Two-Phase Traceback of DDoS Attacks with Overlay Network

Zaihong Zhou[1, a], Jiang Wang[2, b] and Xi Chen[3, c]

[1-2]School of information Engineering, GuangDong Medical University, Dongguan 523808, China

[3]Kunming University of Science and Technology,Kunming 650000, China

[a]Corresponding author, email: sqzhou2012@126.com, [b]email: wrdzsu2003@163.com,[c]email: biometrics@yeah.net

Keywords: Network Security; DDoS Attacks; Oveylay Network; Adaptive CUSUM; Two-phase traceback.

Abstract. An overlay network based traceback scheme against DDoS attacks is proposed in this paper. A CAT server is set in each ISP domain, and receives the alert packets from routers in the domain. According to the alert packets, the intra-domain attack tree is constructed. An alert will be sent to the victim once an intra-domain attack tree is formed. The inter-domain attack tree is constructed at the CAT server of the victim end according to the received alert packets from upstream domains. The traceback request is sent to each CAT server of the inter-domain attack tree once the DDoS attacks are detected. Having received the request, the CAT server will find the attack source along the intra-domain attack tree, and take measures to stop DDoS attacks. The proposed scheme implements two-phase traceback of DDoS attacks effectively and fast.

Introduction

DDoS attacks are the critical threat to the internet. However the dynamic, stateless and anonymous nature of the internet makes it extremely hard to trace back the source of these attacks. A number of traceback approaches are proposed, but most of them adopt packet marking and logging or the hybrid of the two methods.

There are two major methods for packet marking, the probabilistic packet marking (PPM) and the deterministic packet marking (DPM). Savage et al first introduced the probability-based packet marking method and proposed the FMS scheme [1]. It splits each router's IP address and redundancy information into eight fragments and probabilistically marks the IP packet with one of the eight fragments. But it doesn't work well in case of DDoS attacks. Another shortcoming of the FMS is that the packet marking could be forged. To solve this problem, Song et al proposed advanced and authenticated marking scheme-AMS [2]. AMS authenticates the marking information with message authenticate code- MAC function. But the distribution of the secret key is difficult. Goodrich uses the 25 bits of the IP header to store the marking information with link message. Only the fragments with the same link are reassembled into the IP address [3]. It greatly reduces the number of combinations of the fragments and accelerates the path reconstruction. It also reduces the false positives resulted from combinations of the fragments. But it does not mark the distances from the source to the current router. So it can not prevent the attackers from injecting the spoofed information.

The number of packets required for path reconstruction is large and the reconstruction time is long in PPM. Aiming at the shortcoming of PPM, Belenky et al proposed the deterministic packet marking (DPM)[4]. It marks a packet at the edge ingress router. The IP address of each edge ingress router is divided into two fragments. The router will select one of the fragments randomly and write into a packet passing through it. But the false positives are very high in case of DDoS attacks. Aiming at the shortcoming in DPM, Lee et al proposed a deterministic packet marking scheme for tracing multiple internet attackers- DPM-AD [5], but both DPM-AD and DPM mark each packet passing through the router which makes the computation overhead very high when the DDoS attacks occur. Xiang et al proposed flexible deterministic packet marking-FDPM [6]. It can adjust the length of the marking information according to the network protocol and adjust the marking speed according to the router's overload. Thus, it can implement traceback in large-scale DDoS attacks.

PPM and DPM suffer a number of serious drawbacks: lack of scalability; vulnerability to packet pollution from hackers and so on. Logging is another approach to traceback even after the attack has completed. Partial packet information will be stored in routers for the traversed packets and this information provides a trail of the attack path. Full attack path can be reconstructed by applying some data extraction methods. The advantage of this approach is that it does not increase traffic flow, but it increases the storage requirement of the participating routers. Aiming at the drawbacks of the packet marking and logging methods, a two- phase traceback scheme with overlay network is proposed.

The Overlay Network Construction

The ISP domain is treated as the unit of traceback in our proposed scheme. A change aggregation tree (CAT) server is set in each ISP domain and it aggregates the attack information from the routers in the ISP domain. The overlay network is consisted of the CAT servers from all ISP domains. Adaptive CUSUM algorithm is adopted to detect abnormity at each router in the ISP domain. Once an abnormity is found, an alert packet will be sent to the CAT server in the local ISP domain. Having constructed the intra-domain attack tree with traffic weight according to the received alert packets at the CAT servers, another alert packet carrying with weight and domain name is sent to the CAT server at the victim. According to the received alert packets, the CAT server at the victim constructs the inter-domain attack tree with weight and computes the weight of the constructed inter-domain attack tree. If the weight is greater than a detection threshold, it is considered that the DDoS attacks aroused.

Two- phase traceback of DDoS Attacks

The proposed traceback scheme of DDoS attacks is based on the detection of DDoS attacks. Having detected DDoS attack at the victim, the victim CAT server will send traceback request to each CAT server of the inter-domain attack tree. The CAT server traceback to the attack sources according to the constructed intra-domain attack tree and take measures to stop the DDoS attacks.

Adaptive CUSUM based Abnormity Detection. We consider the traffic to port p_i of the router in the t_mth monitoring cycle as observation sequence, and denote it as $X(t_m, p_i)$. In order to apply nonparametric CUSUM, a transformation is made to $XT(t_m, p_i)$ as follows.

$$XT(t_m,p_i)= X(t_m,p_i)\text{-}XX\ p_i \tag{1}$$

To attain accurate $XX\ p_i$, we adopt estimation of mean and variance based adaptive CUSUM algorithm to generate the parameter.To the mean μ and variance σ, we adopt equation (2) and equation (3) to estimate online during each monitoring cycle to adjust the XXp_i adaptively.

$$\hat{\overline{X}}_{t_m,p_i} = \frac{1}{m}\sum_{j=1}^{m} X_{t_j,p_i} = \frac{1}{m}\left[(m-1)\hat{\overline{X}}_{t_{m-1},p_i} + X_{t_m,p_i}\right] \tag{2}$$

$$\hat{s}^2_{t_m,p_i}|_X = \frac{1}{m-1}\sum_{j=1}^{m}(X_{t_j,p_i} - \overline{X}_{t_{j-1},p_i})^2 = \frac{m-2}{m-1}\hat{s}^2_{t_{m-1},p_i} + \frac{1}{m}(X_{t_m,p_i} - X_{t_{m-1},p_i})^2 \tag{3}$$

According to the estimation value of mean and variance online, parameter XXp_i can be adjusted adaptively according to equation (4).

$$XXp_i= \hat{\overline{X}}_{t_m,p_i} +2\ \hat{s}_{t_m,p_i}|_X \tag{4}$$

We define $Z_{in}(t_m,p_i)$ as the accumulation of stochastic variable $XT(t_m,p_i)$

$$Z_{in}(t_m,p_i)=\max\{0,Z_{in}(t_{m-1},p_i)+X(t_m,p_i)-XX\,p_i\} \quad (5)$$

In order to reflect the change more accurately, we define $RD_{in}(t_m,p_i)$ (Relative Deviation) as an indicator of attack.

$$RD_{in}(t_m,p_i)= Z_{in}(t_m,p_i)/\hat{\overline{X}}_{t_m,p_i} \quad (6)$$

If $RD_{in}(t_m,p_i) > \beta$, here, β is the threshold of the router, then the DDoS attacks are declared at the router.

Whether attack traffic is aggregative or not, it can be determined by the ratio of the incoming traffic deviation and the outgoing traffic deviation at the port p_i. We define $Y(t_m,p_i)$ as the outgoing traffic from port p_i in the t_mth monitoring cycle and make a transformation to it as follows.

$$YT(t_m,p_i)= Y(t_m,p_i)-YYp_i \quad (7)$$

$YY\,p_i$ is a parameter of the outgoing traffic to port p_i of the router. To attain accurate $YY\,p_i$, we also adopt estimation of mean and variance based adaptive CUSUM algorithm to generate the parameter.

We define $Z_{out}(t_m,p_i)$ as the accumulation of stochastic variable $YT(t_m,p_i)$

$$Z_{out}(t_m,p_i)=\max\{0,Z_{out}(t_{m-1},p_i)+ Y(t_m,p_i)- YYp_i\} \quad (8)$$

Then the ratio *DR* of I/O traffic deviation is,

$$DR= Z_{out}(t_m,p_i)/Z_{in}(t_m,p_i) \quad (9)$$

If *DR*>=1, then the attack is aggregative at the router. So, an alert packet is sent to the local CAT server.

The Intra-Domain Attack Tree Construction. The intra-domain attack tree is constructed according to the maintained network topology and the alert packets from all routers at the local CAT server in a monitoring cycle. Denote *G* as the copy of the local network topology. The router is the node in *G*. It contains the following messages :{ *R_ID*, *Weight*, *UP_NUM*, UP_R_1, UP_R_2, …, $UP\_R_{up\_num}$, *DN_R*}, where *R_ID* is the router *ID*. *Weight* is the edge weight between current router and downstream router, *UP_NUM* is the number of upstream routers, $UP\_R_{up\_num}$ is the address of upstream routers, and *DN_R* is the address of downstream routers respectively. The alert packet contains {*R_ID*, *FLOW_ID*, *AttackTraffic}*. They are the router *ID* - *R_ID*, flow *ID* - *FLOW_ID*, the attack traffic respectively. Denote the address of the root in *G* as R_0, the being processed node as *R*, the next being processed node as *Q*, alert packet as *P*.

CAT server starts the process from the root R_0 in *G*. If current node is not a leaf, the children's message is saved. A scanning for the alert packets is done to get whether any alert packets are from the current router. If not found, the current node will be removed. Otherwise, the *AttackTraffic* in the alert packet is assigned to the field *Weight* of current router. Repeating the process to all the children nodes of R_0 till the child is leaf.

The Inter-Domain Attack Tree Construction. Having constructed the intra-domain attack tree at the CAT server of the intermediate network, the weight *W* of each intra-domain attack tree is calculated at the CAT server to reduce the storage and computation overhead at the victim end, here, $W=\sum w(R_i,R_j)$. An alert packet is sent to the CAT server at the victim end. The alert packet is a 4-tuple {*AS_ID,UP_AS_ID,DN_AS_ID,W*}, where *AS_ID* is the *ID* of current AS, *UP_AS_ID* is the

ID of upstream AS, *DN_AS_ID* is the *ID* of downstream AS, and *W* is the weight of intra-domain attack tree.

The inter-domain attack tree is constructed according to the alert packets from upstream CAT server of the victim end. Starting from the AS of the victim end, if an AS's *DN_AS_ID* is equal to the victim's *ID*, the AS is added to the victim's child. Then, starting from the child, all ASs will be the child's children if *DN_AS_ID* is equal to the child's *ID*, and so on, till all ASs nodes are disposed. The weight $W(AS_i, AS_j)$ of the edge between domain nodes AS_i and AS_j is the weight of intra-domain attack tree in AS_i domain. Having constructed inter-domain attack tree at the victim end, the weight of the domain tree is calculated, which is the sum of the weight *W* of all edges. The sum of weight *W* indicates the attack traffic from all routers. If $\sum W_i > \gamma$, it is determined that the victim end is suffered from DDoS attacks. Then the victim end will traceback distributedly according to the inter-domain attack tree and the intra-domain attack tree.

Experimental Results

The proposed traceback scheme is based on the detection of DDoS attacks using adaptive CUSUM at the router. Once the DDoS attacks are detected, the alert packet will be sent, and then the attack tree is constructed, and the DDoS attacks source is found. An accurate comparison is done between the ID of current node and the DN_AS_ID of the child node to determine whether the current node adds into the tree while the inter-domain attack tree is constructed. So the construction algorithm will not result in false positives. The construction of the intra-domain attack tree is based on the network topology. The router node will be deleted if it didn't send any alert packet. Whether the alert packet will be arise at the router is determined by the detection rate of the adaptive CUSUM algorithm and whether the false positives from alert packet will be arise is determined by the false positives of the adaptive CUSUM algorithm. So we test the detection rate and false-positive rate of the adaptive CUSUM algorithm at the router to evaluate the effectiveness of the traceback scheme.

We use NS2 simulator and adopt real ISP topology downloaded from the Rocketfuel project website in University of Washington. Having attained and set all parameters in our detection scheme – A_CUSUM, we measure the detection rate of UDP attacks and TCP attacks in 1, 2, 4,8,16 ISPs when the attack sources are distributed randomly. We also study the trade-off between detection rate and false-positive rate of UDP attacks. The detected results are shown as Fig.1, Fig. 2 and Fig. 3.

Conclusions

In this paper, we proposed an overlay network based traceback scheme against DDoS attacks. It doesn't need to probabilistically mark the packets or deterministically mark the packets, so it avoids the drawbacks: lack of scalability; vulnerability to packet pollution from hackers and extraordinary challenge on storage space at victim or intermediate routers. Once the DDoS attacks are detected at the victim, the traceback request will be sent to each CAT server of the inter-domain attack tree. Having received the traceback request, The CAT server begins to find the attack sources according to the intra-domain attack tree and take measures to stop the DDoS attacks. Our scheme implements two-phase traceback against DDoS attacks. It is fast compared with other schemes which traceback the attackers hop by hop. But the traceback time it costs needs to be measured further. In addition, our scheme can not distinguish the DDoS attacks and flash crowds. These are needed to be solved in the future.

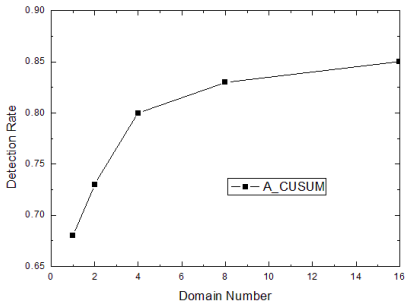

Fig.1 The Detection Rate of UDP attacks

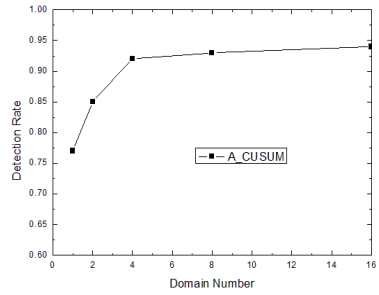

Fig.2 The Detection Rate of TCP attacks

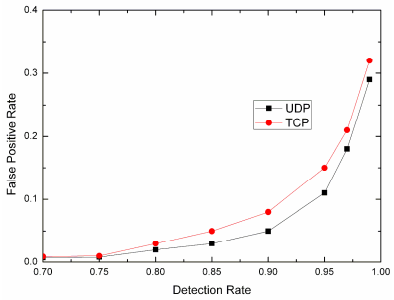

Fig.3 The Detection Rate and False-Positive Rate of A_CUSUM

Acknowledgements

This work was supported in part by the Doctoral Fund of Guangdong Medical College with Grant No. B2012055 and B2012057, and the Zhanjiang Municipal Science and Technology Bureau（Grant No.2013B01089 and Grant No.2013B01093）and by the National Natural Science Foundation of china under (Grant: 61262040), the applied basic research projects of Yunnan Province under (Grant: KKSY201203062, KKS0201503018).

References

[1]Savage S, Wetherall D, Karlin A, et al. Network Support for IP traceback. ACM/IEEE Transactions on Networking, 9(3):226-237. (2001)

[2]Song D X, Perrig A. Advanced and Authenticated Marking Schemes for IP Traceback. In: Proceedings of 20th Annual Joint Conference on Computer Communications (INFOCOMM'2001). Anchorage, Alaska,USA:IEEE Press, 2:878-886.(2001)

[3]Goodrich M T. Probabilistic Packet Marking for Large-Scale IP Traceback. IEEE/ACM Transaction Network, 16(1): 15-24.(2008)

[4]Belenky A, Ansari N. IP Traceback with Deterministic Packet Marking. IEEE Communications Letters,7(4):162-164.(2003)

[5]Lee T H, Huang T Y W, Lin I. A Deterministic Packet Marking Scheme for Tracing Multiple Internet Attackers IEEE International Conference on Communications, 2005(ICC'2005). Seoul Korea:IEEE Press,850-854.(2005)

[6] Xiang Y, Zhou W L, Guo M Y. Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks. IEEE Transactions on Parallel and Distributed Systems, 20(4):567 – 580.(2009)