A Network Intrusion Detection Algorithm Based on FSA Model

Fei Wu[1], Donghui WU [2], Yingen Yang [3]

[1]College of Computer Information Engineering, Jangxi Normal University, Nanchang, 330022,China

759908970@qq.com, 952270568@qq.com, 8812453@qq.com

Keywords: Intrusion detection, Finite state automaton, Protocol analysis technology, State transition diagrams, Session list.

Abstract. At present network attack technology is constantly updated,which bring network security workers huge challenges. In view of the fact that the existing intrusion detection technology is difficult to detect multi-step fragmentation attacks, distributed attacks and evading attacks,a network intrusion detection algorithm called FSA algorithm is proposed based on finite state automaton (FSA) model in this paper, and the key implementation technology is analyzed.The state transition diagram is used to illustrate the attack triggering and transfer process,and according to different protocol data,four different mechanisms are designed to detect invasion based on FSA.Experiments show that the algorithm not only can more precisely detect common attacks,but also can detect the unobvious attacks such as distributed and fragment attack very well,which can not be detected by other detection technologies.It is believe that it removes the limitations of the current intrusion detection technology and has an important research and practice value.

1 Introduction

Intrusion detection technology is a key technology in the field of network security, it is a reasonable addition to the firewall technology. Now with network attack techniques constantly updated, invasion means becomes complicated, and it is becoming increasingly difficult to detect. For example, the attacker uses fragmented attacks[1] and coordinated attacks[2] to avoid detection, which leads to not continuing to use the traditional such as pattern matching techniques to detect intrusions. Protocol analysis technique[3] takes the circumstances of attacks having steps, continuity and mobility into account, and automatic machine can describe every detail of attack's trigger and transfer process.Therefore according to the state protocol analysis (SPA) technology, we designed a intrusion detection algorithm based on finite state automaton (FSA) model.

2 Intrusion detection algorithm based on finite automaton

2.1 Proposed and defined for the algorithm

Currently network attacks often carry out with steps and around relevance. According to this feature, the finite state automaton (FSA) detection model is proposed in this paper based on protocol analysis technology.According to different status of network connection and the transfer sequence between the status, the steps and the order of attacks are described.Therefore we propose a new intrusion detection algorithm-FSAA,and some handling mechanisms such as quantity statistics and transfer actions are introduced, thereby it is easily to detect multi-step fragmentation attacks and distributed attacks which is detected difficultly by existing technologies.

To this end firstly the definition of FSA state transition model is given as follows :

Definition 1. FSA state transition model is defined by a six-tuple M = (P, Q, Σ, W, q0, F) where:

P is an protocol shunt collection of the FSA model, which represents a collection of network data protocol type used. Through this you can filter packets,and according to the this shunting purposes is achieved, such as P = {TCP}, it indicates that it is only to allow TCP protocol data flows into the state machine;

Q is a finite set of states FSA model, represents a collection of all possible states under normal protocol operation process;

Σ is the symbol action set of FSA model which triggers state transitions (for example, when P = {TCP}, Σ = {SYN, <SYN, ACK>, ACK});

W: Q × Σ → Q is the state transition function collection which represents the process that M is in the qi-1 state is transferred to the next state qi by symbol action packets' triggering.

q0 is the initial state of FSA model which indicates a request for a first state of the network connection;

F is the end state of FSA model, which is either a normal completion status or can also be connected to the attack completion status.

2.2The key data structures and algorithms handling mechanism

Above model just defines the state transition case of a network connection. In order to detect all connections of the entire network, it is the most key that how to organize the connection information, express state transition model and associate connection information with the state transition model in the algorithm.

2.2.1Network connection list

The paper introduces the concept of 'session' on the basis of the traditional protocol analysis technology which is used to detect intrusion, and the 'session' can be seen as a conversation (i.e. a network connection) between two computers. Any protocol conversation can be made up of a 5tuple[4] (source IP address, destination IP address, source port, destination port, protocol type).The introduction of the session makes detection process no longer take the packet as the unit,while the session is taken as the unit, so as to reduce the system overhead.

Because the session is dynamically created and closed, it is necessary to quickly locate, add and delete connections during the algorithm processing, so this paper uses the linked list structure to organize the session information, shown in Figure 1.

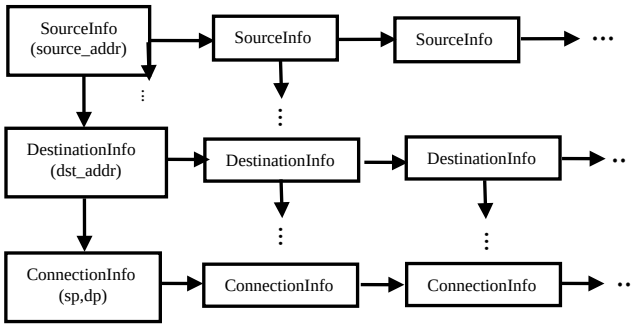

Fig 1. The session linked list

The first layer consists of different source address nodes which form the main chain, and each source address node points to the next source address node in the main linked list and contains a pointer which points to all destination address node list which establishes a session with the source address. In addition each destination node also contains a pointer which point to the session node linked list of port pair, and a port pair correspond to a certain session connection(i.e. The connectionInfo in Figure 1).Therefore many trees are organized into a complex multilayer linked list by means of a main chain, which constitutes the data structure which can organize network session information in the algorithm.

2.2.2State transfer tree

In order to use the FSA model in definition 1 to detect intrusion , this paper use a state transfer tree to describe state transfer mechanism of the detection model, shown in Figure 2.

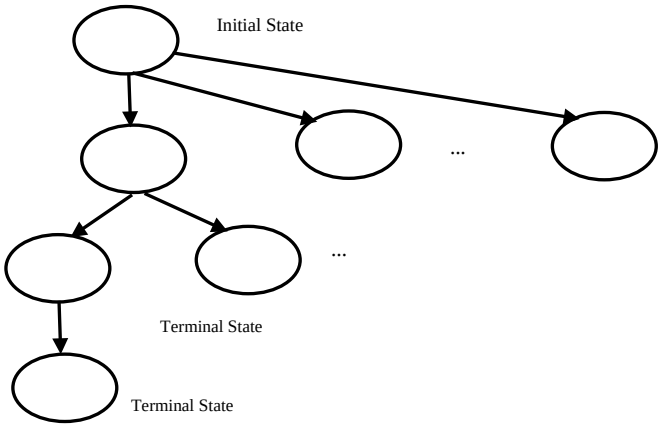

Fig 2. The state transfer tree

State transfer tree of the algorithm corresponds to the state transition diagram (STD)[5] of automaton model in logic structure, and the relationship between the various nodes of the tree reflects the relationship of the status migration which is regulated by the state transfer function of automaton model.

2.2.3 Detection mechanism

In order to detect all sessions within the network,it is necessary to associate session linked list with the information of state transition tree, and this detection mechanism design as shown in Figure 3.

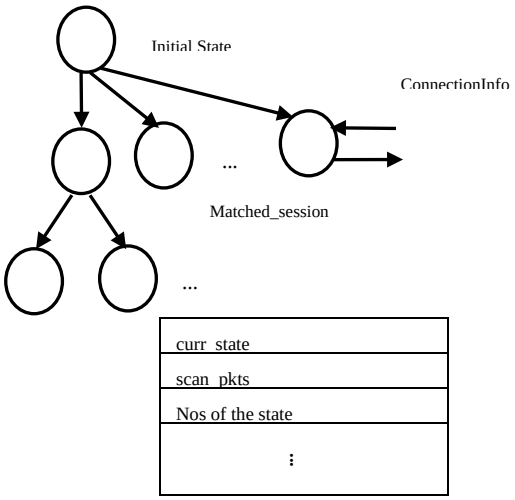

Fig 3. The match of state tree and session list

Each connection information node of the session in figure 1 contains a state node pointer, which points to the node corresponded to the connection of current state in the state tree. Meanwhile each state node in figure 2 contain a pointer list, and each node in the list points to the information node of current session connection in that state. In this way it establishes a two-way track mechanisms between state nodes and the connecting nodes. Each storage linked list corresponded to each state node contains a variety of information about the current state, such as state names, the state in which the number of connections and so on.

According to detection data packets of different protocols, four different detection mechanisms are given as follows :

(1) Source address detection mechanism

Do statistics and estimate that whether the number of scanning ‘scan_cnt’ of source address node in connection node is more than the extremum N1.This mechanism can be used to detect network scanning attacks;

(2) the leaf node detection mechanism

According to the fact that it is necessary to finish the principle of three-way handshake process[6] before establishing TCP connection, the paper gives the stipulation that when the nodes of the state tree located in Σ = <SYN, ACK> state satisfies that the number of half-open connections 'matched_cnt' is more than or equal to the threshold value N2 and the time '| t -t0 |' between the initial state and the current state is less than or equal ΔT, then an alarm is generated. This detection mechanism can be used to detect a variety of attacks based on TCP connection;

(3) transceiver proportional detection mechanism

According to the characteristics that the proportion of UDP packets between sending and receiving of the network interface trends to be stable, we set the stipulation that if the receiving volume to sending volume ratio (Pur / Pus) of UDP packets is more than the threshold N3,then we can determine there are UDP attacks;

(4) ICMP echo request limit detection mechanism

Calculate the amounts of the ICMP packets which are received by the same target host and the alarm is given when the amounts are more than the threshold N4. The common ICMP attacks are ping of death and smurf attack, and they attack the target hosts by sending a high-priority ICMP echo packets, so you can use this mechanism to detect ICMP attacks.

2.3 Detection Algorithm-FSAA

According to the above description of the FSA two key data structures as well as the introduction of the detection mechanism, detection algorithm is given as follows:

Algorithm1.The Intrusion Detection Algorithm based on finite automaton.

```
void FSAA (Packet p) /*put a new capture network packets as input * /
ptrConnNode = FindConnetion (p); /* Find the list in the session if the connection already exists */
If (ptrConnNode == null) /* If the connection does not exist, create a new connection */
  ptrConnNode = New Conn (p);
  ptrConnNode → curr_state = q0;
End If
TransConnState (ptrConnNode, p); /*according to the state transition function W, carry out the session state transition */
If (StateChanggedFlag); /*If the session status have changed */
  AppendToDetectionPkts (ptrConnNode, p); /*the data packet is appended to session detection node list */
End If
Curr_State = pteConnNode → curr_state;
If IsLeaf (Curr_State) /*If the session state to state tree leaf node * /
  Curr_State → match_cnt ++; /* increment the current state counter */
  SrcInfoNode = GetSourceNode (ptrConnNode);
  DstInfoNode = GetDestinationNode (ptrConnNode);
  SrcInfoNode → scan_cnt ++; /* increase the source host scan count */
  DstInfoNode → ICMP echo_cnt ++ /* increase the target host echo packet count */
  Get DstInfoNode → Pur / Pus_cnt /* do statistics for the current state of UDP packet transceiver ratio */
End If
CleanOldConnectin () /* Clear invalid connection */
If (Curr_State→match_cnt> = Curr_State → N2 && |t-t0| <=ΔT OR SrcInfoNode → scan_cnt> = N1 OR Pur/ Pus_cnt> = N3 OR
DstInfoNode → ICMP echo_cnt> = N4)
  alert ();
End If
Return
```

2.4 The key technology

2.4.1 The state transition sequence rule description language

In order to establish the state tree when the algorithm is running, it is necessary to describe different session state transition sequences[7]. This description not only express metastasis relationship between the states, but also describe the trigger conditions needed for the realization of state transition. Therefore, this article designs a kind of scripting language based on BNF[8] and named state sequence description language(StateSDL). It is as follows:

<State description>::=<State name>{<Keyword-Value pair>}|<State name>:<State name>{<Keyword-Value pair>}

<State name>::=any String

<Keyword-Value pair>::=<Keyword>:<Value>|

<Keyword>:<Value>:<Keyword-Value pair>

<Keyword>::=direction|server_ignore|protcol|tcp_flag|flag_mask|threshold|action|msg

<Value>::=String|Number

Above state name uniquely identifies a state, and in order to avoid the appearance of ambiguity when the state tree is parsed, the same state name should not appear in the description file of the same state sequence; when two state names appears in a rule sequentially, it means that the second is the parent state of the first one, and a state can have one parent state at most. The keyword-value pair behind the state describes trigger conditions of the parent state transferring to that state, such as the transmission direction and protocol type of the data,etc.

2.4.2 Clear invalid connections

A network connection is dynamically created and closed, and in order to ensure the accuracy of detection, it is very critical to clear the invalid connections in time. In this article, remove invalid connections when the system meet a predetermined alarm condition and ready to alarm. In practical applications, due to the fact that the frequency of the alarm will not be too high, so this way of cleaning takes low additional load to system.

3 Experiment results and discussion

3.1 Experiment results

The experiment runs at 100Mbps environment of shared LAN, and select a part of the KDD CUP99 data which is provided by DARPA at MIT Lincoln Laboratory in 1999 as the experimental data. The KDD CUP99 divides data records into five parts: Normal, Dos, U2L, Probing and R2L,which is the most comprehensive data set of attack test. The improved snort system with FSA algorithm runs on a host, and the test data set containing part of KDD CUP99 runs on another host as the attacker. Compare the performance of intrusion detection methods based on FSA algorithm, BM algorithm and state protocol analysis(SPA)[9]technology. Test results are as follows.

Table 1 The situation of test data

Data Type	Quantity
Normal	6059
Probe	2692
DoS	5773
U2R	44
R2L	815

Table 2 Detection rate (DR) and false alarm rate (FR) of 3 methods(%)

Methods	FR	DR
BM	11.78	79.94
SPA	8.23	87.72
FSA	6.73	92.51

Table 3 Detection rate of 3 methods to 4 attacks(%)

Methods	Probe	DoS	U2R	R2L
BM	82.32	78.67	21.86	16.57
SPA	89.15	86.65	38.47	22.76
FSA	93.49	92.21	52.78	36.83

3.2 Discussion

The experimental results shows that the intrusion detection algorithm based on FSA model proposed by this paper has superior performance than based on SPA and BM algorithm in terms of the detection rate and the false alarm rate, especially for the detection of the Probe and DoS attacks.

However ,although the FSA algorithm has better detection performance than other algorithms about detection U2R and R2L attacks, the detection rate and the false alarm rate are unsatisfactory. It is because the FSA algorithm describes the mechanisms about Probe and DoS more than other two attacks.

4Conclusion

In order to describe the trigger and transfer process of attacks, and detect network attacks accurately and in real-time, this paper presents an intrusion detection algorithm based on automaton state transition analysis (i.e. FSA model), and some key problems of system implementation are discussed. Experiment proved that the detection mechanism based on the FSA model and algorithm improves the efficiency of the intrusion detection also reduces the rate of false positives.

Acknowledgments

First and foremost, I would like to show my deepest gratitude to my supervisor, Mr Yang, a respectable, responsible and resourceful scholar,who has provided me with valuable guidance and help during the study.

Afterwards, I want to thanks my alma mater.Thank her for providing me experimental environment and support.

Next, I would like to thank the experts for reviewing.

Finally, be grateful to my dear parents.

References

[1] Singh, R.,Kumar, H. and Singla, RK., A Reference Dataset for Network Traffic Activity Based Intrusion Detection System[J].International Journal of Computers Communications & Control, 2015,10(3):390-402.

[2] Cat Catania, Carlos A., and Garcia Garino, Carlos. Automatic Network Intrusion Detection: Current Techniques and Open Issues[J].Computers & Electrical Engineering, 2012,38(5):1062-107.

[3] Liu,Bing. Protocol Analysis and Packets Capturing Technology[C].2012 International Conference on Intelligence Science and Information Engineering, 2012,20:141-144.

[4] Bul'ajoul, Waleed. and James, Anne.,Improving Network Intrusion Detection System Performance Through Quality of Service Configuration and Parallel Technology[J].Journal of Computer and System Sciences.2014,81(6):981-999.

[5] Schuster, Franka and Paul, Andreas. A Distributed Intrusion Detection System for Industrial Automation Networks[C].2012 IEEE 17th Conference on Emerging Technologies & Factory Automation (ETFA),2012.

[6] Wang G, and Hao J and MaJ, et al,A New Approach to Intrusion Detection by Machine Artifical Neural Networks and Fuzzy Clustering [J].Expert Systems with Applications,2010,37(9):6225-6232.

[7] Garcia, K.A.,and Monroy,R.et al,Analyzing Log Files for Postmortem Intrusion detection [J].IEEE Transactions on Information Theory, 2012, 42(6):1690-1704.

[8] Wright J, and Yang A Y,and Ganesh A, et al,Robust Face Recognition via Sparse Representation[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2009, 31(2): 210-227.

[9] Zhi, Zhang.IPv6 Network Intrusion Detection Protocol Analysis Techniques[C]. Proceedings of the 2012 International Conference of Modern Computer Science and Applications,2013,191:89-94.