Intrusion Detection System based on Fuzzy Default Logic

ZHANG Jian, DING Yong, and GONG Jian
Department of Computer Science and Technology
Southeast University
Nanjing 210096, China
{zhangj,yding,jgong}@njnet.edu.cn

Abstract — **Current IDSs usually have several shortcomings. First, the speed and sensitivity of detection are not so ideal. Secondly, the response system lacks the ability to correct errors. Thirdly, the cost of intrusion detection is not considered, that is, the response policy is static. This paper applies fuzzy default theory to transform reasoning and response engine of IDS, based on the proving of IDS as non-monotonic, and set up an intelligent IDS—FDL-IDS. The experiment result showed that FDL-IDS increased the detection speed and sensitivity and decreased the cumulative cost as compared with traditional intrusion detection expert system.**

Index Terms—**Fuzzy Default Logic, Intrusion Detection, Monotonic Logic , Response Rollback**

Ⅰ INTRODUCTION

The development of computer networking has changed the stand-alone pattern of computing, but it has also increased the risk and opportunity of network intrusion. The design of secure measures to prevent unauthorized accesses to resources and data of systems becomes a very important issue in the network security domain. At present, it is impossible to completely eliminate the occurrences of security events, and all the security faculty can do is to try their best to discover intrusions and intrusion attempts so as to take effective measures to patch the vulnerabilities and restore systems. That brought about intrusion detection and intrusion detection system (IDS).

Artificial intelligence is applied in the intrusion detection research. Dickerson[1] proposed to develop an intrusion detection system based on fuzzy theory, whose main technique is to substitute fuzzy rules for ordinary rules so as to map the knowledge represented in natural language to that represented in computer more accurately. Siraj[2] argued that Fuzzy Congnitive Map(FCM) could be used to support the decision making of intelligent intrusion detection systems. This kind of graph reflects the fuzzy cause and effect relation between events, and can be used to calculate the confidence degree of events, so that the intrusion detection engine can make wiser decisions. Christopher[3] proposed to employ artificial intelligent methods in intrusion detection systems in order to recognize the attackers' plans.

In order to achieve a certain security level, IDS should meet the following requirements:

1) IDS must recognize the attacker's plans and direct responses as early as possible, when precision is guaranteed to some extent. With the progressing of intrusions, the protected object may suffer more severe damage, so there is an urgent requirement on the improvement of speed and sensitivity of detection.

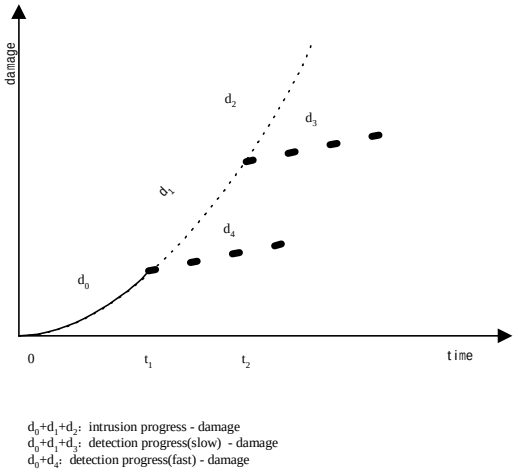

Fig. 1 The influence of detection speed

Fig. 1 shows the damage caused by intrusions as a function of time when Nimda out-broke in CERNET[1]. The damage of protected objects is quantified as continual variant varying with the progress of intrusions. It can be seen that without the protection of IDS, the damage will increase in exponential grade. If the detection speed is slow, for example, the responses are carried out at t_2, the increase of damage will only be linear, and stop after some time. While with fast detection speed, responses will be carried out as early as t_1, so that the damage is greatly decreased.

2) On the occasions of false alarms, the original responses should be rolled back, and correct responses should be carried out, so that the damage of false responses can be decreased. This technique is called Response Rollback.

However, the two requirements are quite difficult to meet. Because IDSs need to collect sufficient evidences so as to decide whether the current behaviors indicate intrusions, but the collection of many evidences is expensive in cost,

[1] CERNET: China Education and Research Network

and often through the whole process of intrusion, which makes it difficult to recognize the intentions and direct responses in time. Furthermore, current IDSs use monotonic reasoning mechanism, in which the inferences from current evidences and the corresponding responses are regarded as non-retrievable, even though they are proved to be false as new knowledge and evidences are added.

Fuzzy default logic is a kind of non-monotonic logic which incorporates both fuzzy logic and default logic. The theory of fuzzy logic is used to ameliorate the knowledge basement of IDS, and to support fuzzy reasoning, while the theory of default logic is used in plan recognition and response rollback. So fuzzy default logic can be a powerful tool to handle the above requirements.

This paper puts forward a fuzzy default logic based intrusion detection system (FDL-IDS). The system is composed of a knowledge basement based on fuzzy default logic (FDL-KB), the corresponding reasoning engine (FDL-IRE), and a response engine with rollback mechanism (RRE). FDL-IRE substitutes the monotonic logic based reasoning for fuzzy default logic based reasoning. RRE decides on how to respond to the intrusions based on cost sensitive model, and is capable of rolling back false responses. There are several advantages of FDL-IDS:

1) FDL-IRE is capable of deciding whether the current behaviors indicate intrusions with insufficient evidence, so that the detection speed is improved.

2) When new knowledge overthrows the previous conclusions, FDL-IRE incorporates it into reasoning process, and come into new conclusions, and then request RRE to roll back the original responses and carry out correct responses.

3) Cost is considered in the decision of responses, which makes the response system more intelligent and reasonable.

Ⅱ The Basic Concepts of Fuzzy Default Logic

A The non-monotonicity of IDS

Theorem: The IDS which may generate false alarm is non-monotonous logic system.

Proof: The IDS always starts out from the knowledge that is already known, and recognizes intrusion behaviors through some detection algorithms (in anomaly detection) or some detection rules (in misuse detection), so it can be regarded as a logic system.

Suppose that the logic system is L={E,O,A(a,t),R}. E represents the set of atom logical expressions, O is the set of operations on E, A represents the set of axioms which is a subset of well-formed formulas (wff). In IDS A(a,t) means the data collected from time a to time a+t, which can be regarded as the known knowledge. R is the set of rules of inference which are used to infer new wffs from A and the wffs that have already been proved. all the theorems can be proved in L is represented as T(L).

In IDS, the set of intrusion events detected by IDS based on the current knowledge is represented as Event(A(a,t)), which is equal to T(L). when $t_1 \geqslant t$, $A(a,t) \subseteq A(a,t_1)$, and for the new logic system $L_1=\{E,O,A(a,t_1),R\}$, the set of theorems that can be proved in L_1 is represented as Event(A(a,t_1)).

The fact that IDS may generate false alarms can be formally described as the following:

$$\forall a \forall t \forall t_1 \exists e((t \le t_1) \wedge (e \in E(a,t)) \rightarrow (e \notin E(a,t_1))) \quad (1)$$

Suppose L is monotonic logic system, then

$$\forall a \forall t \forall t_1 \forall e((t \le t_1) \wedge (e \in E(a,t)) \rightarrow (e \in E(a,t_1))) \quad (2)$$

which is in contradiction with (1). So L is non-monotonous logic system.

Suppose I denotes an intrusion method, then it can be described by the following disjunctive formulas:

$$I = R_1 \cup R_2 \cup \mathbf{L} \cup R_n,$$
$$R_i \Leftrightarrow f_1 \cap f_2 \cap \mathbf{L} \cap f_{m_i}, i = 1,2,\mathbf{L},n$$

In the formulas, R_i is the rule for recognizing I, and the rules are independent of each other. Each rule is the conjunction of several signatures, f_1, f_2……f_m, and the rule is triggered only if each signature is satisfied.

Let the signature set of rule R is $P(R)$, $P(R) = \{f_1, f_2, \mathbf{L}, f_m\}$. The non-monotonicity of IDS lies in that:

1) The description of the rule is incomplete. Suppose R is incompletely described as R', that is P(R') ⊂ P(R).The incompleteness of the rule causes normal behaviors to be misjudged as intrusions, though the probability of false alarms is very low.

2) Many rules are inherently qualitative and fuzzy, which can be explained in two facets. Firstly, each rule has a certain confidence degree. Though each rule may has high confidence degree, it is not absolutely correct. Secondly, the premises of rules are often fuzzily defined, which are only appropriate to be described in natural language. This is often one of the causes of false alarms. The rule that satisfies these two requirements is called the fuzzy rule which is the generation of common rules. It is the fuzziness of the rules that makes the normal rule representation and reasoning absolutize the problem and generate false alarms.

B The Theory of Fuzzy Default Logic

Fuzzy default logic is built on the base of fuzzy mathematics and default logic. Fuzzy mathematics is created by Zadeh, which can be used to represent fuzzy knowledge and carry out fuzzy reasoning. Default logic[4] is a kind of non-monotonic logic, which can be used in reasoning based on inadequate proof.

The disadvantage of default reasoning lies in that its conclusion lacks the parameter of confidence degree. Nevertheless, what we most concern in the research of IDS is how to get reliable conclusions and how to further improve the reliability of the conclusions. Fuzzy logic is a good mechanism to compensate for the shortcomings of the default reasoning logic. This paper puts forward a default logic theory based on fuzzy logic which is called fuzzy

default logic based theory in order to satisfy the requirements of IDS.

Definition 1: The general form of the rules in fuzzy default logic is:

$$a(\vec{x}) : Mb_1(\vec{x}), \mathbf{L}\, Mb_m(\vec{x}) \rightarrow w(\vec{x}) \quad CF, t \qquad (3)$$

where $\vec{x} = < x_1, \mathbf{L}, x_n >, a(\vec{x}), b_1(\vec{x}), \mathbf{L}, b_m(\vec{x}), w(\vec{x})$ are well-formed formulas in fuzzy logic; $a(\vec{x})$ is called the precondition of the rule which is known facts or fuzzy facts; $b_i(\vec{x})$ is called the default condition of the rule which is an event of probability, and its occurrence often has close relation with the preconditions; $w(\vec{x})$ is the conclusion of the rule; τ is the threshold of confidence of the preconditions in the rule, if $T(a(\vec{x})) \geqslant \tau_0$, $T(b_i(\vec{x})) > 0.5, i = 1, \mathbf{L}, m$, the rule is activated; CF is the confidence degree of the rule which is a number within [0,1].

Definition 2: Let L={E,O,A,R} is fuzzy default logic, where E is the set of atomic fuzzy logical formulas; $O \subseteq \{\neg, \vee, \wedge, \rightarrow\}$; A is the set of fuzzy propositions; R is the rules of inference in fuzzy default logic which includes the syllogism in fuzzy default logic.

The syllogism in fuzzy default logic is the extension of that in fuzzy logic. It is represented as the following:

$$\begin{array}{ll} a : Mb_1, \mathbf{L}, Mb_m \rightarrow w & CF \\ a & T(a) \\ b_i & T(b_i) \quad i = 1, \mathbf{L}, m \\ CF + \min(T(a), T(b_1), \mathbf{L}, T(b_m)) > 1 & \\ \hline w & T(w) = \min(T(a), T(b_1), \mathbf{L}, T(b_m)) + CF - 1 \end{array}$$

III FDL-KB and FDL-IRE

A *The Establishment of FDL-KB*

The traditional knowledge base of expert system for intrusion detection only contains facts and ordinary rules. This kind of knowledge base has several disadvantages.

1) The knowledge is static. Once the knowledge is input, it is seldom updated, especially the modification and deletion of knowledge.

2) Ordinary facts and rules cannot give a complete description of knowledge, For example, the concepts of fuzziness, conviction, and experience cannot be represented by ordinary facts and rules.

3) The knowledge base needs artificial maintenance. It depends on human to input the new knowledge, and check the consistency of the rules.

Due to these disadvantages, we devise a fuzzy default logic based knowledge base to substitute the traditional knowledge base. FDL-KB is the counterpart of A in the self-contained formal fuzzy default logic system {E,O,A,R}.

Definition 3: Let C be the set of measures of IDS. The collection cost of a measure is calculated based on the amount of system resources it occupies and the time needed for the collection. C can be divided into n non-intersected subsets based on the collection costs of measures. The measure of minimum collection cost is called the first class measure, while the measure of maximum collection cost is called the nth class measure. Other classes are defined in the same way.

For example, the measures can be divided into three classes in the IDS which takes network connection as its objects of detection. Among them, the source IP, the destination IP, the source port, and the destination port are in the first class of measures. The status of connection is in the second class, which can be collected at any time during the lifetime of the connection. The number of packets and the number of bytes in the connection are in the third class, which have the highest collection cost because they can only be collected in the end of the connection.

The measures in higher class not only consume a large amount of system resources, such as the requirement of matching a string from the beginning to the end of the packet; but also slower the speed of detection, because these measures often cannot be calculated until the intrusion process is achieved when the loss of the intrusion already reaches to its maximum.

The collection of higher class measures can be avoided by substituting fuzzy default rules for ordinary rules of intrusion detection. In this way, higher class measures are used for the default conditions of fuzzy default rules, and lower class measures are used for the preconditions, then it not only makes the collection of evidences of intrusion more simple and more fast, but also improves the speed and sensitivity of detection.

Let the set of measures for an IDS be C, and $c \in C$. E(c,a) is a predicate, which means the value of c is a. Suppose $c_1, c_2, \ldots, c_n \in$ C, then the association rules discovered by data-mining techniques are represented as: $\bigwedge_{i=1}^{n-1} E(c_i, a_i) \rightarrow E(c_n, a_n) \quad [Supp, Conf]$, where *Supp* is the degree of support of the association rule, which equals to $P(E(c_1,a_1) \wedge E(c_2,a_2) \wedge \ldots \wedge E(c_n,a_n))$; Conf is the degree of confidence of the association rule, which equals to $P(E(c_n,a_n) | E(c_1,a_1) \wedge \ldots \wedge E(c_{n-1},a_{n-1}))$. If *Conf* > 0.5, the self-contained formal fuzzy default rules can be established as:

$$\bigwedge_{i=1}^{n-1} E(c_i, a_i) : ME(c_n, a_n) \rightarrow E(c_n, a_n) \quad CF, t$$

where *CF* = *Conf*, and τ is decided by experts.

B *The Establishment of FDL-IRE*

Traditional expert systems on IDS often use non-monotonic reasoning, The advantage of this reasoning engine is its simplicity and easiness of implementation. But it is based on the non-monotonic knowledge base, so if the knowledge base is ameliorated to fuzzy default knowledge base, then comes the need for changing the original

reasoning engine, that is, the corresponding fuzzy default logic based reasoning engine must be set.

Definition 4: The table of propositions is the log of fuzzy default logic based reasoning, which records the facts that are added or deleted each time when new knowledge is collected and reasoning steps are performed. Each line includes five fields including the preconditions of the rule, the default conditions, conclusions, the confidence degree of conclusions, and the deleted facts.

The table of propositions is the interface between FDL-IRE and response engine. After a reasoning step is performed, FDL-IRE records the related information in the table, then perform the next reasoning step. The response engine keeps querying whether new conclusions have been made. If there are new conclusions, corresponding responses will be carried out.

The reasoning of FDL-IRE are performed in the following steps:

1) Perform the reasoning based on the data output from the collector and fuzzy default rules.

2) If some intrusion behaviors are inferred, then the information of the reasoning process, including preconditions of the rule, default conditions, and confidences of conclusions etc., is added to the table of propositions. At the same time, the conclusions are inspected of their consistency with the previous conclusions, preconditions, and default conditions. If there is inconsistency, then the previous default conditions and conclusions are undone and added to the table of propositions as deleted facts.

3) If no intrusion behaviors are inferred, then check the consistency of the collected data with the default conditions in the table of propositions. If inconsistency are detected, then the original default conditions and conclusions are undone and added to the table of propositions as deleted facts. Then go back to step 1).

Ⅳ The Establishment of RRE

RRE has two features:

1) It supports the rollback of responses.

2) It makes decisions of responses based on the cost model. RRE first calculates the ratio of the cost of taking a certain response and the cost of not taking the response, and then decides on how to direct responses based on the ratios of costs.

RRE is an indispensable component of FDL-IDS because:

1) RRE is part of the implementation of fuzzy default theory.

2) RRE is the crucial component to decrease the general cost of IDS.

A The Weighted Cost Sensitive Model which Supports Decision of Responses

a. Analysis of The Costs of Intrusion Detection and Response

1) Detection Cost:

It is the amount of resources that is consumed in the detection, noted as ICost.

2) Response Cost:

It is the amount of resources that is consumed in the responses of intrusions, noted as RCost.

3) Damage Cost:

It is calculated in three conditions. In the first condition, it is the damage when no responses are carried out, noted as Dcost. In the second condition, it is the damage caused by the intrusion after some responses are directed, noted as DICost. In the third condition, it is the damage caused by responses themselves, noted as DRCost, such as the loss to normal users caused by the shutdown of a server.

b. Cost Sensitive Model

Before establishing the cost sensitive model, we need to assign the weight to each cost.

The weight of a cost indicates the importance of this cost in the cost sensitive model. Let the set of all costs be $C = \{c_1,\ldots\ldots,c_n\}$, and the vector of weights is $\omega = \{\omega_1,\ldots, \omega_n\}$, where ω_i is the weight of c_i (i=1,…n), and $\omega_1+\ldots+\omega_n=1$.

The vector of weights reflects the security goal in a certain environment, which is assigned by experts in general.

In order to support the decision of responses, the model first calculates the cumulative cost when a certain response is taken and that when the response is not taken, then direct responses based on the magnitude relation of the two costs.

Let RC be the cost when a certain response is taken, then it can be represented as:

$$RC = w_I \times ICost + w_R \times RCost + w_{DI} \times m \times DICost + w_{DR} \times DRCost \quad (4)$$

Let NRC be the cost when the response is not taken, then it can be represented as:

$$NRC = w_I \times ICost + w_D \times m \times DCost \quad (5)$$

So the cost sensitive model M can be represented as:

$$M = \frac{RC}{NRC} \quad (6)$$

where μ is the confidence degree of the detected intrusion event, and $\omega_I+\omega_R+\omega_D+\omega_{DI}+\omega_{DR}=1$. If $M \geqslant 1$, then no response is taken; otherwise, take the response of minimum RC.

B Response Rollback

The rollback of responses is a special action of response. It interrupts or undoes the responses of false alarms, and eliminate the negative influences of these responses.

Based on Curtis's[5] survey of the response techniques of IDS, responses are classified into three categories based on whether responses can be undone and whether the influences of responses can be eliminated.

1) Responses that can be undone, including locking users' account, blocking the sources of attack, shutting down the host, isolating from network and so on. For these

responses, it only needs to carry the converse actions to roll back them.

2) Response that cannot be undone, but whose influences can be eliminated, including generating reports, generating notifications, making backups and so on. For these responses, the influences can be eliminated by interrupting or generating rollback logs.

3) Responses that cannot be undone and whose influences cannot be eliminated, including warning the intruders, interrupting the session, and so on. For these responses, the rollback module reports to security managers or records them in the log.

The rollback techniques needs the corresponding response logs, which records all the responses. Once RRE receives requests of rollback, it will consult the response logs and carry out the rollback.

Ⅴ Experiments and the results

A The Objectives of Experiments

The objective of the experiment is to test the detection speed and sensitivity of FDL-IDS and evaluate the cost of FDL-IDS. To test the detection speed, PPS(packet per second) is used, while EPS(Event per Second) is used to test sensitivity of FDL-IDS. To evaluate the cost of FDL-IDS, Wenke Lee[6]'s cost-sensitive model and CPE(Cost per type of event) is used.

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes. But Snort hasn't automated response system. So we transformed Snort as following:

1) Add a manager for Snort, manager is an automated response system in fact.

2) Snort directly reports intrusion events to manager, not logs them.

The transformed Snort is called Snort-IDS. Snort-IDS is further tranasformed into FDL-IDS as following:

1) Transform the rule base of Snort into FDL-KB.

2) Transform the packet-matching module of Snort into FDL-IRE.

3) Transform the manager so that it has the function of response rollback.

In the experiment the performance of FDL-IDS is compared with that of Snort-IDS.

B System architecture and data

The system is composed of a collector, an analyzer, and a manager. The collector collects packets from the high-speed channel, takes on some simple tasks of filtering packets[2], and then sends the filtered packets to the analyzer. The analyzer, which is the kernel of the system, is FDL-IRE in essence. It matches the packets based on its internal FDL-KB. If the matching succeeds, then the corresponding information of the intrusion, including event type and the confidence of the event, is submitted to the manager. The tasks of the manager includes directing responses for intrusions and maintaining the database of intrusion events which contains the concrete information of detected intrusions such as source addresses, destination addresses, events, and etc. The architecture of the system is in Fig. 2.

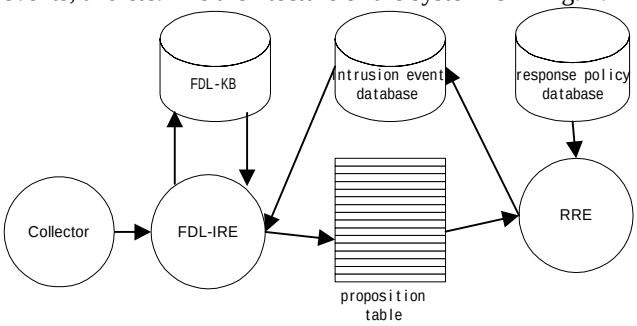

Fig.2 The architecture of FDL-IDS

The Snort-IDS has the similar architecture as above. The differences of them can be concluded as following:

Table 1
The differences of FDL-IDS and Snort-IDS

	FDL-IDS	Snort-IDS
Analyzer	FDL-IRE and FDL-KB	Module for packet match and common rule base,without proposition table
Manager	RRE	Automated response system without the capability to rollback

Additionally, FDL-KB in the initial running period and the rule base of Snort-IDS have the same rules, that is, approximately 600 rules. These rules include buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Many of these rules normally need to be matched by searching the content of a packet, which spends a lot of CPU resource and time. It is these rules that fully show the advantage of fuzzy default rules.

A set of *tcpdump* data is available at http : // iris.cs.uml.edu:8080 / network.html, that is part of an Information Exploration Shootout. The data is used as input of collector in the experiment.

C The work theory of Analyzer

In the experiment, FDL-KB can be divided into two parts. one consists of permanent rules which are expert knowledge in fuzzy default rules form. Another consists of

[2] e.g. to filter packets based on destination port or packet flag.

temporary rules which are produced by data mining in the period of 10 minutes. These temporary rules are mined from intrusion event database by applying RIPPER, and then transformed into fuzzy default rules in the method as chapter Ⅲ. These temporary rules are the key to improve detection speed and sensitivity because only the measures of low class need to be computed.

In the period when the system initially runs,FDL-KB only consists of permanent rules because there aren't recent events in the intrusion event database. Moreover, FDL-IRE needs to compute the confidence of event. So the detection speed of FDL-IDS is a little slower than that of Snort-IDS. But in the following period, the speed of FDL-IRE improves greatly since temporary rules have been produced.

FDL-KB records everything relevant of every intrusion event to proposition table. When following data is added to reason showing the event is misreported, FDL-IRE requires RRE to rollback the response.

D The work theory of RRE

The architecture of RRE is shown as Fig. 3

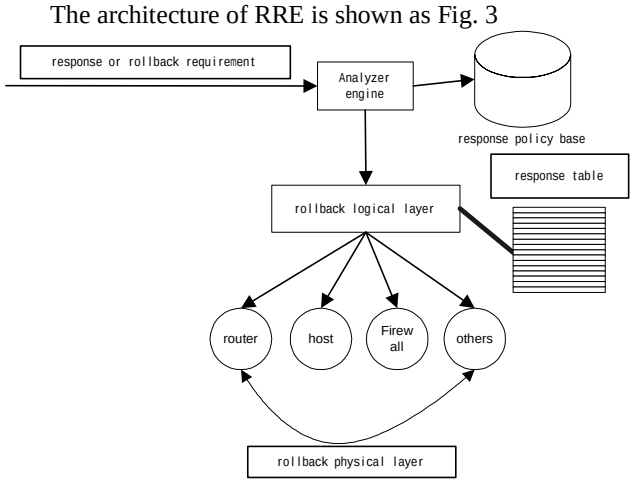

Fig.3 The architecture of RRE

RRE consists of analyzer engine, rollback logical layer and rollback physical layer.

When analyzer engine receives a response requirement, it firstly looks up response policy base for suitable response actions, and then computes the cost of these response actions (including no response) according to chapter Ⅳ. Lastly RRE selects the response action with minimized cost. Anlyzer engine orders rollback logical layer to carry out the response action. In the experiment the set of costs C={*ICost,RCost,DCost,DICost,DRCost*}, the vector of cost weights ω_C=<*1,1,10,10,1*>, which shows that the cost of intrusion damage(including *DCost* and *DICost*) is regarded as more important than the other cost types.

Rollback logical layer maintains a response table, which consists of the fields of eventNo, response equipment and response action etc. When receives requirement to response to an event, it translates the response action into some response script after it records the action to response table, and then orders rollback physical layer to carry out the script. When it receives the requirement to roll back an event, it looks up the response table, translates the undo response actions into rollback script and passes it to rollback physical layer.

Rollback physical layer concretely carries out the response script and response rollback script.

E The results of the experiments

We perform experiments on Collector(Intel ISP4400 server, Redhat 6.2), Analyzer(Intel ISP2150 server, Redhat 6.2) and Manager(Sun Sparc 20, Solaries 7). Intrusion event database adopts SYBASE.

To measure PPS and EPS, we use TCPREPLAY to simulate network traffic as the input of Collector. TCPREPLAY is a tool that can transfert *tcpdump* file to concrete packets. So the performance comparsion is table2:

Table 2
Performance comparsion of FDL-IDS and Snort-IDS

	Initial PPS(M/S)	Initial EPS(M/S)	PPS(M/S)	EPS(M/S)
Snort-IDS	0.21	0.042	0.21	0.042
FDL-IDS	0.167	0.033	3.71	0.72

According to the attack taxonomy of Lee and his idea about cost calculation, on the assumption that the false positive rate of Snort-IDS is 0[3], we design the following process to calculate the cumulative Cost of Snort-IDS and FDL-IDS:

1) the cumulative cost of eveny event in intrusion event database of Snort-IDS is calculated and add together. If the set of intrusion events is E, then

$$CPE_{Snort-IDS} = CumulativeCost(E) \Big/ |E|$$

2) Compared the events of event database of FDL-IDS with that of Snort-IDS. If there is an event not in Snort-IDS but in FDL-IDS, the event is the outcome of false positive to FDL-IDS. If there is an event not in FDL-IDS but in Snort-IDS, the event is the outcome of false negative to FDL-IDS. Additionally, since *DICost* and *DRCost* are difficult to quantify, we invite some experts to decide them.

Table 3
CPE comparison of FDL-IDS and Snort-IDS

	CPE	The rate of response rollback	The rate of still
Snort-IDS	247.73	—	—
FDL-IDS	73.43	5.12%	10.32%

The result showed that PPS and EPS of FDL-IDS greatly increase compared to Snort-IDS. This is because that FDL-IDS needs less proof to draw a conclusion than

[3] Because a detection rule in Snort is assumpted to be precisely descripted a type of intrusion.

Snort-IDS. Moreover, CPE of FDL-IDS is lower than that of Snort-IDS because FDL-IRE only needs first class measures and RRE greatly decreases DRCost. The rate of response rollback means that the rollbacked events accounted for 5.12 percent of all the events. So DRCost to these events decreased. Still means that no response to some events is cost -optimistic.

Ⅵ Conclusion

The current IDSs usually have some problems in the speed and sensitivity of detection. The speed of detection involves the performance of data processing of IDS on high-speed data channels; while the sensitivity involves whether the IDS is capable of recognizing the intrusion plans. The paper discusses on how to improve the reasoning engine of IDS by using the theory of fuzzy default logic, especially to the reasoning engine of expert system of IDS. The experiment shows that the idea is instrumental in improving the detection speed and sensitivity of IDS.

The rollback of responses is another new concept put forward in this paper, and it is mainly for handling the condition when responses of false alarms have been taken. The response itself can also incur damage, such as the damage to users when the server is shut down. So the rollback of responses is indispensable, which can decrease the damage of false responses. The experiment shows that the rollback technique can effectively decrease the cost of IDS.

In the paper, the strategy of comparing the cost of taking responses and the cost of taking no responses is used to decide whether to carry out the responses. The goal of IDS is to achieve maximal security level with minimal cost, which is a trend in the IDS development. In the paper, we set up a cost sensitive model of intrusion detection to direct responses. The advantage of this model lies in that it assigns each cost with a weight, so that it is adaptive in all kinds of environments.

The FDL-IDS is a combination of all the above techniques. Based on the theory of fuzzy default logic and the cost sensitive model to direct responses, this system is made more intelligent.

Ⅶ ACKNOWLEDGMENT

This research is supported by National Natural Science Fundation of China (90104031).

Ⅷ REFERENCES

[1] J. E. Dickerson，J. Juslin，O. Koukousoula，and J. A. Dickerson, “Fuzzy intrusion detection”. In IFSA World Congress and 20th NAFIPS International Conference，2001，3：1506-1510

[2] A. Siraj, S. M. Bridges, and R. B. Vaughn, “Fuzzy congnitive maps for decision support in an intelligent intrusion detection system”. In IFSA World Congress and 20th NAFIPS International Conference，2001，4: 2165-2170

[3] Christopher W. Geib, and Robert P. Goldman, “Plan Recognition in Intrusion Detection System”. In DARPA Information Survivability Conference & Exposition II，2001，1：46-55.

[4] R Reiter, “On Reasoning by Default”.

[5] Curtis A, and Carver Jr, “Intrusion Response Systems: A Survey”, Department of Computer Science，Texas A&M University，2000，Tech Rep.

[6] Wenke Lee, Wei Fan, Matthew Miller, Sal Stolfo and Erez Zadok, “Toward Cost-Sensitive Modeling for Intrusion Detection and Response”, Computer Science Department， North Carolina State University，2000，Tech Rep.