competition in the market to some extent. However, the openness of the recommender system makes it vulnerable to shilling attacks. Shilling attack is a way to control the ranking of the target items in the recommendation system. Shilling attack greatly affects the stability and accuracy [2] of recommendation systems by injecting malicious information. According to the relevant research, malicious users only need to inject 1% shilling attack user profiles into recommendation systems to improve the recommendation ranking of the target item to the first place [3].

Researchers have deeply carried out research on this kind of problem. The detection methods based on unsupervised learning such as the PCA and PLSA proposed by Mehta [4] use a clustering method to detect malicious users. These methods usually have the problem of high false-positive and low robustness [5]. Detection methods based on supervised learning such as the CoDetector [6] and RDMA [7] need labels of samples to train the classification model. However, due to the noise of samples and labels, it is difficult to extract and facilitate the accurate embedding of detection, therefore it is challenging to further improve the detection performance.

To tackle the challenge, in this paper, we propose a shilling detection model based on meta self-paced learning [8] (a. k. a MSPLD). MSPLD using a self-paced learning process to form better data selection tendency to select training samples from easy to difficult. It can mitigate the problems caused by the noise of samples and labels. The model consists of three parts. 1) To extract latent features based on models such as CoDetector [6], Node2Vec [9], and DL-DRA [10]. 2) To obtain metadata candidate sets by regression methods. 3) Metadata and latent feature embeddings are put into the model to optimize the age loss function and the loss function of the classifier itself with bilateral optimization. The relationship between age and sample loss of the classifier will determine the weight of sample selection. Using the tendency of the age, the samples are gradually selected from easy to complex. Inducing the model to fit the classification surface by this learning method can greatly improve the detection accuracy of the detection model for complex samples. Moreover, through the comparison of the combination of CoDetector [6] and Node2Vec [9] and other feature extraction methods, it can be found that the shilling attack detection model trained by the self-paced learning method can not only greatly improve the detection accuracy, but also further improve various evaluation metrics of detection. In summary, the contributions of the paper are as follows:

- We formally introduce the model of the shilling attack detection based on meta self-paced learning and show how

* Corresponding author

2021 International Joint Conference on Neural Networks (IJCNN) | 978-1-6654-3900-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/IJCNN52387.2021.9533622

978-0-7381-3366-9/21/$31.00 ©2021 IEEE

these malicious users are accurately identified in the self-paced learning process.

- We conduct experiments to validate the improvement of using the MSPLD model and explain why the model can improve the evaluation metrics on different datasets within both low and high accuracy ranges.
- Through the visual analysis of the training process and the combination of relevant evaluation metrics (such as the KL divergence), we illustrate the reliability of the training process of self-paced learning.

The remaining structure of this paper is as follows: In the next section, we provide the related research of shilling attack detection the meta self-paced learning method. The structure of the proposed shilling attack detection will be proposed in Section 3. The experiments and results will be illustrated in Section 4. Finally, we summarize our work and look forward to future researches in Section 5.

II. Related Work

Recommendation system-oriented shilling attack detection is, in essence, feature extraction and the combination of the two classification problems. And this section will introduce the recommendation system-oriented shilling attack detection research. Finally, the meta self-paced learning strategies will be introduced in this section.

A. Shilling attack detection

Nowadays, shilling attack detection in recommender systems has attracted the attention of researchers at home and abroad. Shilling attacks of malicious users will bring great harm to open recommendation systems. To solve this problem, researchers have proposed many shilling attack detection studies for recommender systems. Some of them detect malicious users by using users' rating information for projects, such as CoDetector and BayesDetector. CoDetector [6] factorizes both the user-rating item rating matrix and the user-user interaction matrix to obtain the embedding features of different users. BayesDetecor [11] uses the Bayesian method to improve the ability of CoDetector to extract users' feature embedding vectors. The algorithms above all depend on the matrix factorization to extract feature embedding vectors of users, but the extraction of feature embeddings often has a high complexity of data, and the classification results are often unsatisfactory when using a common shilling attack detection classifier. The Node2vec [9] is to construct the complex network architecture diagram of user-item-user and extract the potential feature embedding of different users from the diagram by using the random walk method. Compared with the matrix factorization feature extraction model, the effect of feature embedding extraction is better, but there is still a lot of room for optimization. The DL-DRA algorithm proposed by Zhou et al. [10] used an interpolation algorithm to adjust the density of the rating matrix and built a deep learning network, which is based on the CNN. The above algorithms are all detection algorithms based on supervised machine learning. And they all have unavoidable problems such as manual labeling.

Unsupervised learning and semi-supervised learning will solve the problem of manual labeling to some extent. The semi-supervised algorithm, such as Semi-SAD [13] , combines with the Bayesian classifier and maximization of extended distribution expectation to train labeled and unlabeled user data together. Unsupervised algorithms, such as the PCA and PLSA [4] method is through the collaborative clustering on the user level, by using the Markov model to calculate the user's suspicious degree, which combines with the hierarchical clustering method of user classification to achieve the purpose of shilling attack detection. However, these two kinds of methods still have problems such as high false-positives and the great influence of noise data.

Although those traditional attack detection algorithms for the traditional attack have good detection effect, but some new complex attacks are challenging to them.

B. Meta self-paced learning

Self-paced learning comes from curriculum learning. In 2009, Bengio first proposed the concept of curriculum learning in the ICML [14]. For curriculum learning, the model first learns the easy-to-understand, universal and simple knowledge structure by imitating the mechanism of the human learning process, and then selects a more complex and precise knowledge structure as the learning process progresses gradually. Self-paced learning is a further improvement based on curriculum learning. By setting age parameters, it can automatically select the knowledge structure that should be selected for the corresponding age, namely sample data. Then, it selects samples depends on the setting of model age hyperparameters and training strategies. The rationality and accuracy of the selected samples also determine the success of the self-paced learning process. Therefore, to achieve the purpose of self-adjusting the super-parameter age of self-paced learning, we adopt the method of meta self-paced learning.

In traditional machine learning, the objective function is usually as Eq. (1).

$$\mathbf{w} = \arg\min \mathbf{L}\left(\mathbf{f}_{\mathbf{w}}\left(\mathbf{X}\right), \mathbf{y}\right) \tag{1}$$

where $\mathbf{w} = (w_1, w_2, \cdots, w_n)'$ is the model hyperparameter, $\mathbf{X} \in M_{m,n}(\mathbf{R})$ is the user rating matrix, x_{ij} is the rating of the j product by the i user. $\mathbf{f}_{\mathbf{w}} : \mathbf{X} \to \mathbf{y}$ is the prediction function, and $\mathbf{L}(\mathbf{f}, \mathbf{y})$ is the model loss function. However, in self-paced learning, the objective function is

$$\{\mathbf{w}, \mathbf{v}\} = \arg\min\left(\mathbf{v} \cdot \mathbf{L}\left(\mathbf{f}_{\mathbf{w}}\left(\mathbf{X}\right), \mathbf{y}\right) + \mathbf{g}\left(\mathbf{v}, \lambda\right)\right) \tag{2}$$

Where $\mathbf{v} = (v_1, v_2, \cdots, v_m)'$ represents the selected weight of each data, $v_i \in [0,1]$; $\mathbf{g}(\mathbf{v}, \lambda)$ is the self-paced regularization function.

III. Method

We will introduce our model from three aspects: 1) The structure of shilling attack detection model for recommendation

systems. 2) Shilling attack detection classifier based on meta self-paced learning. 3) Data processing.

A. The structure of shilling attack detection model

The structure can be divided into three main parts (Fig. 1). The first part is to use the algorithms to get potential feature embedding vectors of users. The second part is to select the metadata adaptively. The final part is the shilling attack detection classifier based on the meta self-paced learning.

Firstly, we label the users-items data which are set to be detected, and then put them into the model. Secondly, multiple feature extraction algorithms are used to extract different types and dimensions of users' potential embedding vectors. Thirdly, some regression algorithms (such as Bayesian regression and logistic regression) are used for preliminary regression fitting to calculate the sample loss of the classifier. Using this method, we can select the metadata candidate set of potential users' embeddings according to their losses. Finally, the metadata can be selected from the candidate sets and put into the shilling attack detection classifier based on meta self-paced learning.

TABLE I. DETECTION CLASSIFIER BASED ON META SELF-PACED LEARNING

• variable	• Description
$\mathbf{X}=(\mathbf{x}_1,\mathbf{x}_2,\cdots,\mathbf{x}_m)'$ $\mathbf{x}_i=(x_{i1},x_{i2},\cdots,x_{in})$	$\mathbf{X}\in M_{m,n}(\mathbf{R})$ is rating matrix containing malicious users.
$\mathbf{y}=(y_1,y_2,\cdots,y_m)'$	User labels. $\forall y_i\in\{0,1\}$, 1 for legitimate users, and 0 for malicious users.
$D^m{}_{data}=(\mathbf{X},\mathbf{y})$	User potential characteristics embedding. m is the total number of users.
$D_{e-data}=(\mathbf{X}(i_j),\mathbf{y}(i_j))_{j=1}^{k}$	Metadata. Select a small number of k of user sample from D_{data} ($k<<m$).
$\Lambda=\{\lambda,\gamma\}$	The age parameter is used to describe the growth stage of the self-paced learning model. Comparing with the loss of the sample, it can calculate the selection weight.
$\mathbf{v}=(v_1,v_2,\cdots,v_m)'$	m dimension vector valued function.
$\mathbf{g}(\mathbf{v},\lambda)=(g(v_1,\lambda),\cdots,g(v_m,\lambda))'$	$g(v_i,\lambda)$ is a self-paced normalization function, i = 1, 2, …, m.
$\mathbf{f}_\mathbf{w}:\mathbf{X}\to\mathbf{y}$ $(x_{ij})\mapsto\hat{\mathbf{y}}$	$\mathbf{f}_\mathbf{w}(\mathbf{X})=(f_\mathbf{w}(\mathbf{x}_1),f_\mathbf{w}(\mathbf{x}_2),\cdots,f_\mathbf{w}(\mathbf{x}_m))'$ with $\mathbf{w}=(w_1,w_2,\cdots,w_n)'$, is a mapping space from user samples to labels, and it is also the classification function.
l_i	The loss function of $f_\mathbf{w}(\mathrm{X_i})$ and y_i. We consider the Euclidean distance between $f_\mathbf{w}(\mathrm{X_i})$ and y_i as the value of l_i.
$\mathbf{L}(\mathbf{f}_\mathbf{w}(\mathbf{X}),\mathbf{y})=\sum_{i=1}^{m}l_i$	The loss function.
α	Learning rate of age optimizer.
β	Learning rate of loss optimizer.

The self-paced age regularization and sample selection weight strategy is chosen for calculating the age loss and sample loss of the classifier in self-paced learning. These two losses are alternately put into the optimizer for bilateral optimization to get the parameters of the classifier conforming to the self-paced learning process. Finally, the classifier can use the parameters to detect the shilling attack.

B. Shilling attack detection classifier based on meta self-paced learning

In the first and the second parts of the system, we get the latent users' embeddings and the metadata candidate set adaptively selected according to the corresponding embeddings. Using the data, we can detect the shilling attack by shilling attack detection classifier based on meta self-paced learning. The variables used in the model are described in Table I.

1) Training sample weight selection and self-paced regularization

In the process of self-paced learning, it is necessary to attach the self-paced regularization to the age parameter loss function. Because the loss of age parameter without self-paced regularization will be proved to tend to 0 in the process of optimization (It will give up the selection of all samples in the learning process). To modify the result of the model whose age gradually tends to 0 in the learning process. Here we make a strict definition of our self-paced regularization function $\mathbf{g}(\mathbf{v},\lambda)$.

For any component function of $\mathbf{g}(\mathbf{v},\lambda)$, the $g(v_i,\lambda)$ satisfies the following two points:

① $g(v_i,\lambda)$ related to its variables v_i which satisfies $\forall v_i^1,v_i^2\in[0,1]$

$$q\cdot g(v_i^1,\lambda)+(1-q)\cdot g(v_i^2,\lambda)\geq g(qv_i^1+(1-q)v_i^2)\,q\in[0,1] \quad (3)$$

② The variable v_i of $g(v_i,\lambda)$ is a function of the mapping loss l_i of user samples and the age λ of the detection model.

$$v_i(l_i,\lambda)=\arg\min_{v_i\in[0,1]}(v_i l_i+\varphi(v_i,\lambda)) \quad (4)$$

The selection weight of training samples v_i is monotonically decreasing about l_i and monotonically increasing about λ, and satisfy the following two formulas.

$$\lim_{l_i\to 0}v_i(l_i,\lambda)=1\ \lim_{l_i\to+\infty}v_i(l_i,\lambda)=0 \quad (5)$$

$$\lim_{\lambda\to 0}v_i(l_i,\lambda)=0\ \lim_{\lambda\to+\infty}v_i(l_i,\lambda)=1 \quad (6)$$

The solution of our self-paced regularization and selection weight of user samples is shown as follows.

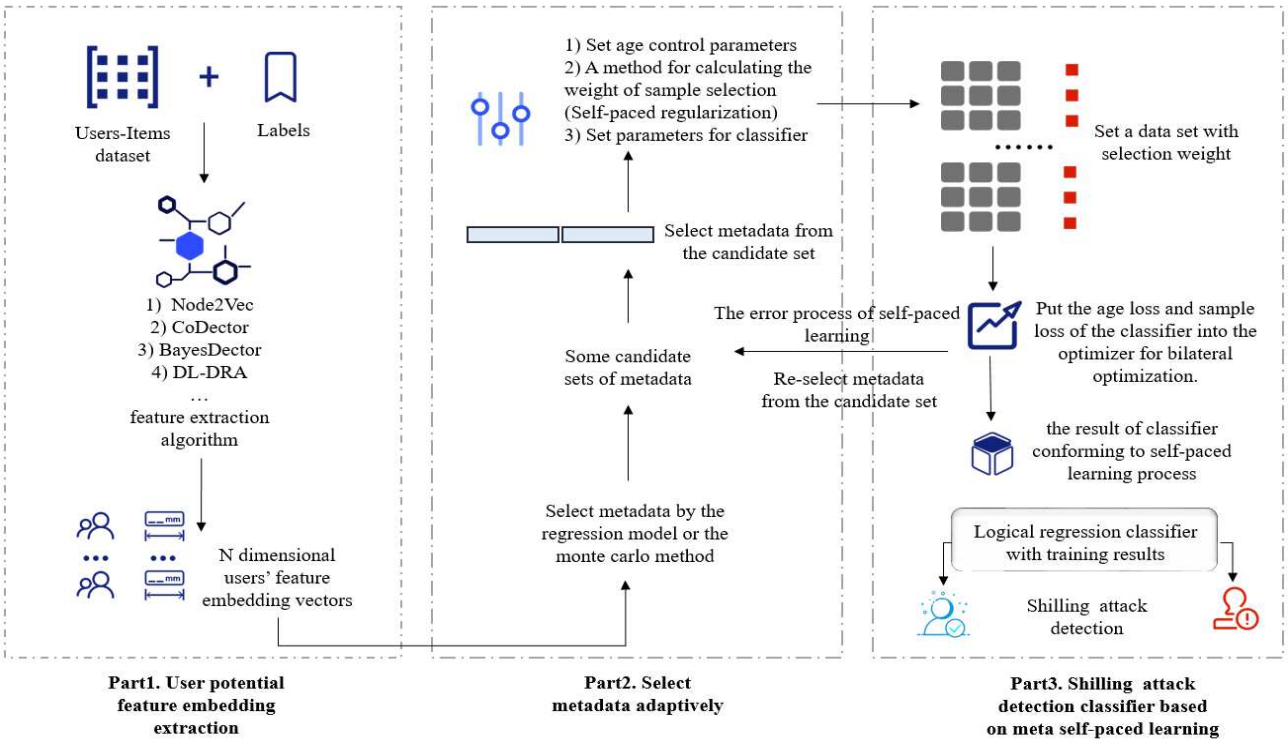

Fig. 1. The structure of MSPLD (shilling attack detection model for recommendation systems based on meta self-paced learning).

$$\varphi(v,\lambda)=\lambda\left(\frac{1}{2}v^2-v\right)\quad v(l,\lambda)=\begin{cases}-\dfrac{l}{\lambda}+1, & l<\lambda\\ 0, & l\geq\lambda\end{cases} \tag{7}$$

2) Training algorithm of shilling attack detection classifier based on meta self-paced learning

Firstly, select a little sample of user data as metadata

$$D_{e-data}=\left(\mathbf{X}(i_k),\mathbf{y}(i_k)\right). \tag{8}$$

The *Sigmoid* function is selected as the potential feature embedding prediction

$$f_{\mathbf{w}}(\mathbf{x})=\phi(\mathbf{xw})=\frac{1}{1+e^{-\mathbf{xw}}}. \tag{9}$$

The self-pace regularization is

$$\varphi(v,\lambda)=\lambda\left(\frac{1}{2}v^2-v\right). \tag{10}$$

and the selection weight of user samples is

$$v(l,\lambda)=\begin{cases}-\dfrac{l}{\lambda}+1, & l<\lambda\\ 0, & l\geq\lambda\end{cases}. \tag{11}$$

In these function, it satisfies $\Lambda=\lambda$.

According to the function above, the optimized objective function is

$$\lambda=\arg\min_{\lambda}\left\|\mathbf{f}_{\mathbf{w}}\left(\mathbf{X}(i_k)\right)-\mathbf{y}(i_k)\right\|_2, \tag{12}$$

$$\begin{aligned}(\mathbf{w},\mathbf{v})&=\arg\min\left(\mathbf{v}\cdot\left\|\mathbf{f}_{\mathbf{w}}(\mathbf{X})-\mathbf{y}\right\|_2+\mathbf{g}(\mathbf{v},\lambda)\right)\\&=\arg\min\left(\mathbf{v}\cdot\sqrt{\sum_{i=1}^{m}\left(\frac{1}{1+e^{-\mathbf{x}_i\mathbf{w}}}-y_i\right)^2}+\mathbf{g}(\mathbf{v},\lambda)\right),\end{aligned} \tag{13}$$

Then the problem is abstracted into a bilateral optimization problem. Gradient descent algorithm is used to solve $\mathbf{w}$, $\mathbf{v}$, λ in the above objective functions.

Step1. Establish the virtual presentation of the parameters of the prediction $\hat{\mathbf{w}}$.

$$\hat{\mathbf{w}}^{(t)}=\mathbf{w}^{(t-1)}-\alpha\cdot\nabla_{\mathbf{w}}\mathbf{v}\sqrt{\sum_{i=1}^{m}\left(\frac{1}{1+e^{-\mathbf{x}_i\mathbf{w}}}-y_i\right)^2}. \tag{14}$$

Update the age λ of the detection model：

$$\lambda^{(t)}=\lambda^{(t-1)}-\beta\frac{d}{d\lambda}\sqrt{\sum_{i=1}^{m}\left(\frac{1}{1+e^{-\mathbf{x}_{i_k}\mathbf{w}}}-y_{i_k}\right)^2}\Bigg|_{\lambda^{(t-1)}}. \tag{15}$$

Step2. Solve selection weight of user samples **v** based on the $\mathbf{w}^{(t-1)}$ in last step and the $\lambda^{(t)}$ updated.

$$\mathbf{v}^{(t)} = \arg\min_{\mathbf{v}\in[0,1]^m} \mathbf{v}\cdot\sqrt{\sum_{i=1}^{m}\left(\frac{1}{1+e^{-\mathbf{x}_i\mathbf{w}^{(t-1)}}}-y_i\right)^2} + \mathbf{g}\left(\mathbf{v},\lambda^{(t)}\right) \quad (16)$$

Step3. Use gradient descent algorithm to solve the real parameters of the prediction $\mathbf{w}^{(t)}$ based on **v** updated.

$$\mathbf{w}^{(t)} = \mathbf{w}^{(t-1)} - \alpha\cdot\nabla_{\mathbf{w}}\mathbf{v}^{(t)}\sqrt{\sum_{i=1}^{m}\left(\frac{1}{1+e^{-\mathbf{x}_i\mathbf{w}}}-y_i\right)^2}\Bigg|_{\mathbf{w}^{(t-1)}} \quad (17)$$

Finally, apply the parameters **w** into the prediction of the generalized sample. In the experimental design and result analysis after this section, we will continue to discuss the improvement of the shilling attack detection classifier based on meta self-paced earning by combining different algorithms.

Algorithm: The process of shilling attack detection system based on meta self-paced learning

Input: A dataset containing malicious users $\mathbf{X} = (\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_m)'$, $\mathbf{y} = (y_1, y_2, \cdots, y_m)'$, metadataset $D_{e-data} = (\mathbf{X}(i_k), \mathbf{y}(i_k))$ The ending conditions for training program.

Output: Parameters of the Shilling attack detection classifier based on Meta Self-paced Learning **w**.

1: Initialize $\mathbf{w}^0, v^0, \Lambda^0$
2: While the ending conditions is not satisfied
3: iteration+=1
4: solve the equation (12)(13)(14) by order
5: if reach the maximum number of iterations or satisfy other ending conditions: break

IV. EXPERIMENS AND RESULT ANALYSIS

In this section, we will introduce the experimental results on two public datasets. The results show the metricize improvement of the MSPLD model, which is analyzed by comparing the state-of-art model. Then we illustrate the self-paced training process by visual analysis. It can be proved that the training process conforms to the self-paced learning process.

A. Datasets

In this paper, the shilling attack detection experiments were conducted on the Amazon [15] and FilmTrust [16] datasets. The Amazon contains 5,055 users, 16,885 items, and 51,346 ratings, respectively. There are 3,118 legitimate users and 1,937 malicious users in it. The number of legitimate and malicious users in Amazon is usually fixed. To verify the performance of the detection algorithm under different attack modes, the FilmTrust is used, which contains 1,508 users, 4,032 items, and 52,308 ratings, respectively. The FilmTrust only contains datasets of legitimate users. Following the experiments for other detection models [18][19], we utilize the random attack and average attack models to inject 10% of malicious users. The statistics for the datasets are shown in Table II.

TABLE II THE STATISTICS OF DATASETS

	Amazon	FilmTrust
The number of legitimate users	3,118	1,508
The number of malicious users	1,937	150
The proportion of malicious users	38.32%	10%(0.1attacksize)
The number of items	16,885	4,032
The number of ratings	51,346	52,308

B. Combining algorithm and evaluation

We selected several combining algorithms such as CoDetector, Node2Vec, and DL-DRA to compare and analyze the results. CoDetector factorizes the user-rating item rating matrix and user-user interaction matrix to obtain the embedding characteristics of different users. Node2vec uses the construction of user-item-user complex network architecture diagram, then it uses the random walk method to extract the potential feature embedding of different users from the network diagram. DL-DRA algorithm uses the interpolation method to resize the rating matrix and then builds a deep learning network based on CNN for detection.

C. Result analysis and discussion

We randomly selected 80% data as the training set and the left as the test set. The shilling attack detection classifier, which is based on the meta self-paced learning, needs to select the appropriate hyperparameter, e.g., 1) random range of initial age, 2) whether to perform normalization, 3) metadata selection strategy, and 4) the type of optimizer) by different users' potential embeddings extracted from different algorithms. For Amazon, we will select the hyperparameter as Table III. Because the FilmTrust is our own injected dataset, there is no standard hyperparameter selection. It is necessary to select the hyperparameter according to the attacking model and the actual injected data.

TABLE III. HYPERPARAMETER SELECTION OF AMAZON

Algorithm	Random range of initial age	Normalization	Metadata selection strategy	Optimizer type
Node2Vec	0.6-0.8	No	Logistic regression	AdagradOptimizer
CoDetector	0.6-0.8	Yes	Logistic regression	AdagradOptimizer
0.6-0.8	0.005-0.01	Yes	Logistic regression	AdamOptimizer

Shilling attack detection classifier, which is based on the meta self-paced learning, shows different improving efficiency values for different feature extraction algorithms. Then, we will combine these algorithms to get the performance on the two datasets to show the improvement of our shilling attack detection based on meta self-paced learning. In addition, the learning process of the model is visualized to enhance the theoretical reliability of the training process.

1) The performance of shilling attack detection classifier based on meta self-paced learning combined with different algorithms on Amazon.

As the CoDetector is the traditional matrix factorization algorithm, the extracted feature embeddings are too difficult for regression classifiers to process. The accuracy of classification is not good. Therefore, compared with other algorithms, the CoDetector has a relatively poor extraction on the user's potential feature embedding vectors. Thus, the sample embeddings are complexing and the traditional simple classifiers are often difficult to achieve accurate classification. Using the shilling attack detection classifier based on meta self-paced learning can select relatively easy and appropriate classified samples to adapt the model towards the right training direction (the right model parameters change process) in the early training process. This method can achieve low classification efficiency and accuracy because of the complexity of the sample itself.

We run our model ten times independently and put the same embedding into logistic regression classifier and shilling attack detection classifier based on Meta Self-paced Learning respectively to get the results as shown in Table IV.

TABLE IV. THE RESULTS ON AMAZON

Algorithm	Evaluation	P	R	F1-score
CoDectector	Non-SPL	0.6497	0.6411	0.6427
	SPL	0.7799	0.7730	0.7756
	Improve	20.04%	20.57%	20.67%
Node2Vec	Non-SPL	0.8863	0.8873	0.8866
	SPL	0.8944	0.9049	0.8981
	Improve	0.92%	1.98%	1.29%
DL-DRA	Non-SPL	0.9118	0.9223	0.9189
	SPL	0.9225	0.9198	0.9167
	Improve	-1.16%	0.27%	0.24%

It can be found easily when facing the complex user potential features embeddings extracted by CoDetector, the performance of the traditional logistic regression classifier is poor. However, after a completed self-paced learning process, it can be obviously found that the evaluation metrics have improved a lot. The evaluation metrics P, R and F1-measure of Node2Vec are better than those of CoDetector. However, using the self-paced learning method can still improve it to be better. That indicates our shilling attack detection classifier still has a good performance for the models that can achieve high accuracy.

Combining the deep learning algorithm DL-DRA, we set the output variables of the hidden layer in the full connection layer as the input data of the self-paced classifier. Compared with the deep learning algorithm, it can be found that the self-paced learning method can also improve its detection performance.

2) The performance of shilling attack detection classifier based on meta self-paced learning combined with different algorithm on filmtrust (injected).

Because the improvement of the self-spaced learning model combining with an excellent feature extraction algorithm is limited, we select the CoDetector algorithm which has great improvement to show the results on the Filmtrust dataset. Average attack and random attack are selected as the attack modes. The results are shown in Table V.

TABLE V. THE PERFORMANCE OF CODECTECTOR + SHILLING ATTACK DETECTION CLASSIFIER BASED ON META SELF - PACED LEARNING WHEN FACING DIFFERENT ATTACK SIZES

	Average attack			**random attack**		
attack sizes	***Non -SPL***	***SPL***	***rising rate***	***Non -SPL***	***SPL***	***rising rate***
0.1	0.9130	0.9526	4.34%	0.9062	0.9641	6.39%
0.2	0.8163	0.9445	15.71%	0.8399	0.9497	13.07%
0.3	0.7150	0.9323	30.39%	0.7530	0.9400	24.83%

Combining with other algorithms, we run 10 times on the Filmtrust with the attack size of 0.3 using the average attack injection model. The results are shown in Table VI.

TABLE VI. THE RESULT OF FILMTRUST

Algorithm	Evaluation	P	R	F1-score
CoDectector	Non-SPL	0.3552	0.4967	0.4142
	SPL	0.9175	0.9597	0.9340
	Improve	158.27%	93.23%	125.50%
DL-DRA	Non-SPL	0.9916	0.9963	0.9938
	SPL	0.9926	0.9968	0.9946
	Improve	0.10%	0.04%	0.08%
Node2Vec	Non-SPL	0.9943	0.9947	0.9951
	SPL	0.9932	0.9853	0.9853
	Improve	-0.11%	-0.94%	-0.98%

Because the injected data has certain features, the detection of the better algorithms for feature embedding extraction is good enough. For instance, the results of DL-DRA and Node2Vec combining the common classifier are good or even close to 100%. Due to this, the effect of using the shilling attack detection classifier based on meta self-paced learning will not be better.

D. Analysis of the detection model's learning process

On the Amazon dataset, we selected the learning process of CoDetector (because of the greatest improvement) and Node2vec (because of its high accuracy) for visualization and discussion. To justify our learning process, we give the following definition.

Definition 1. The two-dimensional width of the data selection

Assuming that the original ten-dimensional dataset obtained by t-SNE has a plane point set with two-dimensional coordinates as A, The following defines the measure of A:

Let Γ_n be a smooth convex closed curve family on the plane , D_{Γ_n} is a single connected region bounded by curve Γ_n and satisfied.

1) $\forall\ a \in A \Rightarrow a \in D_{\Gamma_n}$, $n = 1, 2, \cdots$

2) $D_{\Gamma_1} \supset D_{\Gamma_2} \supset \cdots \supset D_{\Gamma_n} \supset \cdots$

From the choice axiom and *zorn's* lemma, $\inf\left\{D_{\Gamma_n}\right\}_{n=1}^{\infty}$ exists, we note.

$$m\left(D_{\Gamma}\right)=\inf\left\{D_{\Gamma_n}\right\}_{n=1}^{\infty} \quad \Gamma=\lim_{n\to\infty}\Gamma_n \tag{18}$$

Then, $m\left(D_{\Gamma}\right)$ is the measure of A. We note the data selected by self-paced learning in the i-th iteration as A_i, where $A=\lim_{n\to\infty}A_n$, and note $m\left(D_{\Gamma_i}\right)$ as the measure of A_i.

Definition 2. Ratio of legitimate and malicious users

The parameter δ_i denotes the ratio of legitimate and malicious users in the data selection in the i iteration of self-learning and δ_∞ denotes as the ratio of global legitimate and malicious users. We visualize the weight of sample selection in the training process of the MSPLD in the Fig. 2 and Fig. 3.

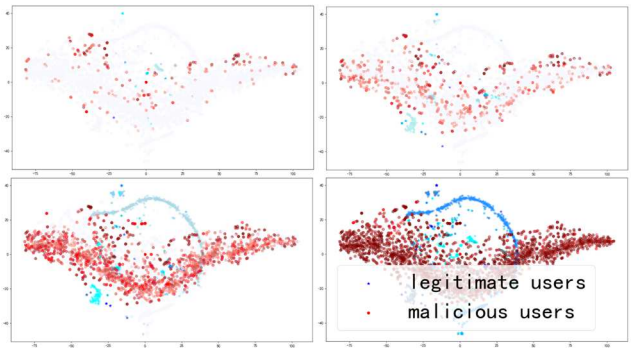

Fig. 2. The weight of sample selection changes by using CoDetector+ shilling attack detection based on meta self-paced learning

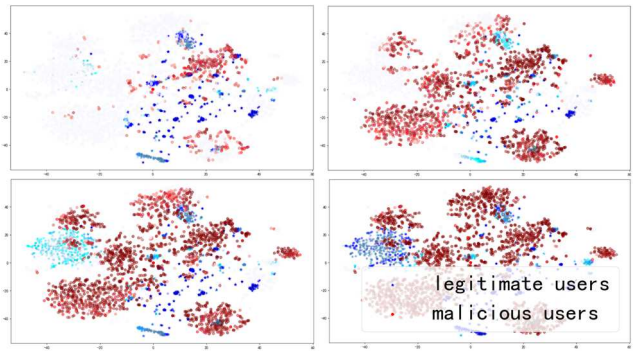

Fig. 3. The weight of sample selection changes by using Node2Vec+ shilling attack detection based on meta self-paced learning

From the experimental figures above, we can draw the following conclusions.

1) At the beginning of learning process, the two curves are almost the same:

$$m\left(D_{\Gamma_1}\right)=m\left(D_{\Gamma_\infty}\right). \tag{19}$$

It indicates that the model selects the users' samples widely and globally at the beginning of the learning process, which can ensure that the data is always chosen towards the global optimal solution possibly rather than falling into the quagmire of the local optimal solution. It reflects the robustness and repeatability of the model.

2) It can be seen in the Fig. 4 and Fig. 5: The Firstly selected data that can be distinguished the legitimate user as the initial selection data in the process of data selection. it will make the age increased quickly at the beginning. However, when the ratio of legitimate and malicious users achieves the global critical value, the learning difficulty increases, malicious users are gradually increasing the proportion of sample data. the result is almost in conformity with selecting training samples of

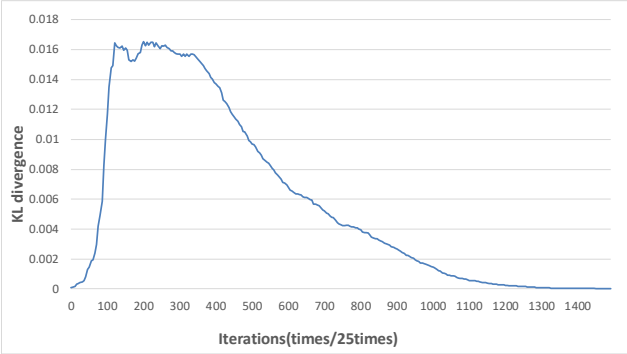

Fig. 4. The KL divergence of Node2Vec+shilling attack detection based on meta self-paced learning

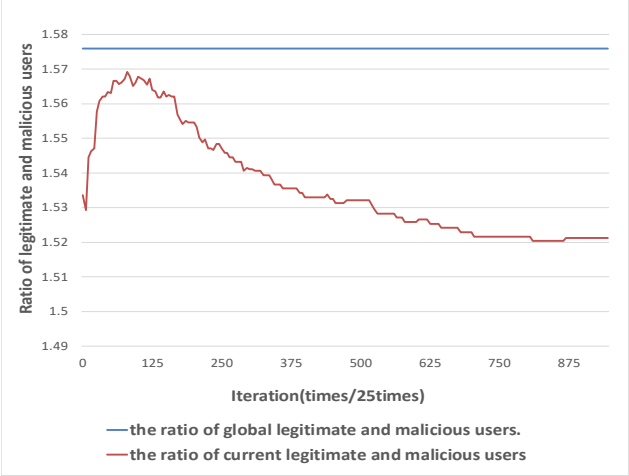

Fig. 5. Ratio of legitimate and malicious users of Node2Vec+ shilling attack detection based on meta self-paced learning

difficulty from easy to difficult in the self-paced learning process.

3) In conclusion, we also calculate the KL divergence and ratio of legitimate and malicious users for further demonstration, as shown in Fig. 4. At the beginning of the learning process, the data selection is less, and the KL divergence value is low. It indicates that the distribution of predictive value and the distribution of the label is quite close. As the growth of age, the

selections of the samples are also increasing. However, for the bilateral optimization model of the classifier, the optimization is too slow to change, which leads to the KL divergence values rebounded. In the end, the samples have been gradually selecting into optimizer. Therefore, the KL divergence is gradually reducing. The result is consistent with our second point in describing learning difficulty through the ratio of legitimate and malicious users above, which indicates that our assumption is reasonable. The samples selected by the model are from easy to difficult, which gradually form the final training results.

V. CONCLUSION

In this paper, we propose a shilling attack detection model based on meta self-paced learning to mitigate the impact of malicious users on the recommendations. Firstly, we use the existing algorithms to extract the users' potential feature embeddings. Then some regression models or Monte Carlo methods are used to select the metadata adaptively. Finally, the shilling attack detection model based on the meta self-paced learning is used to detect malicious users. Experimental results on two datasets show that our model has better performance with various embeddings extracted by different algorithms than other models. Especially, the model improves the performance a lot when facing the complex samples with weak feature extraction. We also explain the processing of our self-paced learning process, and further demonstrate the theoretical reliability of the model.

ACKNOWLEDGEMENT

This research is supported by the National Key Research and Development Program of China (2018YFB1403602), the Technological Innovation and Application Program of Chongqing (cstc2019jscx-mbdxX0008), the Natural Science Foundation of Chongqing, China (cstc2020jcyj-msxmX0690), the Fundamental Research Funds for the Central Universities of Chongqing University (2020CDJ-LHZZ-039), and the Overseas Returnees Innovation and Entrepreneurship Support Program of Chongqing (cx2020097).

REFERENCES

[1] Gao M, Zhang J W, Yu J L, Li J, Wen J H, and Xiong Q Y. Recommender systems based on generative shilling networks: A problem-driven perspective[J]. Information Sciences, 2021, 546(6): 1166-1185.

[2] Min Gao, Kecheng Liu, and Zhongfu Wu. "Personalisation in web computing and informatics: Theories, techniques, applications, and future research."[J] Information Systems Frontiers 12, no. 5 (2010): 607-629.

[3] Chen K K, Patrick P. K. Chan, F Zhang, and Q Li. Shilling attack based on item popularity and rated item correlation against collaborative filtering[J]. International Journal of Machine Learning and Cybernetics 2019, 10(7):1833–1845.

[4] Mehta B, Nejdl W. Unsupervised strategies for shilling detection and robust collaborative filtering[J]. User Modeling and User-Adapted Interaction, 2009, 19(1-2):65-97.

[5] Tan K, Gao M, Li W T, Tian R L, Wen J H, Xiong Q Y. Two-layer sampling active learning algorithm for social spammer detection. Acta Automatica Sinica[J]. 2017, 43(3): 448−461.

[6] Dou T, Yu J L, Xiong Q Y, Gao M, and Fang Q Q. Collaborative shilling detection bridging factorization and user embedding[J]. EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2017,13, 459-469.

[7] Williams C A, Research Advisor, Mobasher B. Thesis: Profile Injection Attack Detection for Securing Collaborative Recommender Systems[J]. Service Oriented Computing & Applications, 2012, 1(3):157-170.

[8] SHU J, MENG D Y and XU Z B Meta self-paced learning[J]. SCIENTIA SINICA Informationis. 2020, 50(6): 781–793.

[9] Aditya Grover and Jure Leskovec. Node2vec: Scalable feature learning for networks[C].//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, USA, August 13-17, ACM, 2016, 855–864.

[10] Zhou Q Q, Wu J X and Duan L L. Recommendation attack detection based on deep learning[J]. Information Security and Applications, 2020, 52:102493

[11] Yang F, Gao M , Yu J L, Song Y Q and Wang X Y. Detection of shilling attack based on bayesian model and user embedding[C]. //In IEEE International Conference on Tools with Artificial Intelligence 2018, 639-646.

[12] Zhou Q Q, Wu J X and Duan L L. Recommendation attack detection based on deep learning[J]. Information Security and Applications, 2020, 52:102493.

[13] Wu Z, Jie C, Bo M, Wang Y. Semi-SAD: applying semi-supervised learning to shilling attack detection[C]. //Proceedings of the 2011 ACM Conference on Recommender Systems, RecSys 2011, Chicago, IL, USA, October 23-27, 2011, 289-292.

[14] Zhang D W, Meng D Y, Zhao L and Han J W. Bridging Saliency Detection to Weakly Supervised Object Detection Based on Self-paced Curriculum Learning[C]. //Proceedings of International Joint Conference on Artificial Intelligence (IJCAI), 2016, 3538-3544.

[15] Xu C, Zhang Jie, Chang K, and Long C. Uncovering collusive spammers in chinese review websites[C]. //In 22nd ACM International Conference on Information and Knowledge Management, CIKM'13, San Francisco, CA, USA, October 27 - November 1, 2013, 979–988.

[16] https://www.librec.net/datasets.html

[17] Guo G, Zhang J, Yorke-Smith N. A novel bayesian similarity measure for recommender systems[C].//Twenty-Third International Joint Conference on Artificial Intelligence, 2013, 2619–2625.

[18] Li W., Gao M., Zeng J., Xiong Q., Hirokawa S., Shilling attack detection in recommender systems via selecting patterns analysis[J]. IEICE TRANSACTIONS on Information and Systems 99, 2016, 2600-2611.

[19] Lin C., Chen S., Li H., Xiao Y., Li L., Yang Q., Attacking recommender systems with augmented user profiles[J]. arXiv preprint arXiv, 2005, 08164