2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

Early Warning System for DDoS Attacking Based on Multilayer Deployment of Time Delay Neural Network

Chang-Lung Tsai[1] Allen Y. Chang[1]
[1]Department of Computer Science
Chinese Culture University
Taipei, Taiwan, 11114, R.O.C.
ccl3@faculty.pccu.edu.tw zyh3@faculty.pccu.edu.tw

Huang Ming-Szu[2]
[2]Graduate Institute of Information Management
Chinese Culture University
Taipei, Taiwan, 11114, R.O.C
vickymail@gmail.com

Abstract—**Distributed denial of service (DDoS) is one of the most persecution network attack techniques to be confronted in recent years. From the definition of DDoS, thousands of network attacks must initiate simultaneously and continuously to achieve a successful DDoS attacking. Therefore, almost all of the information system cannot survive as they confront the DDoS attacks. Although there are a lot of intrusion detection system (IDS) developed, preventing DDoS attack is still difficult and perplexing. In this paper, an early warning system for detecting DDoS attacking has been mounted to a traditional IDS to form a completely system. This early warning system is developed based on the rationale of time delay neural network. In the networking topology, each node is monitored with the deployment of detectors to establish a multilayer architecture. In addition, the activities of each node will be monitored by their neighboring nodes to check whether it is still survival or not mutually. After then, all of the attacking information will be collected and transferred to the expert module for integrating analysis. As those nodes dispatched on the DMZ or between the first and second layer of firewall face some attacking similar as the pattern of DDoS, the kernel expert module which dispatched behind the second firewall will take some feasible actions and initiate the defense strategies to protect the kernel information system. In the meanwhile, those failed nodes will be restarted and act as the role of vanguard to assure the networking under normal operation.**

Keywords-Information security, Time-delay neural network, Denial of service, Distributed denial of service, Internet hacking

I. INTRODUCTION *(HEADING 1)*

The service of cloud computing, Internet and wireless networking emerging, millions of information security events occurred. Moreover, the perplexity of information security problem becomes more complicated and difficult to process. Currently, almost all of the networking system has been deployed with a lot of security hardware or software such as traffic monitors and filters, firewall, antivirus, antispyware, intrusion detection systems, intrusion prevention systems, and etc. However, thousands of network hacking have happened every day. Not only billions of general documents are sniffed or even stolen every day, but also those confidential parameters, classified files and with authorized database are under significant threaten of access and cracking. Unfortunately, currently no one or institute can predict that when will the intruders stop their network hacking.

To solve the knotty information security problem, a lot of techniques are developed from the viewpoint of end point protection, network security, access authentication, data protection, web application, and etc. In addition, a number of different mechanism of intrusion detection system (IDS) such as network based, hosted base, protocol based, and application based IDS and intrusion prevention system (IPS) are developed [1] [2] [3]. However, the detection of DoS and DDoS network attacking is quiet complicated. Although there are some different types of DoS attacking which can be categorized from their initiating feature such as TCP SYN, ICMP, and etc. However, as hackers feed false data to IDS, it is hard to detect the initiation of attacking.

The implementation of IDS is to identify networking attack based on the distinguishing of attacking features. In [4], Chen et al. proposed a mechanism based on particle swarm optimization algorithm (PSO) and radial basis function (RBF) neural network to detect the networking intrusion. In [5], Alim et al. regarding the detection procedure merely and adopted the architecture of recurrent neural network (RNN) to classify those attacking patterns. The output detecting results are shown in posteriori probability forms. After then, the suitable actions are taken based on their corresponding probability. However, how to define an optimal reaction is still under research.

In this paper, an early warning system based on multilayer deployment of time delay neural network for anti-DDoS attacking is proposed. The goal of the TDNN early warning system is to prevent the networking and information system from paralysis.

II. CHARACTERISTIC OF DDOS ATTACKING

There are a lot of IT security threats. The Top 10 items on the list are malware, cracker, insider, system vulnerability, multimedia, application and service of cloud computing, zombie computer, social network engineering, zero time difference attacking, unknown attacking, and spoofing attacking. Among those network attacking methods, the goal of DoS or DDoS attacking is to paralyze the information system.

All of the networking attacks possess their corresponding characteristics. The signature based IDS is

978-0-7695-4222-5/10 $26.00 © 2010 IEEE
DOI 10.1109/IIHMSP.2010.178

performed just based on this theorem. In the following, some characteristics of initiated a DoS or DDoS attacking is listed:

1) Preparation phase: Before the initiation of a DDoS attacking, thousands of zombie computers and proxies had to be prepared. In addition, the vuneralbility of the target networking system must be reconnaissanced.

2) Attacking phase:

a) Large volume of flow will be overwhelmed on the target host or networking server.

b) The User IP that used for attacking might be spoofed. Thus, to identify the source of a network attacking might be very difficult.

c) The packets that forward from the same source IP might possess lower volume that could not effectively to distingush whether the packet is belonged to normal or harmful request. Therefore, if the detecting is based on single sensor, the IDS might not perform with sufficient satisfcation due to high positive and high negative rates.

d) Most of the network attacking approaches or tools that could be obtained freely from Internet always possess special signatures that can be easily detected and analyzed through IDS. Therefore, some techniques of evading the detection from IDS might be adopted to initiate an attacking.

3) Covert phase: After attacking, most of the hackers will try to hide their attacking trail and cleaning or omit the attacking records. In addition, revisit channel might be also established. However, the goal of DoS or DDoS attacking is to paralyze the information and network system. Therefore, the adopted covert techniques will be focused on anti-tracking, i.e., stay in concealment and without any information leakage of the source of attacking.

As one well comprehend the special features of DoS and DDoS attacking, onhe then can develop an optimal prevention system to against the network attacking.

III. Early Warning System for DDoS Attacking

To protect the information system from DoS or DDoS attacking, some detection mechanism are proposed such as based on the analysis of intruder activity and attack approaches, content classification of header, statistical and spectral analysis, and etc. Moreover, some institute might adopt central management with associated distributed defense systems to detect and prevent from DDoS attacking.

A. Rationale of Time-Delay Neural Network

Time-delay neural network (TDNN) is a kind of neural network that the time factor is hidden inside the signal with implicit representation. As a physical process, all of the factors of the recent pre-state that will influence the output result in current state will be treated as input signal. Therefore, the timing relationship of pre-state and prostate can be mapping by those signal of data structure. As for TDNN, there are two kind of architecture. One is multilayer perception which is belonged to feed-forward architecture. Another is utilized the rationale of error back propagation to learning and mapping the static relationship between input and output parameters. In which, the concept of static is belonging to stationary processes which means that the relationship between input and output will not change with timing factor.

The reason that the TDNN has been adopted for early alert to against DDoS attacking in the paper is because an initiation of DDoS attacking to be performed must trigger a lot of zombies or proxies that have been setting up in advanced. Besides, before initiate a real attacking, some reconnaissance must be performed. Therefore, all of the related features that collected in different timing must be integrated for associated analysis.

B. Strategy for anti-DDoS attacking

Some rationale for detecting the DoS and DDoS attack have been proposed, such as entropy based detection [6], statistical and UNN based detection [5], and etc. However, as the networking technique emerging, the hacking techniques and strategies innovated quickly. In the following, a multilayer defense mechanism for DDoS has been proposed as the following. In which some modules are included such as:

1) Sync cookie module: provide to against DoS attacking based on TCP SYN flooding.

2) Multilayer defense agents: which can be performed by rule based or IP based and deployed on each nodes or critical nodes.

3) Sniffer Module: support on-line sniffing to monitor all of the possible anomaly activity and traffic packets.

4) Flow control module: provide the control of data rate for packet transmmision, the establishment of new session and control of concurrent session.

5) Black list module: establish black list and white list for filtering. Although the black list is not the major filtering of network attacking due to thousands of items on the list will deplete the resource, performing pattern matching for those critical features of attacking is still a must. Besides, to ensure the access for those authorized users, white list is the most convinient approach to quickly verify the identification and provide the corresponding access area.

6) Flexible schedule module: provide periodic and inperiodic schedule for system inspection to ensure the whole network is under normal operation.

7) Expert module: in the module, the primary responsibility is to offer the detecting results of all possible network attacking including the DoS and DDoS attacking. In which, the traffic monitoring results, statistical results of IP based, session based, rule based, data rate, and etc. must be recorded on the report. In addition, a report combining properly action against attacking has to be generated after the integrated analysis, i.e., some proposal generated by expert system has to be shown on the report concurrently.

The goal of anti-DDoS attacking is to protect the information and networking system such as mail servers, database servers, and Http servers from paralyzed and ensure the decrease of depletion of bandwidth and decrease the consumption of resource of servers, i.e., providing the assurance of normal operation under DDoS attacking. Moreover, the traffic management system had better provide the capability of suppress those application based on P2P.

C. Proposal for traffic management

The suggestion for traffic management is listed as the following:

1) The system must provide sufficient and satisfied techniques of pattern recognition.

2) The system must possess function of branch-labelling for flow control.

3) The system must offer multi-gateway routing and multi-ISP routing.

4) The system had better possess independent flow management module, independent flow control strategy and scheduling function.

5) Offer flow control on different layers such as at the interface of Internet, mail server, P2P, and ERP, the address and user group, or even on each IP.

6) Managemenet of Bandwidth and Quota and the limitation of supporting bandwidth, static and dynamic bandwidth assurrance.

7) The deployment of traffic managemnet system had better be located close to the client side.

8) Management of user ID and IP based on authentication, authorization, and accounting [7].

9) The stratey of combining the flow rejection and flow managemnet techniques.

10) Restrict to P2P communication.

11) Provide the capability of real time flow statistic and sorting.

The procedure for traffic process is shown in Figure 2.

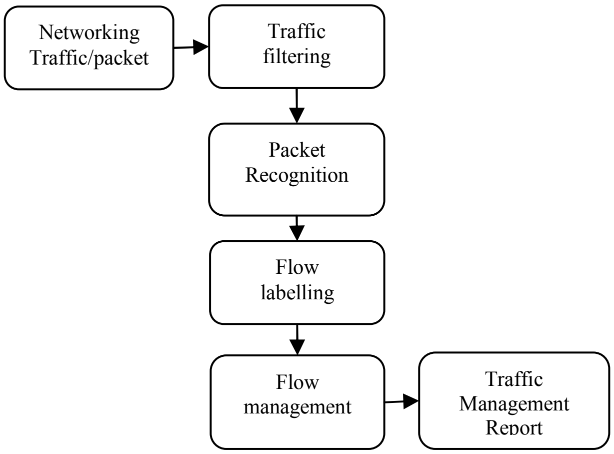


Figure 1. Traffic process and management procedure.

D. The proposed early warning system

The experimental architecture is established based on the rationale of centralized management with multi-distributed monitor agents. Each node of the network will be dispatched with a sensor to collect the traffic information and the distributed monitoring agents will collect all of the associated information from their connected nodes. After then, the whole recorded information that collected by all of the monitoring agents will be transferred to the expert system for integrated analysis.

In the early warning system, those deployed nodes will collect and transfer a sequential record of information based on a defined time units. After then, all of the timing based information will be trained by a time-delay neural network as shown in Figure 2.

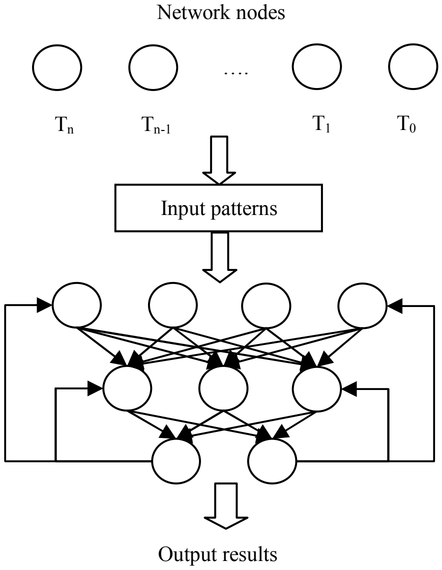


Figure 2. Illustrating of relationship between input patterns based on different timing and the proposed TDNN architecture.

The sensors that mounted on network nodes are dispatched as shown in Figure 3. In which, as the sensors that dispatched on the DMZ which is the first layer of the network confronted DoS or DDoS attcking, those collected information will be transferred to expert system in order to take properly actions to against the attacking. Within the Intranet, second layer of time-delay neural network is deployed to collected those penetrated DoS or DDoS attacking or network attacking which is initiated from insiders. In the proposed architecture, as the first layer of TDNN sensors collected DoS or DDoS attacking signal, the protection mechanism of the second layer that located inside the Intranet will be enhaced. One of the sniffed packets is shown in Figure 4.

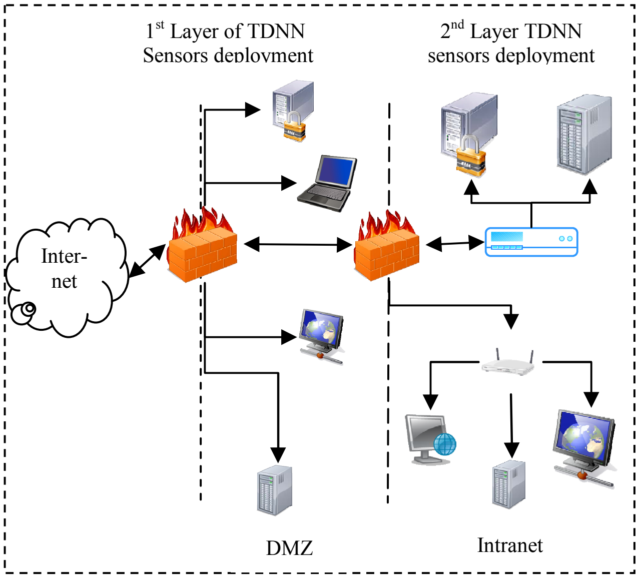
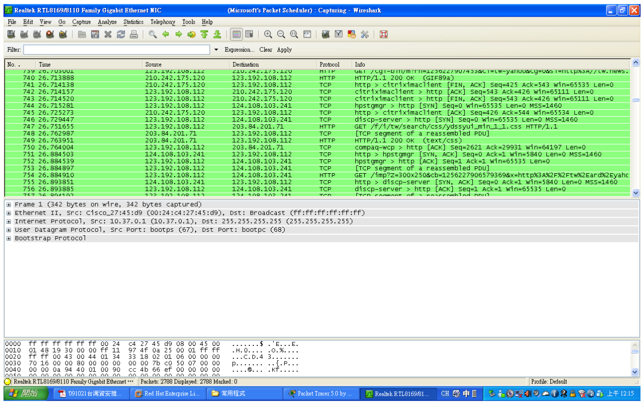


Figure 3. Illustrating the networking topology and the TDNN deployment architecture.



```
Realtek RTL8169/8110 Family Gigabit Ethernet NIC        (Microsoft's Packet Scheduler) : Capturing - Wireshark
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Tools  Help
Filter:                                   Expression...  Clear  Apply
No. .  Time          Source            Destination       Protocol  Info
  739 26.703001      123.192.108.112   210.242.175.120   HTTP      GET /cgi-bin/m?rn=1256227907453&ct=tw-yahoo&cg=0&s1=http%3A//tw.news.
  740 26.713888      210.242.175.120   123.192.108.112   HTTP      HTTP/1.1 200 OK  (GIF89a)
  741 26.714138      210.242.175.120   123.192.108.112   TCP       http > citriximaclient [FIN, ACK] Seq=425 Ack=543 Win=65535 Len=0
  742 26.714157      123.192.108.112   210.242.175.120   TCP       citriximaclient > http [ACK] Seq=543 Ack=426 Win=65111 Len=0
  743 26.714520      123.192.108.112   210.242.175.120   TCP       citriximaclient > http [FIN, ACK] Seq=543 Ack=426 Win=65111 Len=0
  744 26.715281      123.192.108.112   124.108.103.241   TCP       hpstgmgr > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
  745 26.725273      210.242.175.120   123.192.108.112   TCP       http > citriximaclient [ACK] Seq=426 Ack=544 Win=65534 Len=0
  746 26.729447      123.192.108.112   124.108.103.241   TCP       discp-server > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
  747 26.751655      123.192.108.112   203.84.201.71     HTTP      GET /f/i/tw/search/css/ydssyui_min_1_1.css HTTP/1.1
  748 26.762987      203.84.201.71     123.192.108.112   TCP       [TCP segment of a reassembled PDU]
  749 26.763951      203.84.201.71     123.192.108.112   HTTP      HTTP/1.1 200 OK  (text/css)
  750 26.764004      123.192.108.112   203.84.201.71     TCP       compaq-wcp > http [ACK] Seq=2621 Ack=29931 Win=64197 Len=0
  751 26.884503      124.108.103.241   123.192.108.112   TCP       http > hpstgmgr [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
  752 26.884539      123.192.108.112   124.108.103.241   TCP       hpstgmgr > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  753 26.884897      123.192.108.112   124.108.103.241   TCP       [TCP segment of a reassembled PDU]
  754 26.884910      123.192.108.112   124.108.103.241   HTTP      GET /imp?Z=300x250&cb=1256227906579369&x=http%3A%2F%2Ftw%2Eard%2Eyahc
  755 26.893851      124.108.103.241   123.192.108.112   TCP       http > discp-server [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
  756 26.893885      123.192.108.112   124.108.103.241   TCP       discp-server > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  757 26.894192      123.192.108.112   124.108.103.241   TCP       [TCP segment of a reassembled PDU]

⊞ Frame 1 (342 bytes on wire, 342 bytes captured)
⊞ Ethernet II, Src: Cisco_27:45:d9 (00:24:c4:27:45:d9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 10.37.0.1 (10.37.0.1), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊞ Bootstrap Protocol

0000  ff ff ff ff ff ff 00 24  c4 27 45 d9 08 00 45 00   .......$ .'E...E.
0010  01 48 19 30 00 00 ff 11  97 4f 0a 25 00 01 ff ff   .H.0.... .O.%....
0020  ff ff 00 43 00 44 01 34  33 18 02 01 06 00 00 00   ...C.D.4 3.......
0030  70 16 00 00 80 00 00 00  00 00 7b c0 50 07 00 00   p....... ..{.P...
0040  00 00 0a 94 40 01 00 90  cc 4b 66 ef 00 00 00 00   ....@... .Kf.....

Realtek RTL8169/8110 Family Gigabit Ethernet ···   Packets: 2788 Displayed: 2788 Marked: 0   Profile: Default
開始   091021台灣資安推...   Red Hat Enterprise Li...   常用程式   Packet Tracer 5.0 by ...   Realtek RTL8169/81...   CH   中   上午 12:15
```

Figure 4. Illustrating of packet sniff.

TABLE I. Statistical Detection Result of DDoS Attacking

Kind	*General IDS*	*Proposed early warning system*
Correct detect rate	46.3%	82.7%

The detecting result is tabulated as shown in Table I. In which, the rate for a general IDS to sucessfully detect the DDoS attacking is about 46.3%. As to our proposed early warning system, the rate for sucessfully detecting the DDoS attacking is about 82.7%.

IV. CONCLUSION

In the paper, an early warning system based on multilayer deployment of time delay neural network for anti-DDoS attacking is developed. In the networking topology, each node is monitored with the deployment of detectors to establish a multilayer architecture. In addition, the activities of each node will be monitored by their neighboring nodes to check whether it is still survival or not mutually. After then, all of the attacking information will be collected and transferred to the expert module for integrating analysis. As those nodes dispatched on the DMZ or between the first and second layer of firewall face some attacking similar as the pattern of DDoS, the kernel expert module which dispatched behind the second firewall will take some suitable actions and initiate the defense strategies to protect the kernel information system. In the meanwhile, those failed nodes will be restarted and act as the role of vanguard to assure the networking under normal operation.

ACKNOWLEDGMENT

The research is sponsored by National Science Council of Taiwan and Chinese Culture University.

REFERENCES

[1] K. K Gupta, B. Nath, and R. Kotagiri,“Layered Approach Using Conditional Random Fields for Intrusion Detection,” IEEE Transactions on Dependable and Secure Computing, Vol. 7, No. 1, pp. 35-49, Jan 2010.

[2] G. G. Mohammad, M. Reza, and S. Y. Hadi, “Intrusion Detection by New Data Description Method,” 2010 International Conference on Intelligent Systems, Modeling and Simulation, pp. 1-5, 2010.

[3] M. A. Pérez del Pino, P. García Báez, P. Fernández López, and C. P. Suárez Araújo, “Towards Self-Organizing Maps based Computational Intelligent System for Denial of Service Attacks Detection”, INES 2010, 14th International Conference on Intelligent Engineering Systems, pp. 151-157, Spain, May 5–7, 2010

[4] Z. F. Chen, P. D. Qian and Z. F. Chen, “Application of PSO-RBF Neural Network in Network Intrusion Detection”, 2009 3rd International Symposium on Intelligent Information Technology Application, pp.362-364, 2009

[5] RFC 5637 Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6, http://www.faqs.org/rfcs/rfc5637.html, Access on Jul 15, 2010.

[6] A. B. M. Alim, AI Islam, and Tishna Sabrina, “Detection of various Denial of Service and Distributed Denial of Service Attacks using RNN Ensemble”, Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009), Bangladesh, pp.603-608, 21-23 December, 2009.

[7] Y. Gu, A. McCallum, D. Towsley, “Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation”, Internet Measurement Conference, 2005.