Account Takeover Detection on E-Commerce Platforms

Conference Paper · June 2022

DOI: 10.1109/SMARTCOMP55677.2022.00052

1 author:

Min Gao
Fudan University
11 PUBLICATIONS **12** CITATIONS

Account Takeover Detection on E-Commerce Platforms

Min Gao
School of Computer Science, Fudan University, Shanghai, China
mgao21@m.fudan.edu.cn

2022 IEEE International Conference on Smart Computing (SMARTCOMP) | 978-1-6654-8152-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/SMARTCOMP55677.2022.00052

***Abstract*—Account takeover is a type of malicious attack where a fraudster steals accounts and passwords from normal users, causing the loss of money and the exposure of personal information. Existing solutions either rely on extensive manual labeling, or require behavior sequences and context graphs of accounts. In this paper, I propose a Siamese neural Network-based Multi-Relation Graph Embedding method (MRGE-SiameseNet) to detect stolen accounts. The key idea of MRGE-SiameseNet is that the two inputs from the same users are similar. I adopt the idea of the siamese neural network to judge whether two different inputs are from the same user. To get a powerful representation of each account, I integrate several embeddings of multiple relationships of accounts and profile feature embedding for each account with multi-head attention mechanism. The fully connected module is employed to obtain the similarity score, which can be utilized to identify whether the account is stolen by account takeover.**

***Index Terms*—Fraud Detection, Account Takeover, Siamese Neural Network, Graph Embedding**

I. Background and Motivation

Account takeover (ATO) [1] is a type of malicious attack where a fraudster illegally obtains login and usage to normal accounts. This attack type results in leakage of personal information and loss of money for users, and also causes damage to the platform's revenue and reputation. Such attack has threatened several areas, such as financial services, online retail and social media. A report from Security.org Team found that 24 million households (22%) of U.S. adults have experienced account takeovers, and the average value of financial losses caused by account takeovers is up to 12,000 dollars in 2021. [1]

However, most of the existing efforts are rarely focused on the task of ATO, they are mostly devoted to other related tasks such as sybil detection [2], fraud detection [3], etc. Some feature-based methods utilize handcraft statistical features from behavior sequences of accounts. Statistical features can significantly distinguish most malicious accounts from normal ones [3]. Some recurrent neural network-based methods [5] are presented to address this problem. Tao et al. [5] adopted the attention mechanism and LSTM to solve the task of account takeover. Graph neural network-based methods [4] have also been proposed to characterize normal and malicious accounts based on user interactions. However, these methods have several limitations. First, they require extensive manually labeled data for training. While manually labeling is laborious and costly. Second, they cannot capture new fraud patterns and behavioral characteristics, which requires domain experts to periodically re-filter statistical characteristics and retrain the model. Third, they rely on relatively long-term behavioral sequences and contextual information about the accounts, which gives malicious actors ample time to conduct fraudulent activities.

In this work, I provide a new perspective to solve the problem of account takeover detection. Intuitively, the historical behaviors and habits of the same user are similar and stable. Thus, the problem of account takeover detection can be transformed into the calculation of the similarity score of different data of the same account. This intuition fits well with the idea of the siamese neural network [6]. With the same parameters and weights, siamese neural networks have at least two subnetworks to enable the ranking of inputs and learning a similarity function, which can be used to identify similarities between inputs. It was first introduced for the problem of signature verification [6]. Meituan [7], one of the largest Online-to-Offline e-commerce platforms in China, has also faced the risk of account takeover. To counter this threat, I employ the idea of siamese neural network to detect the stolen accounts. The key contributions of this paper include a new interpretation for the problem of account takeover detection, and a new method named MRGE-SiameseNet, which adopts the architecture of siamese neural network to detect stolen accounts caused by account takeover.

II. MRGE-SiameseNet Architecture

In this section, I propose a MRGE-SiameseNet model to detect the stolen accounts caused by account takeover. For each account, there are two inputs. I aim to determine whether two inputs of the same account are generated by the same user. The higher similarity score between two inputs is, the more likely the account is stolen. Within each input, I construct several different types of relationships and extract some profile features of the account. In MRGE-SiameseNet, two subnetworks are utilized to characterize two inputs from the same account. For each subnetwork, there are four dedicated modules. Ego Graph Embedding Module, Bipartitie Graph Embedding Module, and Profile Feature Embedding Module are designed to enrich an input from different perspectives, respectively. The Multi-Head Attention Module is utilized

[1] https://www.security.org/digital-safety/account-takeover-annual-report/

2693-8340/22/$31.00 ©2022 IEEE
DOI 10.1109/SMARTCOMP55677.2022.00052

to merge the embeddings from different perspectives and generate a fused embedding for an input. Finally, the Fully Connected Module is utilized to compute a similarity score between two inputs from an account. With the similarity score, I can determine whether the account has been stolen. Figure 1 depicts the framework of MRGE-SiameseNet model.

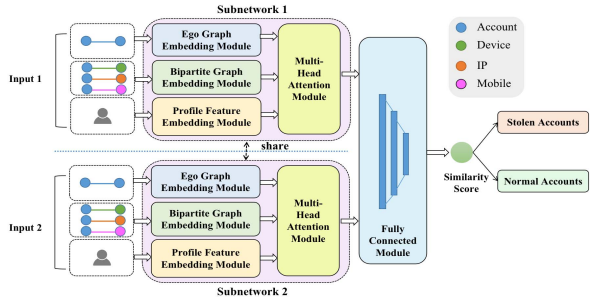

Fig. 1. The framework of MRGE-SiameseNet model.

Ego Graph Embedding Module Given the historical behavior data of an account, account-account relation is constructed if there is a sharing behavior or trading behavior between this account and another account. The ego graph embedding module is designed to capture the relations from the accounts within the ego of an account. For the ego account, I employ the message passing mechanism to get embedding of the ego account, as illustrated in

$$e_X^k = \sigma(W^k * CAT(e_X^{k-1}, AGG(e_u^{k-1}, u \in N_X))), \quad (1)$$

where W^k is the weight matrix in the layer k, CAT and AGG are concat function and aggregate function, respectively. N_X is the optimized neighbor set of account X. $e_X^{(k-1)}$ and e_X^k are the embedding of account X in the layer $k-1$ and k, respectively.

Bipartite Graph Embedding Module. Given the historical behavior data of an account, account-device/IP address/mobile phone number relation is constructed if there is a connection between this account and a(an) device/IP address/mobile phone number. The bipartite graph embedding module is constructed to extract several types of relations. Here I utilize the LightGCN model to get embeddings of the account with different relationships.

$$b_X^k = \sigma(CAT(b_X^{k-1}, AGG(b_u^{k-1}, u \in N_X))), \quad (2)$$

where CAT and AGG are the concat function and aggregate function, respectively. N_X is the optimized neighbor set of account v. $e_X^{(k-1)}$ and e_X^k are the embedding of account X in the layer $k-1$ and k, respectively.

Profile Feature Embedding Module. Given an account, this module takes the fully-connected networks to present profile features of the account.

$$p_X = ReLU(FCL(ReLU(FCL(p_X)))), \quad (3)$$

where $ReLU$ and FCL refer to the relu activation function and a fully connected layer, respectively, and p_X is the initial representation of the profile features of account X.

Multi-Head Attention Module. To get a complete embedding of one input of the account, I employ multi-head attention module to effectively integrate several embeddings within one input.

$$m_X = CAT(ATT_i(Q * W^Q, K * W^K, V * W^V), W', i \in N_{\text{head}}), \quad (4)$$

where CAT, ATT, and N_{head} are the concat function, attention function, and the number of heads, respectively. W^Q, W^K, W^V, and W' are the corresponding weight matrices, respectively.

Fully Connected Module. Here a fully connected module to utilized to compute the similarity score of two inputs of the same account. If the similarity score is close to 0, the probability of the two inputs from two different users is higher, and the account is stolen. Conversely, if the similarity score is close to 1, the probability of the two inputs from the same user is higher, and the account is normal.

$$sim(X_1, X_2) = ReLU(FCL(ReLU(FCL(CAT(m_{X_1}, m_{X_2}))))), \quad (5)$$

where $ReLU$ and FCL refer the relu activation function and the function within a fully connected layer, respectively, and m_{X_1} and m_{X_2} are the fused embedding of account X_1 and X_2, respectively.

Loss Function. The loss function consists of the cross-entropy loss and the regularization term, as expressed as follows.

$$L(X_1, X_2) = \min_\theta -(y * log(D_\theta(X_1, X_2)) + (1 - y(X_1, X_2)) * log(1 - D_\theta(X_1, X_2))) + \|X\|_2 . \quad (6)$$

III. Conclusion and Future Work

In this paper, I propose a siamese neural network-based multi-relation graph embedding method (MRGE-SiameseNet) to solve the problem of account takeover detection. The MRGE-SiameseNet model identifies whether an account is stolen by learning the similarity score of two inputs of the same account.

In the future, I plan to construct multiple graphs and extract some profile features of each account. The MRGE-SiameseNet model will be constructed according to the proposed method. The dataset provided by Meituan will be utilized as our dataset. I will preprocess the data of accounts, and divide them into training set and test set, followed by the verification of the effectiveness of the method on the test set. Furthermore, I aim to deploy the proposed model on Meituan to detect stolen accounts earlier. Moreover, I look forward to expanding the idea of the proposed model to other problems of fraud detection.

References

[1] P. Doerfler, K. Thomas, M. Marincenko, et al. Evaluating login challenges as a defense against account takeover, Proc. of WWW, 2019.
[2] A. Breuer, R. Eilat, U. Weinsberg. Friend or faux: graph-based early detection of fake accounts on social networks, Proc. of WWW, 2020.
[3] Z. Xia, C. Liu, N. Z. Gong, et al. Characterizing and detecting malicious accounts in privacy-centric mobile social networks: A case study, Proc. of ACM KDD, 2019.
[4] D. Wang, J. Lin, P. Cui, et al. A semi-supervised graph attentive network for financial fraud detection, Proc. of IEEE ICDM, 2019.
[5] J. Tao, H. Wang, T. Xiong. Selective graph attention networks for account takeover detection, Proc. of IEEE ICDMW, 2018.
[6] J. Bromley, I. Guyon, Y. LeCun, et al. Signature verification using a "siamese" time delay neural network, Proc. of NeurIPS, 1993, 6.
[7] Q. Ye, Y. Gao, Z. Zhang, et al. Modeling Access Environment and Behavior Sequence for Financial Identity Theft Detection in E-Commerce Services, Proc. of IJCNN, 2022.