Research on Attack Source traceback

Wei XU
College of Computer Science and Technology,
Zhejiang University of Technology,
Hangzhou, China
xw@zjut.edu.cn

Qiaohong XU
College of Computer Science and Technology,
Zhejiang University of Technology,
Hangzhou, China

***Abstract*—The existing methods of attack traceback still have many defects, such as input debugging method requires the professional intervention; ICMP traceback message takes up the network bandwidth resources and so on, so a new collaborative network is picked up, based on ant source of ideological attack tracking method. This method is mainly used strategy from ICMP traceback message, that is, data packet attacked is backed-up on the network monitor, and then the scope of the query path information is reduced using the ant colony algorithm, enabling rapid construction of the attack path. Experiments show that the method improves the query speed of tracking information and the accuracy of positioning the source attack.**

Keywords- intrusion detection system; the source of network attack; pheromone

I. INTRODUCTION

Now along with the network popularization, people can have very convenient access to network service, but at the same time, the network attack technologies also develop and improve continually, attack means are much more diverse, It is more and more difficult to locate the attack source accurately and quickly. For example attack source can use other host ‘s System flaw to make other host under its control and implement the sabotage. Attack source can span multiple network area to attack legitimate hosts , increase the difficulty of accurate positioning to the attack source, it is not an easy thing to locate the the real source address accurately by existing technology, only can traceback to the router which close to the attack source, but the result of the traceback is still of some positive effect, can use other technology to filter the source of the attacker, minimizing the destruction of the network as far as possible.

II. CORRELATIONAL STUDIES

In the field of tracebacking the attacker, the professionals at home and abroad have done a lot of researchs, for example: input debugging method [1], ICMP positioning message method,

APPM(adaptive probability packet marking algorithm) [2], etc. Among them, the input debugging method is applicable to attacks which are going on, concluding attack characteristics and tracing to the attacker; ICMP positioning message method is using a new iTrace news, its principle is using the router to macke the iTrace news for trafficing packets with certain probability, then transmit the iTrace new forward to its destination, when its destination received enough ICMP positioning message can reconstruct the attack-path; APPM is based on ICMP positioning message method, the routers in network area, which *are certain probability for marking iTrace new for* trafficing packets , so that reduce the number of data packets to reconstruct the attack-path. These technologies have their own flaw, such as the input debugging method is applicable to attacks which are going on, if the attacker stop the attack, the method does not work.

According to the shortcomings of the above methods, the author propose a new method about network cooperated to traceback the attacker, which is based on ant colony, divides complete reconstruct attack-path into several path, and use pheromone to transfer searching path information, use pheromone a priori knowledge to reduce search range, and also use pheromone to get the "optimal solution" of the attack-path, and comparing the existing approaches, this method take advantage of attacker can't change hardware identification on the link when data packets transfering on the path ,and can better solve the problems of upstream and downstream on the attack-path, and also has the ability to locate the attacker after the attack, therefor this method can trackback the attacker timely and accurately .

III. THE TRACCBACK ATTACK OF SYSTEM MODEL

This system use a network monitor distributing in sharing network to detect and filter packets, and the network monitor is using distributed network intrusion detection system [3-4] to detect message. In order to give an accurately alarm to attack messages, and try to reduce error rate, use misuse detection system, its principle is that matching the messages with the known attack signature, so can reduce false rate, but the shortcoming of this method is that is can do nothing to the new attack.

A. The Protocol of tracebacking attacker system

The method use communication protocol for network monitor and the analyzer to share the attack information, so this paper defines a new traceback protocol based on IP protocol. The new protocol is used for sending path inquiring information between network monitor and the analyer, as well as the monitors send path query information for each other. Figure 1 describes the data packet format of the new protocol .

Published by Atlantis Press, Paris, France.

The protocols redefine the IP packer header, using the field which do not often use: news marks, information area.

The bit of the packets type

1).The bit of news marks: 0 means query information, this information means that the network attack is detected by monitor, and send this query information to other monitors to get information of attack-path.

2).The bit of news marks: 1 means response information.

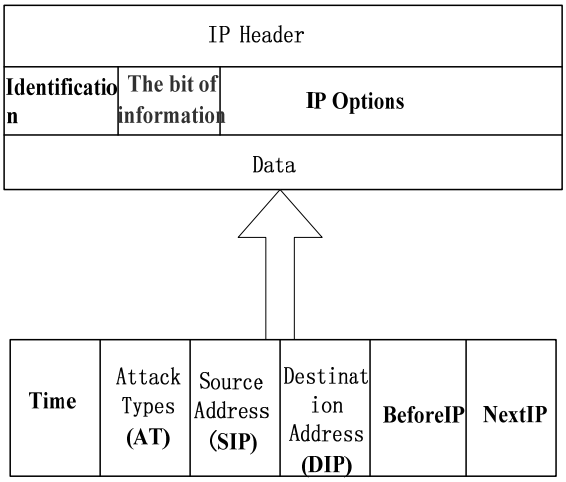

Fig.1 The format of alarm packet

The inquiring information of the analyzer

The bit of information area means querying information of the analyzer, mainly for the analyzer to send query information to a monitor for getting information of attack-path, or send query information to other analyzer nearby. Specific message types as is shown in table 1:

Table 1 Message type of analyzer

00	Send the query attack-path information to monitor
01	Send the query attack-path information to analyzer
10	unused
11	unused

The packet of data region

Data region contains AT, SIP, DIP, BeforeIP, NextIP. AT is mean attack type to judge specific attacks; SIP, DIP is a mark to distinguish simultaneous attacks from multiple attackers; the above data is used to distinguish whether the same attack is from the one attacker. BeforeIP, NextIP is used to reconstruct attack- path, and be difference between other attack- path.

B. Reconstruct attack-path algorithm based on ant colony ideal

The reconstruct attack-path mechanism based on ant colony algorithm, each network monitor maintenance two tables, local alarm information table C and information query table T. Local alarm information table C keeps attack information of the monitor (including AT, SIP, DIP, BeforeIP, NextIP), these information is for querying and reconstruct attack-path, and information query table T is a dimensional array M[S1,S2,…,Sm],it contains m elements(namely the number of adjacent monitors), initial value of each element is

$$s_1(0) = \frac{1}{|\,path\,|} \quad (1)$$

There into, | path| is the number of adjacent monitors. That mean the opportunity of sending query information to the monitors is equal, along with the query and time consumption, numerical values of the a dimensional array will change

The reconstruct attack-path algorithm is as follows:

1). Network analyzer will send a query attack-path message to the monitor randomly ,and the information includes: AT, SIP, DIP.

2).When the network monitor receive this query packet from analzyer, it will first check its Local alarm information table, and find out the record related this query, this record contains 6 elements M (time, AT, SIP, DIP, BeforeIP, NextIP), and generate an inquire ant in this monitor. First of all, the inquire ant search information query table of local monitor, finding out the monitor nearby which pheromone Infij (means the first j a monitor I adjacent monitors the value of pheromone)is over threshold P, if the number of monitor node meeting the conditions is more than 1, then send the query pocket to those monitors, if there is no node then send query pocket to nearby monitor according to the number order of the pheromone, and add searched sign for the monitor which has searched.

3). when the forwarded query information reach a next network monitor, the first thing to do is judging : if the attack type is AT, the attack source IP is right, whether this monitor has visited , if be visited, the message fails, otherwise, query the alarm information table, sent the attack-path information to the analyzer to do relevant analysis and reconstruct attack-path, and monitor creates a response message, this message will return to the previous monitor carrying information which has been confirmed and updated information of the pheromone.

C. The update mechanism of pheromone

The aim of using pheromone mechanism is to learn which monitor the network attack messages traffic. More Correctly, which link have traffic bigger data flow, so it is more likely to detect attack packet, but these pheromones also can't increase outrageous, they should as time goes by and volatile, its computation follow as

$$s_{ij}^{'}(k) = (1-p)s_{ij}(k-1) \quad (2)$$

When monitor received confirmation packet, then update the corresponding monitor's pheromone value.

Published by Atlantis Press, Paris, France.

$$s_{ij}^{'}(k)=(1-\varphi)s_{ij}(k-1)+\frac{\varphi}{|path|} \quad \varphi\in[0,1] \quad (3)$$

$s_{ij}^{'}$ the value after the update; φ for volatile coefficient; $s_{ij}^{'}(k)$ For i the jth adjacent monitors after k times the value of the pheromone update

We can draw a conclusion that the more verifying information its j nearby monitor get the more pheromone it will get in a shortest time, the probability of getting needed attack-path information is bigger.

We do simulation to this reconstruct attack-path algorithm, and got the compare result this method to ATCM[5], showing that this method is more efficient in search attack-path. as shown in figure 2.

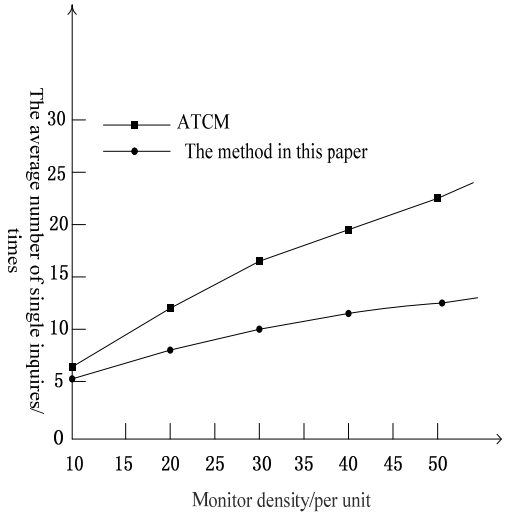

Fig. 2 The compare result between this method and ATCM

D. *The set of attack-path*

The analyzer will use information of attack-path in packet to reconstruct attack- path, when it receive the response of path inquires packet. The direct basis is the information belonging to the same attack path, the same attack types AT, and the same IP of victim and attacker, with the help of address of last and next hop to reconstruct attack-path. Such as the attack- path {Attacker, R1, R2, R3, Victim}, as shown in figure 3.

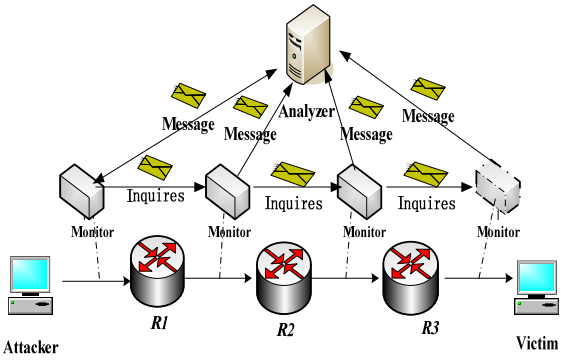

Fig.3 The example of attack path

Analyzer reconstruct attack-path according to the information of the network monitor, as shown in figure 4.

If analyzer found that one link lacks information, it will send query packet to monitors to get attack-path information to complete attack-path.

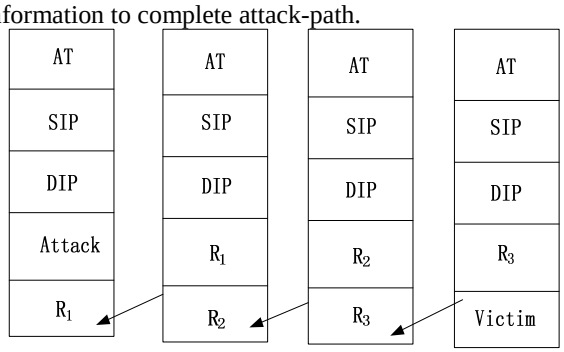

Fig.4 The path of attack

E. *Description of regional collaborative tracking process*

The analyzer can only reconstruct a part of the attack-path when the attacker span multiple network area to attack legitimate hosts. Therefore, analyzer need cooperative work when wants to reconstruct a complete attack-path. When analyzers nearby receive the request packet, the content is M（AT, SIP, DIP, BeforeIP, NextIP）, first of all, take out AT, SIP, DIP and judge whether there is the same attack-path, if the related record exist, we take out next hop node NextIP and match it with the record of BeforeIP, if matching successfully, analyzer nearby will send the whole record to the previous communicate analyzer to finish reconstruct attack-path.

IV. CONCLUSION

Put forward an Attack traceback method which is based on ant colony ideas, realize the main algorithm. This method take advantage of attacker can't change hardware identification on the link when data packets transfering on the path to solve upstream and downstream and can reconstruct attack-path accurately.

The method need not only cooperative work of different network analyzer ,but also need deep mining to attack-path information when the attacker span intra-domain attack the hosts, and still need to improve correlate analysis of each attack-path, there are more

Published by Atlantis Press, Paris, France.

further research work to do for us.

REFERENCES

[1] Wang-yan,"Performance analysis on techniques of tracing network attacks",Comouter Applications and Software,pp.294-297, Feb 2011.

[2] Lv-junliang and Liu-li,"New fragment marking algorithm for IP traceback",Computer Engineering and applications,pp.4-7,March 2010.

[3] Ling-Guoyuan and Cao-Tianjie, "A servey on intrusion detection system",Computer Applications and Software,pp.14-17, March 2009.

[4] Shi-Zhicai and Xia-Yongxiang,"Survey on intrusion detection techniques for high-speed networks",Application Research of Computers, pp.1606-1610,May 2010.

[5] Xiao-Dan,Yang-Yingjie and Shi-Minjian,"Attack traceback method based on collaborative mechanism",

Computer Applications,pp.854-858,April 2007.

Published by Atlantis Press, Paris, France.