RESEARCH ARTICLE OPEN ACCESS

Sybil Belief: A Semi- Creation New Approach for Structure –Based Sybil Detection

K.Ravikumar[1], B. Selvam [2]

[1](Asst.professor, Dept.of.Computer science, Tamil University (Established by the Govt.of.Tamilnadu), Thanjavur)

[2] (Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur.)

----------**********----------

Abstract:

Sybil attacks are a fundamental threat to the security of distributed system. There has been a growing interest in leveraging social network to mitigate Sybil attacks. We introduce Sybil belief a semi supervised learning framework to detect Sybil nodes. Sybil Belief takes a social network of the nodes in the system, a small set of known benign nodes, and, optionally, a small set of known Sybil's as input. We show that Sybil Belief is able to accurately identify Sybil nodes with low false positive rates and low false negative rates. Sybil Belief is resilient to noise in our prior knowledge about known benign and Sybil nodes. Sybil accounts in online social networks are used for criminal activities such as spreading spam or malware stealing other users' private information and manipulating web search results. Sybil defenses require users to present trusted identities issued by certification authorities. However, such approaches violate the open nature that underlies the success of these distributed systems.

Keywords **— Sybil attack, social work, Detection.**

----------**********----------

I. INTRODUCTION

Sybil attacks, where a single entity emulates the behavior of multiple users, form a fundamental threat to the security of distributed systems .Example systems include peer-to peer networks, email, reputation systems, and online social networks. For instance, in 2012 it was reported that 83 million out of 900 million Face book accounts are Sybils. Sybil accounts in online social networks are used for criminal activities such as spreading spam or malware, stealing other users' private information , and manipulating web search results via "+1" or "like" clicks. Traditionally, Sybil defenses require users to present trusted identities issued by certification authorities. However, such approaches violate the open nature that underlies the success of these distributed systems. Recently, there has been a growing interest in leveraging social networks to mitigate Sybil attacks. These schemes are based on the observation that, although an attacker can create arbitrary Sybil users and social connections among themselves, he or she can only establish a limited number of social connections to benign users. As a result, Sybil users tend to form a community structure among themselves, which enables a large number of Sybil users to integrate into the system. Note that it is crucial to obtain social connections that represent trust relationships between users, otherwise the structure-based Sybil detection mechanisms have limited detection accuracy.

1.1. OBJECTIVE

Sybil Belief a semi-supervised learning framework, to perform both Sybil classification and Sybil ranking. Sybil Belief overcomes a number of drawbacks of previous work. We extensively evaluate the impact of various factors including parameter settings in Sybil Belief, the number of labels, and label noise on the performance of Sybil Belief using synthetic social networks.

1.2. EXISTING SYSTEM

Sybil detection mechanisms rely on the assumption that the benign region is fast mixing. we recast the problem of finding Sybil users as a semi-supervised learning problem, Sybil detection

methods decrease dramatically when the benign region consists of more and more communities they cannot tolerate noise in their prior knowledge about known benign or Sybil nodes and they are not scalable.

2.1.EXISTING SYSTEM DISADVANTAGES

- They can bootstrap from either only known benign or known Sybil nodes limiting their detection accuracy.
- They are not scalable

PROPOSED SYSTEM

We analyze the problem of behavioral characterization Sybil accounts in online social networks are used for criminal activities such as spreading spam or malware.

2.2. PROBLEM DEFINITION

Sybil Belief using both synthetic and real world social network topologies. We show that Sybil Belief is able to accurately identify Sybil nodes with low false positive rates and low false negative rates. Sybil Belief is resilient to noise in our prior knowledge about known benign and Sybil nodes. They can bootstrap from either only known benign or known Sybil nodes, limiting their detection accuracy, they cannot tolerate noise in their prior knowledge about known benign or Sybil nodes. They are not scalable.

2.3. METHODOLOGIES

Sybil Belief a semi-supervised learning framework, to perform both Sybil classification and Sybil ranking. Sybil Belief overcomes a number of drawbacks of previous work. We extensively evaluate the impact of various factors including parameter settings in Sybil Belief, the number of labels, and label noise on the performance of Sybil Belief using synthetic social networks.

2.3.1. MODULES

USER

1.Authentication
2.Registration Form
3.Edit profile
4.Request Friend

2.3.2 MODULE DESCRIPTION

Authentication

If you are the new user going to consume the service then they have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself..

Registration Form:

In this Module If he is a new user he needs to enter the required data to register the form and the data will be stored in server for future authentication purpose.

Edit profile:

A profile can be used to store the description of the characteristics of person. This information can be exploited by systems taking into account the persons' characteristics and preferences.

Request Friend:

Someone is the act of sending another user a friend request on Social Network. The two people are social network friends once the receiving party accepts the friend request. Deleting a friend request removes the request.

Blocked Profile:

Admin can compare with profile to all profile. It will match the profile. This profile is identifying fake profile. So that profile will be blocked.

4.CONCLUSION

In this paper, we propose Sybil Belief, a semi-supervised learning framework, to detect Sybil nodes in distributed systems. Sybil Belief takes social networks among the nodes in the system, a small set of known benign nodes, and, optionally, a small set of known Sybil nodes as input, and then Sybil Belief propagates the label information from the known benign and/or Sybil nodes to the remaining ones in the system. We

extensively evaluate the influence of various factors including parameter settings in the SybilBelief, the number of labels, and label noises on the performance of SybilBelief. Moreover, we compare SybilBelief with state-of-the-art Sybil classification and ranking approaches on real-world socialnetwork topologies. Our results demonstrate that SybilBelief performs orders of magnitude better than previous Sybil classification mechanisms and significantly better than previous Sybil ranking mechanisms. Furthermore, SybilBelief is more resilient to noise in our prior knowledge about known benign nodes and known Sybils. Interesting avenues for future work include evaluating Sybil-Belief and previous approaches with datasets containing real Sybils and applying our SybilBelief framework to other security and privacy problems such as graph based Botnet detection, reputation systems ,and private information inference .

5.REFERENCES

[1] J. R. Douceur, "The Sybil attack," in IPTPS, 2002.
[2] Malicious/fake accounts in Facebook, http://www.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts/index.html.

[3] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time url spam filtering service," in IEEE S & P, 2011.
[4] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in WWW, 2009.

[5] P. L. Fong, "Preventing Sybil attacks by privilege attenuation: A design principle for social network systems," in IEEE S & P, 2011. [6] Google Explores +1 Button To Influence Search Results, "http://www.tekgoblin.com/2011/08/29/google-explores-1-button-toinfluence-search-results/."

[6] Google Explores +1 Button To Influence Search Results, "http://www.tekgoblin.com/2011/08/29/google-explores-1-button-toinfluence-search-results/."
[7] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defenses," in SIGCOMM, 2010.

[8] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman., "SybilGuard: Defending against Sybil attacks via social networks," in SIGCOMM, 2006.
[9] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A nearoptimal social network defense against Sybil attacks," in IEEE S & P, 2008.

[9] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A nearoptimal social network defense against Sybil attacks," in IEEE S & P, 2008.

[10] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil nodes using social networks," in NDSS, 2009.