Phishing short URL detection based on link jumping on social networks

Bailin Xie*, *Qi* Li, and *Na* Wei

School of Information Science and Technology, Guangdong University of Foreign Studies, Guangzhou, China

Abstract. Nowadays, a large number of people frequently use social networks. Social networks have become important platforms for people to publish and obtain information. However, social networks have also become the main venue for hackers to initiate online fraud. Phishing is a common way used by hackers to launch online fraud on social networks. This paper proposes a method for detecting phishing short URL based on the link jumping. The method uses a hierarchical hidden Markov model with two-layer structure to describe the link jumping process after user clicking on short URL, so as to identify phishing short URL on social networks. The proposed method includes a training phase and an identification phase. In the identification phase, the average log-likelihood probability of the observation sequence is calculated. An experiment based on real datasets of Weibo is conducted to evaluate this method. The experiment results validate the effectiveness of this method.

Keywords: Social networks, Phishing, Short URL, Hierarchical hidden Markov model.

1 Introduction

With the development of network defense techniques, it becomes more and more difficult for hackers to break through the security defense systems only relying on technical means. Under this background, a large number of hackers began to use Internet fraud to obtain benefits, resulting in a rapid increase in Internet fraud. Internet fraud is very harmful. Even the most vigilant and cautious users will suffer from clever Internet fraud [1]. Currently, social networks are developing rapidly, and a large number of people frequently use social networks. Most of these users have a relatively low degree of mastery of network security knowledge, and their awareness of network security is weak. Moreover, hackers can easily obtain the personal information of users from social networks. Therefore, social networks have become the main venue for hackers to launch online fraud.

Phishing is a common way used by hackers to initiate online fraud. For instance, the "2016 Internet Fraud Trend Research Report" released by 360 Company shows that their hunting network platform received 20,623 Internet frauds submitted by users in China [2]. These frauds involved 195 million Yuan, of which 110 million Yuan was involved by

* Corresponding author: bailinxie@gdufs.edu.cn

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

phishing. Therefore, the research on phishing detection is important. This paper proposes a detection method for phishing URL based on the link jumping. The method adopts a hierarchical hidden Markov model with a two-layer structure to describe the link jumping process after user clicking on short URL for identifying phishing short URL on social networks.

The remainder of the paper is organized as follows. Section 2 reviews recent studies on phishing short URL detection. In section 3, we introduce the principle of phishing short link detection. Experimental results are given in section 4. Finally, we conclude the paper in section 5.

2 Related works

In the aspect of phishing URL detection on social networks, Aggarwal *et al*. [3] choose URL-based features, WHOIS-based features, blog post-based features, network-based features, and then use the random forest classification algorithm to detect phishing URL on Twitter. In this method, the URL-based features include: URL length, the number of "." in the URL, etc; the WHOIS-based features include: the domain name registered by the user and the time when the domain name was registered, etc; the blog post-based features include: the label in the blog post, the number of blog posts, the length of the blog post, the number of times the blog post was replied, etc; the network-based features include: the number of followers, the number of friends, the number of blog posts published by the user, etc. Manju *et al*. [4] choose the location of the URL in the blog post, the length of the redirected URL, the number of different accounts sending the same URL link, the user account registration time, and then adopt classification algorithms to identify phishing URL on Twitter. Gupta *et al*. [5] choose the characteristics of link creation time, domain name creation time, user type who generated short links, and then use the random forest classification algorithm to identify phishing URL on Twitter. Wang *et al*. [6] propose to detect spam links on Twitter based on a classifier. The features include: the number of times users click links, the number of users who click links from different countries, and the number of referers. Spoorthi *et al*. [7] propose to detect suspicious links based on the SVM classification algorithm using features such as the time the blog post is published, the language used by the user, and the Twitter client. Nepali *et al*. [8] choose the length of the blog post, the number of URLs in the blog post, the number of times the blog post is replied, the number of followers, the number of friends of the user, and then use classification algorithms to identify malicious links on Twitter.

Cao *et al*. [9] present a method for detecting malicious links on Weibo. This method chooses URL-based features, forwarding-based features, graph-based features, and then use classification algorithms to detect malicious links on Weibo. The URL-based features include the length of the URL, etc.; the forwarding-based features include: the ratio of the number of times the blog post is forwarded to the number of times it is commented, and the friends who forward the malicious link in the proportion of all friends who forward the blog post, etc; the graph-based features include the ratio of the number of followers to the number of friends. Guan *et al*. [10] choose the characteristics of the number of URLs contained in the text information published by users on the wall post, the number of "-" in the URL, the registration time of the top-level domain name of the URL, and then use classification algorithms to identify malicious links on Facebook. In addition, Sahoo *et al*. [11] conduct a comparative analysis of some existing malicious URL detection methods based on machine learning algorithms, and point out the main challenges faced by existing research [14][15].

The above methods are mainly based on classification algorithms to detect phishing URL on social networks. These methods do not effectively consider the link jumping

process after users click on links. However, the jumping process of normal short link is different from that of phishing short link.

This paper adopts the hierarchical hidden Markov model (HHMM) [12] with a two-layer structure, to describe the link jumping process after a user clicks a normal short link, so as to detect phishing short links on social networks.

3 Phishing short URL detection

Currently, Twitter and Weibo use short URL links. When a user clicks a short URL link, the short URL link will be restored to a long URL link in the browser, that is, the link will jump. For example, when a user clicks the short URL link " http://t.cn/RUOXbuS " in a text message on Weibo as shown in Figure 1, the URL link will be restored to the long URL link " tv.cntv.cn/video/C10375/eb654c1bf 3f146ab85ed7e236070bf5e " in the browser. The jumping process of phishing short URL links is different from that of normal URL links. For example, after a user clicks some phishing short URL links, these links will jump multiple times in the browser, and the characters in the restored long URL links are arranged in the same order. When a user posts a short URL link on a social network such as Weibo, the content of the URL link is generally described in the first two sentences or the last two sentences of the link. In this work, the first two sentences of the short link, the short link, the last two sentences of the short link, and the characters in the link jumping process are used as observations. Then a special hierarchical hidden Markov model with a two-layer structure is used to describe the normal short link.

Figure 1 shows the hierarchical hidden Markov model of the link jumping process of a normal short link, where o_1, o_2,..., o_{106} are the observations, q_1^1, q_2^1 are the states of the first-layer hidden Markov model (HMM), and a_{12}^1 are the state transition probability of the first-layer hidden Markov model, the state transition of the first-layer hidden Markov model represents a jump from one link to another link. q_1^2, q_2^2, q_3^2, q_5^2, q_6^2, q_7^2, q_9^2, q_{i-1}^2, q_i^2, q_{j-1}^2, q_j^2 are the states of second-layer hidden Markov model, a_{12}^2, a_{23}^2, a_{55}^2, a_{65}^2, $a_{7(j-1)}^2$, $a_{(j-1)j}^2$, $a_{9(i-1)}^2$, $a_{(i-1)i}^2$ are the state transition probability of the second-layer hidden Markov model.

Hierarchical hidden Markov model is a structured multi-level stochastic process, which is an extension of hidden Markov model (HMM) [13]. In the hierarchical hidden Markov model, each high-level state corresponds to a low-level HMM model (ie, a sub-HMM model). Only when the low-level sub-HMM model enters the final state, the high-level state can jump. Hierarchical hidden Markov models have been applied in many research fields, such as speech recognition, text classification, network anomaly detection, etc. In this work, a hierarchical hidden Markov model with a two-layer structure is adopted to describe the link jumping process.

4 Experiments

4.1 Data set

In order to evaluate the proposed method, lots of normal short URLs and phishing short URLs are collected from Weibo. On Weibo, users can submit suspect phishing short URL reports based on the official services. If a short URL is verified to be a phishing, warning signs will be labeled on the post. Based on this, 1,078 verified phishing short URLs have been collected. In addition, 3,132 normal short URLs have been collected.

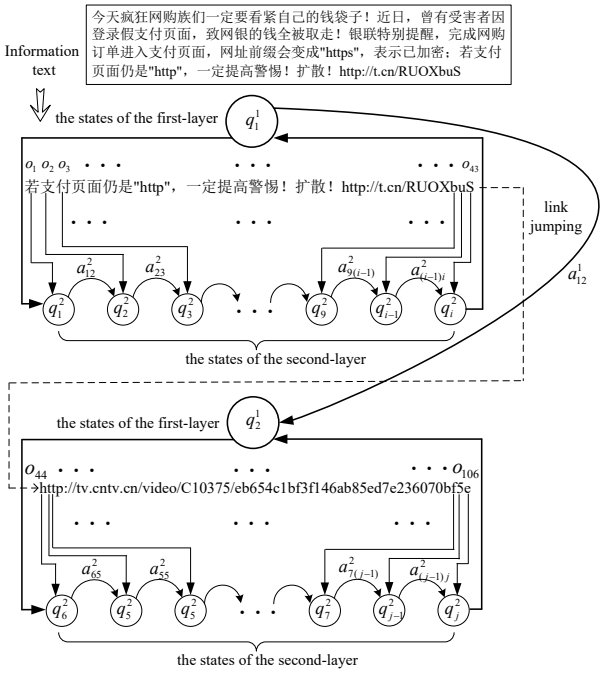

Fig. 1. Link jumping process.

4.2 Phishing short URL detection results

In this section, we evaluate the performance of the proposed approach for phishing short URL detection. We use 2,000 normal short URLs to train the HHSMM model, and the rest data for testing. Figure 2 presents the true positive rate and false positive rate of malicious URL detection on the Weibo data set, with the threshold of the average log-likelihood changing from -5 to 0. If the threshold is set as -3.7, the false positive rate is 6.21% and the true positive rate achieves 95.41%.

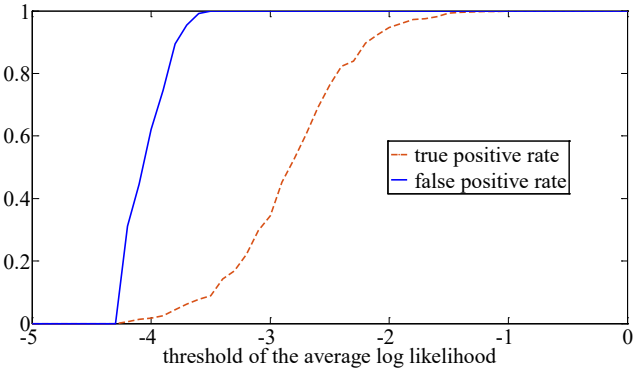

Fig. 2. Adjusting threshold values on Weibo data set.

In addition, we compare the performances of HHMM and HMM using the same training set and testing set. The accuracy, recall, and F1 of HHMM and HMM are shown in Figure 3. The training time and testing time are shown in Table 1. Note that the results are

obtained on a computer with 4×3.46GHz Intel Xeonprocessors, 8GB of RAM. The training time of HHMM is more than 15 seconds. HMM spends 5 seconds to finish the training. In the aspect of testing time, HHMM spends 4 seconds, HMM takes around 1 second.

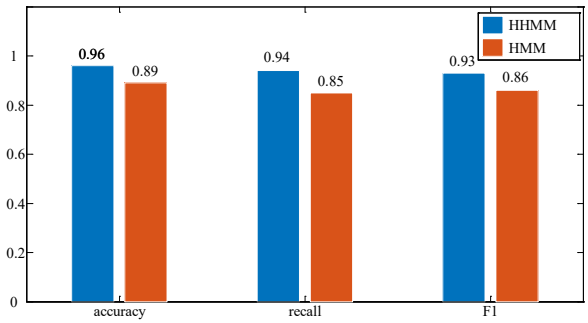

Fig. 3. Comparison testing results.

Table 1. Training time and testing time.

Methods	Training time	Testing time
HHMM	16 s	4 s
HMM	5 s	1 s

5 Conclusion

This paper focuses on the problem of phishing short URL detection. We introduce a hierarchical hidden Markov model with two-layer structure to describe the link jumping process after user clicking on short URL, for detecting phishing short URL on social networks. The first two sentences of the short link, the short link, the last two sentences of the short link, and the characters in the link jumping process are considered as observations. The experimental results show that the method can effectively detect the phishing short URL, and HHMM is better than HMM in describing the link jumping process.

This work was supported by the Guangdong Basic and Applied Basic Research Foundation (Grant No.2018A0303130045), the Science and Technology Program of Guangzhou (Grant No. 201904010334).

References

1. Mitnick K D, Simon W L. The Art of Deception: Controlling the Human Element of Security[M]. John Wiley & Sons, Inc. 2002.
2. 2016 Internet Fraud Trend Research Report [OL]: http://zt.360.cn/1101061855.php?Dtid=1101 062366&did=210142130.
3. Aggarwal A, Rajadesingan A, Kumaraguru P. PhishAri: Automatic Realtime Phishing Detection on Twitter[C], E-Crime'12, 2012:1-12.
4. Manju C N, Prema S. A Distributed System for Detecting Phishing in Twitter Stream[J], International Journal of Engineering Science and Innovative Technology, 2014, 2(3):151-158.

5. Gupta N, Aggarwal A, Kumaraguru P. Bit.ly/malicious: Deep Dive into Short URL Based E-crime Detection[C], 2014 APWG Symposium on Electronic Crime Research, 2014:14-24.
6. Wang D, Navathe S B. Click Traffic Analysis of Short URL Spam on Twitter[C], The 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013:250-259.
7. Spoorthi K, Mail_Alert: Online Suspicious URL Detection of Tweets from Twitter Public Timeline[J], International Journal of Computer Science and Mobile Computing, 2014,4(3):817-824.
8. Nepali R K, Wang Y. You Look Suspicious!!: Leveraging Visible Attributes to Classify Malicious Short URLs on Twitter[C], The 49th Hawaii International Conference on System Sciences, 2016:2648-2655.
9. Cao J, Li Q, Ji Y, et al. Detection of Forwarding-based Malicious URLs in Online Social Networks [J]. International Journal of Parallel Programming, 2016, 44(1):163-180.
10. Guan D J, Chen C M. Malicious URL Detection on Facebook[OL]: https://scholar.google.com /scholar?hl=zh-CN&q =Malicious+URL+Detection+on+Facebook&btnG=&lr=.
11. Sahoo D, Liu C, Hoi S C H. Malicious URL Detection Using Machine Learning: A Survey[J]. Eprint Arxiv, 2017:1-20.
12. Fine S, Singer Y, Tishby N. The Hierarchical Hidden Markov Model: Analysis and Applications[J], Machine Learning, 1998, 32(01):41-62.
13. L.R. Rabiner. A tutorial on hidden Markov models and selected applications in speech recognition [J]. Proceedings of the IEEE, 1989, 77(2): 257-286.
14. Basit, Abdul, et al. A comprehensive survey of AI-enabled phishing attacks detection techniques [J]. Telecommunication Systems, 2021, 76(1): 139-154.
15. Abbasi, A., Dobolyi, D., et al. The phishing funnel model: a design artifact to predict user susceptibility to phishing websites [J]. Information Systems Research, 2021, 32(2):410-436.