A New Attack Model of Anonymous Communications System Based on Rerouting

Chen Zhili
Hunan University of Finance and Economics
Changsha,China410205

He Tiezu
Hunan University of Finance and Economics
Changsha,China410205

***Abstract*—A new attack model is presented in the foundation of the model of anonymous communications system based on rerouting. Based on this model, it proposes one kind of attack algorithm. The premise of this algorithm realization is that only one sender and one receiver are in the anonymous system, and the sender uses the fixed retouting for information transmission. According to the data computation and the theoretical analysis, the probability that the model finds out the sender and destroys the anonymity of the syetem is at 100% and when the system scale, the rerouting length or the observation times have reached a fixed value.**

Keywords- rerouting, anonymous communications system, model, attack

I. INTRODUCTION

One important purpose of anonymous communications is to conceal the identities of both sides or their relationship, which will better protect the privacy of network users' personal communication and confidential communication. [1] Nowadays, research about anonymous communications technology has gradually aroused the attention of network security researchers and it becomes one of the important branches in network security research areas. All the safety defense technologies are put forward according to concrete attacks. Therefore, we can make a research about the attacks in anonymous communications instead of anonymous communications technology. Research about attack model in our country is relatively less at present. This paper proposes a kind of attack algorithm based on anonymous system, which attaches importance to rerouting technology. Meanwhile, a theoretical analysis and simulation for the attack algorithm have been made.

II. AN ATTACK MODEL OF ANONYMOUS COMMUNICATIONS SYSTEM BASED ON REROUTING

According to its rock-bottom routing mechanism，the current anonymous communications system can be divided into two kinds. [2]One is based on broadcast anonymous communications system, another is based on rerouting anonymous communications system. Most anonymous systems are based on rerouting mechanism. According to the different weight routing components, we can put it into three kinds----based on single agent, based on serial agent and based on P2P structure. In this paper, a rerouting anonymous communications system model based on P2P structure is proposed. This model is composed by N a node, and these nodes are V = {vj ｜ 0 acuities j acuities N - 1}. These N nodes cooperate mutually to realise the irrelevant between the sender and receiver. In order to hide the sender's real features, information sent by the source node, through one or more intermediate nodes, achieves a goal node. In the process of information transmission, the path is called rerouting, and can be described as a "S, I1 I2,..., , IL, R >, among them, S is the sender information, L is the path length, and R is the information receiver. Picture 1 is an anonymous communications system which contains 16 nodes. In the graph , an edge means the path from a source computer to the host computer.

In Figure 1 node 0 and node 5 are the message senders.Before they send a message they select the intermediate nodes to go through and reach the final destination node R1 and R2. Rerouting path of note 0 is <0,5,2,7,11,8, R1>. There are five intermediate nodes, and the length of rerouting is 5; Rerouting path of note 5 is <5,10,3,9 , R2>, and there are three intermediate nodes. The length of rerouting is 3.

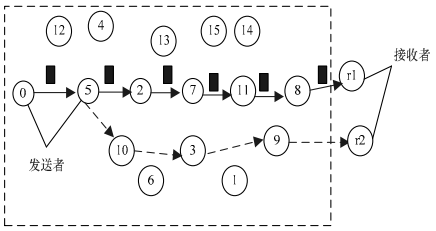

Figure 1. An Attack Model of Anonymous Communications System Based on Rerouting

III. AN ATTACK MODEL AND ITS ALGORITHM

An assumption has been previously made that the attacker takes the passive external attack model. The abilities that the attacker assumed to have are as follows:

The attacker can receive traffic patterns from the attacking object [3], e.g. in MixNets , as the aim of the attacker is to find the connection between the sender and receiver in a traffic , it is easy for the attacker to receive the related traffic pattern directly from the chain which connects to the receiver. As for other anonymous networks, the attacker can receive the target traffic pattern by the method he has learned beforehand .

The attacker can observe all the chains on the network for strengthening attacking power. The attacker is fimiliar with the basic condition of the system, such as the scale of the system, the length of the rerouting (this is a typical assumption when studying the security system.).

The attacker used a method just as algorithm 1 shows. The premise of this algorithm realization is that only one

Published by Atlantis Press, Paris, France.

sender and one receiver are in the anonymous system, and the sender uses the fixed rerouting for information transmission. The number of times that an attacker attacks is K, whose initial value is 1.

Algorithm 1

Step 1. Create an empty set A

Step 2. Create a set S, whose elements are all the nodes of the system.

Step 3. Select a node from the set S randomly and observe it.

Step 4. If the selected node has data receiving and delivering within the given time, put it into set A.

Step 5. operate set S, subtract the just observed node and find out whether the updated set S is empty or not. If it is not empty, switch to step 3, otherwise, switch to step 6.

Step 6. Add 1 to K, repeat step 2 to step 6 several times (the specific times are determined by the attacker) and then switch to step 7.

Step7. Observe each recorded node of set A one by one, and make the observation continuously for a period of time. If any node has data reception during the observation time, remove it from set A. Observe and remove nodes repeatedly until only one node is left, which is considered to be the sender. Then output the sender and the algorithm ends.

Definition: Supposing that the number of members in the anonymous system is N, path length of the rerouting is L, the probability of the dispatcher's sending data is Ps. The duration time of receiving data of the intermediate node is the same as that of the sending data. After the attacker's several rounds' observation, the attacker studies all the nodes in the system with details in every round's observation. After K round's observation, the attacker could correctly find the sender' Pk, see Formula 1：

$$Pk=1-(1-\frac{2}{L+1}\cdot\sum_{i=1}^{N}(\frac{N-L\cdot Ps}{N}\cdot\frac{N-L\cdot Ps-1}{N-1}\cdot\frac{N-L\cdot Ps-2}{N-2}\cdots\frac{N-L\cdot Ps-(i-2)}{N-(i-2)}\cdot\frac{L\cdot Ps}{N-(i-1)}))k \quad (1)$$

Demonstration: after first observation, the probability of attacker can find one point of rerouting path:

$$P0=\sum_{i=1}^{N}(\frac{N-L\cdot Ps}{N}\cdot\frac{N-L\cdot Ps-1}{N-1}\cdot\frac{N-L\cdot Ps-2}{N-2}\cdots\frac{N-L\cdot Ps-(i-2)}{N-(i-2)}\cdot\frac{L\cdot Ps}{N-(i-1)}) \quad (2)$$

The demonstration of formula 2 :

Because in the system the probability of date sending is Ps , and after every first round of observation by the attacker ,the probability of selecting the host node on the rerouting path:

$$P1=\frac{L}{N}\cdot Ps$$

After every second round of observations, the probability of selecting host node on the rerouting path:

$$P2=(1-P1)\cdot(\frac{L}{N-1})\cdot Ps$$

$$=(1-\frac{L}{N}\cdot Ps)\cdot(\frac{L}{N-1})\cdot Ps$$

$$=\frac{N-L\cdot Ps}{N}\cdot\frac{L\cdot Ps}{N-1}$$

After every i round of observations the probability of selecting host node on the rerouting:

$$Pi=\frac{N-L\cdot Ps}{N}\cdot\frac{N-L\cdot Ps-1}{N-1}\cdot\frac{N-L\cdot Ps-2}{N-2}\cdots\frac{N-L\cdot Ps-(i-2)}{N-(i-2)}\cdot\frac{L\cdot Ps}{N-(i-1)}$$

Therefore, after every round of observations, the probability of selecting host node on the rerouting:

$$P0=\sum_{i=1}^{N}Pi$$

$$=\sum_{i=1}^{N}(\frac{N-L\cdot Ps}{N}\cdot\frac{N-L\cdot Ps-1}{N-1}\cdot\frac{N-L\cdot Ps-2}{N-2}\cdots\frac{N-L\cdot Ps-(i-2)}{N-(i-2)}\cdot\frac{L\cdot Ps}{N-(i-1)})$$

Formula 2 is proved.

After the first round of observations, finding the probability of the sender:

$$P'=P0\cdot\frac{1}{1+\frac{L-1}{2}}$$

$$=\frac{2}{L+1}\cdot\sum_{i=1}^{N}(\frac{N-L\cdot Ps}{N}\cdot\frac{N-L\cdot Ps-1}{N-1}\cdot\frac{N-L\cdot Ps-2}{N-2}\cdots\frac{N-L\cdot Ps-(i-2)}{N-(i-2)}\cdot\frac{L\cdot Ps}{N-(i-1)})$$

Therefore, after k rounds of observation, the attacker can find the probability of the sender

$$Pk=1-(1-P')k$$

$$=1-(1-\frac{2}{L+1}\cdot\sum_{i=1}^{N}(\frac{N-L\cdot Ps}{N}\cdot\frac{N-L\cdot Ps-1}{N-1}\cdot\frac{N-L\cdot Ps-2}{N-2}\cdots\frac{N-L\cdot Ps-(i-2)}{N-(i-2)}\cdot\frac{L\cdot Ps}{N-(i-1)}))k$$

Formula 1 is proved.

IV. A Theoretical Analysis And Algorithm

According to the given condition of algorithm, it is known that the system has only one data render and a fixed rerouting path. In consequence, the node we observe anytime is a point of route path. The procedure that the middle node receives data first and then sends the received data , (namely storing and retransmission) enables the attacker observes the data receiving and sending at the same time or just the data sending.

We can infer that the probability that the attacker can find out the sender is related to system machinery number, rerouting path, transmitting probability and observation times from formula 1. Chart 1 calculates that when the number of host machine in anonymity communications system N is 16, the length of rerouting path L ranges from 1 to 5, and the probability of data transmission is 0.8, the attacker can find out the changing probability Pk of the sender .

Tabel 1 When the number of the host computer(N) = 16, the attacker can find out the changing probability Pk of the sender.

From the data of the figure, for the same system , i.e. system node N and the probability of sending data are fixed, with rerouting L 's value increasing, the probability of finding out the sender becomes less. For example, an attacker in the end of the first observation , L = 1, finding the sender's probability is 0.560; L = 5, 0.330. According to the definition of anonymous degrees, when the attacker is completely unable to identify that one entity is the sender, anonymity degree is the strongest. Conversely, if the probability of the sender reaches 1.000, the attacker can

identify it completely. And the anonymity degree is on the provably exposed level ,i.e. the weakest one. In addition, the probability of detecting the sender will increase with the rise of the observation of the wheel number. For example, under the condition of L = 5, the probability of finding out the sender in the first observation is 0.330, the second observation 0.551, the forth observation 1.000. And the anonymity degree falls from the possible innocence level to the provably exposed one.

Figure 2 shows the relations between the probability that attackers discover senders and the length of rerouting L when the system size N , the probability of sending data Ps and observation times k are fixed.

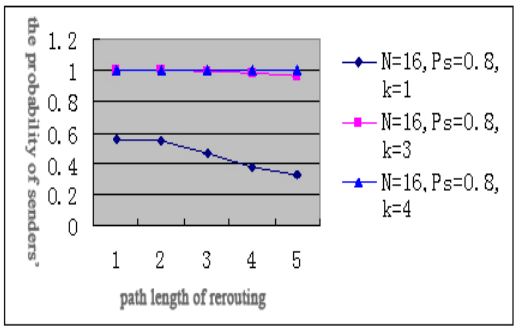

Figure 2. The relations between the probability that attackers discover senders and the length of rerouting L

It is easily seen from Figure 2 that under the same condition the bigger the length value of rerouting L means less the probability of discovering senders and less the success rate of attacking. That is to say, the larger the probability that attackers are not certain about senders the greater the failure rate of attacking and so the better the anonymity .

For the same anonymous system, improving probability of sending statistics can increase probability of finding out senders. Changing node numbers of the system can affect probability of finding senders for attackers.

If Tabel 2 calculates the number of the host computer in the anonymous communications system increasing from N to 100 when the rerouting path length L values from 5 to 25 with 5 as tolerance, set to 0.8 as the transmitfigure data probability, the relationship between probability Pk of the sender and observable number K can be found by the attacker .

As the number of the host N equals 100, the changes of probability Pk of the sender can be found by the attacker.

Compared with figure 2 and figure 1, you can see that if the data is transmitted with the same probability and the number of the system node increase, the probability of the sender will decrease. For example, when N is 16 and L is 5, you can find the probability pk value of the sender is 0.560. When N increases to 100 and L remains, you can find the probability of the sender is 0.160.

When the figure of the system node N and the probability of the transmit figure data are fixed, with the rerouting path length L enlarged, you can find the probability of the sender is getting smaller. For the same system, the probability of the sender will grow with the increase of the observable number.

All the above analyses show that when the system has such an attack as argorithm 1, the anonymous sender will be affected to different degrees.

V. CONCLUSION

This paper proposes an attack model and agorithm based on rerouting anonymous communications system model. Through computation and analysis, it shows that this system can effectively destroy the sender's anonymity if it is attacked by the attack model.

REFERENCES

[1] Xu Hongyun, Chen II, CHEN Song-qiao. Anonymous communication system model of statistical type of attack [J]. Mini-Micro systems, 2004, 25(11): 1926-1929

[2] R. E. Newman-Wolf, B. R. Venkatraman. Performance Analysis of a Method for High Level Prevention of Traffic Analysis[J]. 10th Annual Computer Security and Application Conference, Orlando, Florida Dec.5-9,1994.

[3] Clay Shields,Brian Neil Levine.A Protocol for Anonymous Communications Over the Internet,Proceedings of 7th ACM Conference on Computer and Communications Security, Athens, Greece, November 2000:22-42.

TABLE I. WHEN THE NUMBER OF THE HOST COMPUTER(N) = 16, THE ATTACKER CAN FIND OUT THE CHANGING PROBABILITY PK OF THE SENDER.

K \ P	1	2	3	4	5
1	0.560	0.543	0.463	0.389	0.330
2	0.806	0.791	0.711	0.626	0.551
3	0.999	0.998	0.993	0.981	0.959
4	1.000	1.000	1.000	1.000	1.000
5	1.000	1.000	1.000	1.000	1.000
6	1.000	1.000	1.000	1.000	1.000

TABLE II. WHEN THE NUMBER OF THE HOST COMPUTER(N) = 100, THE ATTACKER CAN FIND OUT THE CHANGING PROBABILITY PK OF THE SENDER.

P / K	5	10	15	20	25
1	0.160	0.134	0.109	0.089	0.075
2	0.294	0.250	0.206	0.171	0.144
3	0.752	0.683	0.602	0.527	0.463
4	1.000	1.000	0.999	0.998	0.993
5	1.000	1.000	1.000	1.000	1.000
…					

Published by Atlantis Press, Paris, France.