LEVERAGING CROWD-SOURCING FOR EFFICIENT MALICIOUS USERS DETECTION LARGE SCALE SOCIAL NETWORKS

FAZIL A

Asst.Prof. Mr. R. SATHISH KUMAR

Krishnasamy College of Engineering and Technology, Cuddalore.

ABSTRACT:

The past few years have witnessed the dramatic popularity of large-scale social networks where malicious nodes detection is one of the fundamental problems. Most existing works focus on actively detecting malicious nodes by verifying signal correlation or behavior consistency. It may not work well in large-scale social networks since the number of users is extremely large and the difference between normal users and malicious users is inconspicuous. In this paper, we propose a novel approach that leverages the power of users to perform the detection task. We design incentive mechanisms to encourage the participation of users under two scenarios: full information and partial information. In full information scenario, we design a specific incentive scheme for users according to their preferences, which can provide the desirable detection result and minimize overall cost. In partial information scenario, assuming that we only have statistical information about users, we first transform the incentive mechanism design to an optimization problem, and then design the optimal incentive scheme under different system parameters by solving the optimization problem. We perform extensive simulations to validate the analysis and demonstrate the impact of system factors on the overall cost.

Key Terms: Crowd sourcing, malicious user's detection, large scale networks**.**

I.Introduction:

Crowd sourcing has gained quick popularity, because of the data-intensive nature of emerging tasks, requiring validation, evaluation and annotation of large volumes of data.While developing a sound definition of crowd sourcing, Estelles and Guevara suggest that micro tasks are of variable complexity and modularity, and entail mutual benefit to the worker and the requester. Gathering small contributions through such micro tasks facilitates the accomplishment of work that is not easily automatable, through rather minor contributions of each individual worker.

II.Literature review:

Paper1. "Botz-4-Sale: Surviving Organized DDOS Attacks That Mimic Flash Crowds," Proc. Second Symp. Networked Systems Design and Implementation(NSDI '05)Recent denial of service attacks are mounted by professionals using Malicious Users of tens of thousands of compromised machines. To circumvent detection, attackers are increasingly moving away from bandwidth floods to attacks that mimic theWeb browsing behavior of a large number of clients, and target expensive higher-layer resources such as CPU, database and disk bandwidth. The resulting attacks are hard to defend against using standard techniques, as the malicious requests differ from the legitimate ones in intent but not in content. We present the design and implementation of Kill-Bots, a kernel extension to protect Web servers against DDoS attacks that masquerade as flash crowds. Kill-Bots provides authentication using graphical tests but is different from other systems that use graphical tests. First, Kill-Bots uses an intermediate stage to identify the IP addresses that ignore the test, and persistently bombard the server with requests despite repeated failures at solving the tests. These machines are bots because their intent is to congest the server. Once these machines are identified, Kill-Bots blocks their requests, turns the graphical tests off, and allows access to legitimate users who are unable or unwilling to solve graphical tests. Second, Kill-Bots sends a test and checks the client's answer without allowing unauthenticated clients access to sockets, TCBs, and worker processes. Thus, it protects the authentication mechanism from being DDoSed. Third, Kill- Bots combines authentication with admission control. As a result, it improves performance, regardless of whether the server overload is caused by DDoS or a true Flash Crowd.

Paper2. "Malicious User Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of- Service Attacks," Technical Report AIB-2005-07, CS Dept. RWTH Aachen Univ., Apr. 2005.Denial-of-Service (DoS) attacks pose a significant threat to the Internet today especially if they are distributed, i.e., launched simultaneously at a large number of systems. Reactive techniques that try to detect such an attack and throttle down malicious traffic prevail today but usually require an additional infrastructure to be really effective. In this paper we show that preventive mechanisms can be as effective with much less effort: We present an approach to (distributed) DoS attack prevention that is based on the observation that coordinated automated activity by many hosts needs a mechanism to remotely control them. To prevent such attacks, it is therefore possible to identify, infiltrate and analyze this remote control mechanism and to stop it in an automated fashion. We show that this method can be realized in the Internet by describing how we infiltrated and tracked IRC-based Malicious Users which are the main DoS technology used by attackers today.

III. Proposed Methodology:

In this paper, we propose an approach to detect malicious users in large-scale social networks from a radical new perspective. The system administrator is not directly participated in the detection process. Instead, it leverages the power of normal users in the social networks to accomplish such a difficult goal, i.e., crowdsourcing the detection tasks to the users. When malicious users perform abnormal activities such as cyber attack or advertisement injection, the users who are the victims of these activities can report them to the system administrator. Obviously, in such a way, the detection cost for malicious cost can be significantly reduced since no additional overhead is incurred. Also, the detection accuracy can be increased.

To existing system issues, we investigate the incentive mechanism to encourage the user participation in the malicious user detection in a large-scale social network. Interestingly, we consider that the malicious users may provide incentives to the normal users when it performs malicious activities (cyber attack, advertisement injection, etc) towards user For example, if a malicious user wants to get users' profile information, providing some incentives can keep more users silent. Besides, users' preferences are typically different for malicious activities. Some users are more tolerant of advertisement injection than other users. We adopt contract theory to tackle our problem i.e., we construct contractual arrangements as incentive mechanism for system administrator to encourage users to help detect the malicious user

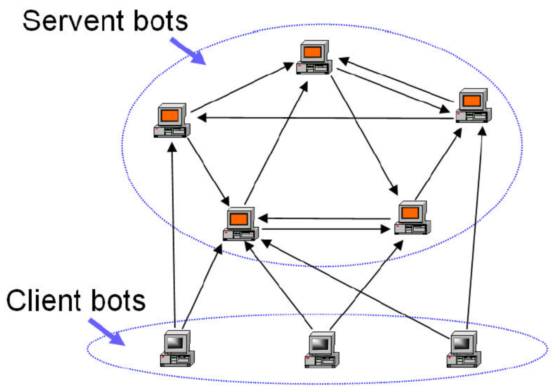
ADVANTAGES

We introduce a novel, efficient, and effective approach, i.e., crowdsourcing, to detect malicious users in lagerscale social networks. Based on this, in order to encourage sufficient users to perform detecting tasks, we formulate the incentive mechanism design problem.

We solve the incentive mechanism design problem in two scenarios: full information of users' preferences and partial information of users' preferences. In full information scenario, we design the optimal incentive mechanism by ordering users' preferences. In partial information scenario, assuming that we only have statistical information about users' preferences, we transform this problem to an optimization problem and solve it by exploring the form of its solution.

We perform extensive simulations to illustrate the relationship between the system' total cost and factors, and validate our analysis.

SYSTEM ARCHITECTURE



IV.FUNCTIONS:

- System Administrator
- Users
- Incentive Scheme

1.System Administrator

When the network size N is to a great degree extensive, it is troublesome for the system administrator to detect the malicious user without anyone else/herself. Accordingly, the system administrator needs to design an incentive mechanism that encourages all users in the network to take an interest in the detection of the malicious user. To abstain from being detected, the malicious user will likewise give incentives to a user *ui* when he/she builds up a link with user *ui*. A link between the malicious user and user could be a cyber attack or advertisement injection. We define the incentives as B which is a constant, in light of the fact that the malevolent user cannot distinguish the difference of users.

2.Users

Users themselves have their own preferences when the malicious user establishes a link with them. So for the so-called malicious user, they will have different response. For example, if the malicious user is trying to promote products to potential customers, their potential customers who have corresponding requirements will have a favorable impression while other users will not like it that much. We denote the preference of each user *ui* by *pi*. It is positive when *ui* has a favorable impression on the malicious user and negative when *ui* thinks it is annoying. We assume that for each *ui* it exactly knows its *pi* and it has no knowledge of other users' preference.

3.Incentive Scheme

The system administrator has to decide an incentive scheme to encourage the report of malicious node from users. We define that u_i's incentive is c_i and c_i >0. Note that the incentives that the system administrator provides vary from person to person. The reason is that the system administrator can have access to some prior information about users in the system so that its incentives can differ as different users' preferences differ. Here we assume that the system will give out its incentives only when there are more than $N0$ users reporting the malicious user, where $N0$ is a predefined threshold. It will cause dishonesty that giving incentives as soon as they report because in this way, users will report all other users including normal users to get a higher payoff. And another assumption is that the system administrator ensures that if each user does as the incentive scheme says, the system administrator can induce $N0$ users and each user's payoff will be maximized. $N0$ should be chosen such that the probability that users in the network report others arbitrarily and finally get the incentive provided by the system is very small.

V.Future Work:

To be well prepared for future Malicious User attacks, we should study advanced Malicious User attack techniques that could be developed by botmasters in the near future. From the robustness and the defense, we can see that the proposed hybrid SOCIAL NETWORK Malicious User makes a future Malicious User harder to be monitored, but most importantly, makes a Malicious User MUCH harder to shut down. By replacing a few isolated C&C servers with a significantly larger amount of interleaved servent bots, the proposed Malicious User greatly increases its survivability. The proposed hybrid SOCIAL NETWORK Malicious User utilizes centralized sensor hosts. This does not make it as weak as a centralized version of Malicious Users. The proposed hybrid SOCIAL NETWORK Malicious User represents only a specific SOCIAL NETWORK Malicious User design. In reality, botmasters may come up with some other types of SOCIAL NETWORK Malicious User designs. However, we believe this research is still meaningful to security community. The proposed design is practical and can be implemented by botmasters with little engineering complexities. Botmasters will come with a similar design sooner or later, and we must be well prepared for such an attack, or a similar attack, before it happens. Defenders would achieve better poisoning defense if they have distributed honeypots and a large number of IP addresses.

VI.CONCLUSION:

The ubiquity of the internet, allows distributing crowd sourcing tasks that require human intelligence at an increasingly large scale. This field has been gaining rapid popularity, not least because of the data-intensive nature of emerging tasks, requiring validation, evaluation and annotation of large volumes of data. Although certain tasks require human intelligence, humans can exhibit maliciousness that can disrupt accurate and efficient utilization of crowdsourcing platforms. In our work, we aim to understand this phenomenon.

VII. REFERENCES:

[1] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-Sale: Surviving Organized DDOS Attacks That Mimic Flash Crowds," Proc. Second Symp. Networked Systems Design and Implementation (NSDI '05), May 2005.

[2] F. Freiling, T. Holz, and G. Wicherski, "Malicious User Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of- Service Attacks," Technical Report AIB-2005-07, CS Dept. RWTH Aachen Univ., Apr. 2005.

[3] T. Strayer, "Detecting Malicious Users with Tight Command and Control," ARO/DARPA/DHS Special Workshop Malicious User, 2006.

[4] Y. Chen, "IRC-Based Malicious User Detection on High-Speed Routers," ARO/DARPA/DHS Special Workshop Malicious User, 2006.

[5.] E.Estelles-Arolas and F.Gonz alez-Ladr on-de Guevara, "Towards an integrated crowdsourcing definition," Journal of Information science, vol. 38, no. 2, pp. 189–2000, 2012.

[6.] K.Ntalianis, N.Tsapatsoulis, A.Doulamis, and N.Matsatsinis, "Automatic annotation of image databases based on implicit crowdsourcing, visual concept modeling and evolution," Multimedia Tools and Applications, vol. 69, no. 2, pp. 397–421, 2014.