ISSN 2047-3338

Network Intrusion Detection System Using KMP Pattern Matching Algorithm

B. Raju[1] and B. Srinivas[2]
[1,2]Kakatiya Institute of Technology and Science, Warangal, India
raju.nestham@gmail.com, srinu1032@gmail.com

***Abstract*– Intrusion detection technology can help the system to deal with network attacks extend the security management ability of the system manager and increase the integrality of information security foundation structure. Intrusion detection system (IDS) is a device (or application) that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Pattern matching algorithm is the core algorithm of intrusion detection system based on feature matching as well as an algorithm which is universally used in current intrusion detection equipment. An implementation of design intrusion detection system based on pattern matching algorithm is proposed in this paper. Apart from the intrusion detection system, the paper has given a detailed case study on different modules used for finding the Intrusion Detection System.**

***Index Terms*– Intrusion Detection, KMP Pattern Matching Algorithm and Data Acquisition Module**

I. INTRODUCTION

NOWADAYS, due to limitations of computer network and vulnerability of information system, hardware resources, communication resources, software and information resources on computer network system are damaged, altered and leaked or their functions are invalid for foreseeable, unpredictable or baleful reasons, which make the information system become abnormal and even lead to system collapse and paralysis, thereby causing enormous economic losses [2]. A great deal of practice has proved that as a newly emerging security technology, it is not enough for intrusion detection to ensure the security of network system only depending on traditional passive protection and a complete security strategy should include real-time detection and fast response.

An intrusion detection system (IDS) is a device (or application) that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents [2].

A. Definitions IDS

Intrusions: attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer system or network (illegal access). Intrusions have many causes, such as malware (worms, spyware, etc…); attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized [7].

Intrusion detection: is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *intrusions (incidents).*

Intrusion detection system (IDS): is software that automates the intrusion detection process. The primary responsibility of an ID is to detect unwanted and malicious activities. Intrusion detection data is obtained through the analysis of the host system log and network data packets, so the module can be divided into host-based intrusion detection module and network-based intrusion detection module two parts [7].

Intrusion prevention *system (IPS)*: is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Basically there are two primary types of IDS: *A Network Intrusion Detection system (NIDS)* transparently monitors network traffic, looking for patterns indicative of an attack on a computer or network device. By examining the network traffic, a network based intrusion detection system can detect suspicious activity such as a port scan or Denial of Service (DOS) attacks. *Host Intrusion Detection System (HIDS)* component is made up of two parts: a centralised manager and a server agent. The manager is used to administer and store policies, download policies to agents and store information received by agents. The agent is installed onto each server and registered with the manager. Agents use policies to detect and respond to specific events and attacks. An example of a policy would be an agent that sends an SNMP trap when three concurrent logins as root have failed on a UNIX server. The working of Intrusion Detection System is shown in Fig. 1.

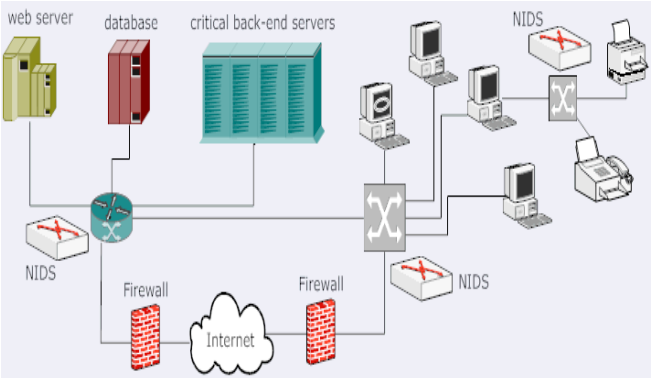


Fig. 1: NIDS in complete deployment mode

II. GENERAL DESIGN OF SYSTEM

The General Infrastructure Design of IDS is shown as Fig. 2, data acquisition module is responsible for capturing various types of hardware frames from network flow and handing these hardware frames to data pretreatment module and then the data pretreatment module strips off hardware frame heads and checks the integrity of messages, after that, according to the application protocols messages belong to, these hardware frames are sent to response protocol analyzing and processing modules respectively [1]. Various protocol processing modules make corresponding treatments according to concrete protocols, for example, TELNET protocol has a process of packet. After that, feature pattern matching starts to judge if the intrusion occurs. If the intrusion is found, the intrusion response module will respond timely, give an alarm, cut off the connection and record the attack log; otherwise, it will make a detailed record of protocol operation log. Firewalls are designed to check the IP packet header information and not the payload portion of the IP packet. But IDS will check the payload of the packet to determine if the pattern of data held within, matches that of a known attack signature.

IDS will check the payload of the packet to determine if the pattern of data held within, matches that of a known attack signature. The benefits of the above information are Instance of attack, Method of attack, Source of attack, Signature of attack.

NIDS is deployed such that it monitors the traffic that traverses any given link within the network, thereby providing an increased security .Thus the NIDS is deployed near the switching nodes within the local network, and near the access routers at the network boundary. In such configurations, the NIDS will no longer monitor the traffic that has been blocked by the firewall, which will lead to a much reduced false alarm rates. A drawback however is that there will be multiple instances of NIDS, and it will become tedious to keep all of them up-to-date in say a large enterprise network. Such configurations are popular in ecommerce back end networks, consisting of web and mail servers and database and storage servers, as an increased security is desirable there. It also aids in keeping an infected server to infect the others within the network.

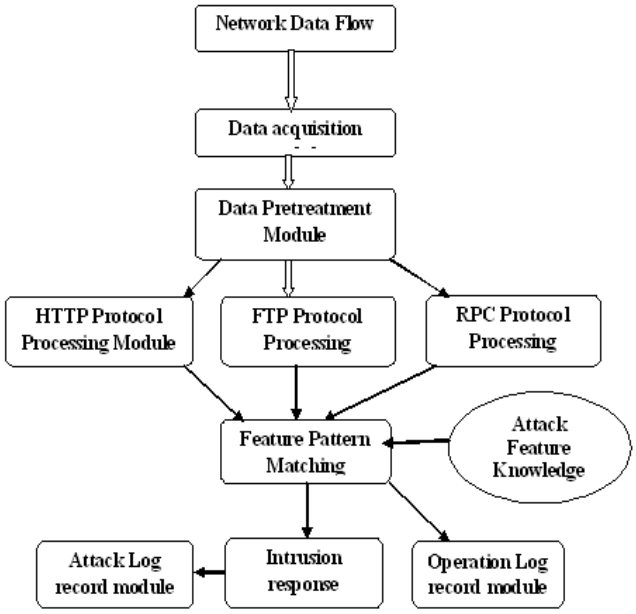


Fig. 2: Infrastructure of IDS

III. DESIGN SPECIFICATION OF SEVERAL MODULES

A. Data Acquisition Module

Data acquisition module can collect data packets in three ways, namely adopting shared concentrator, switch port mirror image and monitoring interface box. If data acquisition module wants to monitor the data which flow through the network card but don't belong to its own host, it must round the processing mechanism when the system works normally and access to the network bottom layer directly. First, set the working mode of network card as promiscuous mode to make it receive data packets on target MAC address not its own MAC address and then access to the data link layer directly to capture relevant data, the data should be filtered by application program not upper layers, such as IP layer and TCP layer, etc, in this way, all the data which flow through the network card can be monitored [1]. Data acquisition module is composed of three parts, namely a data packet audio monitor driver, a low class dynamic link library and a high class static link library.

B. Protocol Processing Module

In this Module all sub-modules aiming at concrete protocol processing: HTTP, FTP, TELNET, POP3, SMTP, IMAP protocol processing module. Some simple intrusion behaviors can be judged in the protocol processing module. Take FTP protocol processing module as an example, after receiving FTP protocol messages, first carry out the heat preservation integrity judgment and then FTP computing operations and parameter lengths can be defined by the user, which can be regarded as FTP long buffering overflow attack. An alarm signal is generated directly to be sent to the attack log record module and intrusion response module, it's unnecessary to continue to hand the alarm signal to the attack feature pattern matching module, which not only enhances the real-time

performance of intrusion detection system but also reduces the resource burdens of using attack feature matching pattern to detect intrusion behaviors.

C. Pattern Matching Module

After the dynamic organization and analysis of rules and data package processing by package capture and analysis module and preprocessor are finished, the detection engine is called to carry out the real-time matching of data packages and rules. Detection function Detect () will use corresponding rule chain lists to check current packages according to different protocols [1].

Here in this dynamic analysis Knuth, Morris and Pratt (KMP) proposed a linear time algorithm for the string matching problem Pattern matching Algorithm is proposed in this paper. Pattern Matching Algorithm [3] is the core algorithm of Intrusion Detection System based on Feature Matching which is used in current intrusion detection equipment. A matching time of O(n) is achieved by avoiding comparisons with elements of 'S' that have previously been involved in comparison with some element of the pattern 'p' to be matched. i.e., backtracking on the string 'S' never occurs.

The prefix function, Π: The prefix function, Π for a pattern encapsulates knowledge about how the pattern matches against shifts of itself. This information can be used to avoid useless shifts of the pattern 'p'. In other words, this enables avoiding backtracking on the string 'S'.

The KMP Matcher: With string 'S', pattern 'p' and prefix function 'Π' as inputs, finds the occurrence of 'p' in 'S' and returns the number of shifts of 'p' after which occurrence is found.

In the matching process, you can use the pattern matching algorithm to match from low appearance probability to high appearance probability of letters in the pattern string in natural English. When a feature matches rules with Content keywords with payloads of data packages, it must call a pattern matching plug-in, this plug-in will use efficient pattern matching algorithms to match payloads of data packages to find potential intrusions. Finally, an output processing plug-in is called according to detection results to log data packages according to the mode set in advance and call concrete processing functions for intrusion behaviors or give an alarm signal.

The KMP Matcher, with pattern 'p', string 'S' and prefix function 'Π' as input, finds a match of p in S. Here is the pseudocode computation for KMP algorithm:

KMP-Matcher (S, p)

```
1 n ← length [S]
2 m ← length [p]
3 Π ← Compute-Prefix-Function (p)
4 q ← 0                    //number of characters matched
5 for i ← 1 to n           //scan S from left to right
6     do while q > 0 and p [q+1]! = S[i]
7           do  q ← Π [q]     //next character does not match
8               if p [q+1] = S[i]
9           then q ← q + 1    //next character matches
10              if q = m      //is all of p matched?
11          then print "Pattern occurs with shift" i – m
12              q ← Π [q]     // look for the next match
```

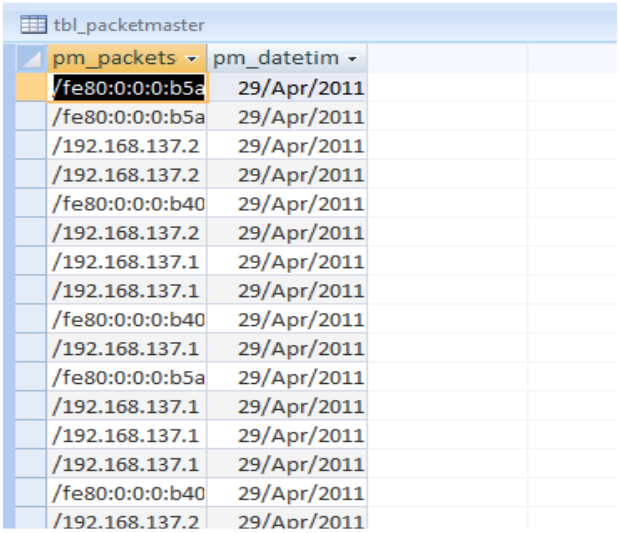
Pseudo-code computation for the prefix function, Π:

Compute-Prefix-Function (p)

```
1 m ← length [p]              //'p' pattern to be matched
2 Π [1] ← 0
3 k ← 0
4         for q ← 2 to m
5           do while k > 0 and p [k+1] != p[q]
6              do k ← Π [k]
7                  If p [k+1] = p [q]
8                   then k ← k +1
9                  Π [q] ← k
10    return Π
```

D. Log Record Module

The log record of intrusion detection system based on attack feature pattern matching can be divided into two types, namely attack log record and protocol operation log record. Attack log record provides essential information for the network manager after intrusion events occur. Protocol operation log record provides a set of comprehensive, operating system-independent and searchable log record, which can be used to audit and trace intrusion behaviors afterwards. Shown as Fig 3, when protocol processing module deals with corresponding protocol messages respectively, if an intrusion behavior is found, it will directly calls the attack log record module to make an attack log record; if no intrusion behavior is found, it calls the protocol operation log record module to make a normal protocol operation log record. Similarly, when attack feature pattern matching module is matched to a certain attack feature, it will also call the attack log record module.


tbl_packetmaster

pm_packets	pm_datetim
/fe80:0:0:0:b5a	29/Apr/2011
/fe80:0:0:0:b5a	29/Apr/2011
/192.168.137.2	29/Apr/2011
/192.168.137.2	29/Apr/2011
/fe80:0:0:0:b40	29/Apr/2011
/192.168.137.2	29/Apr/2011
/192.168.137.1	29/Apr/2011
/192.168.137.1	29/Apr/2011
/fe80:0:0:0:b40	29/Apr/2011
/192.168.137.1	29/Apr/2011
/fe80:0:0:0:b5a	29/Apr/2011
/192.168.137.1	29/Apr/2011
/192.168.137.1	29/Apr/2011
/192.168.137.1	29/Apr/2011
/fe80:0:0:0:b40	29/Apr/2011
/192.168.137.2	29/Apr/2011

Fig. 3: Log Record

1) Attack log record: Attack log record module is used to record the necessary information of intrusion behaviors detected by intrusion detection system. A complete attack log record should include the information as; Occurrence time of intrusion behavior, Source address of intruder, Source port used by intruder, Destination address of intrusion, Objective of intrusion, Name of port attack feature pattern.

2) Protocol operation log record: Protocol operation log record module is a set of comprehensive and open service protocol-oriented operation log record independent of the log record of protected host, which provides detailed network or host access information for the system manager and can be used to trace the source of intruder or the intrusion detection system based on audit, it is independent of the log record of server itself, and therefore even though a practiced hacker dodges the detection of intrusion detection system, intrudes into the network or host and clears away the logs in the intruded server, the network manager can still find his whereabouts from the operation log record of intrusion detection system. For example RPC protocol is as follows: Remote program number, remote program version, remote procedure number, mapping program number and mapping program version.

E. Intrusion Response Module

Intrusion response module gives corresponding responses for verified intrusion behaviors, including static measures, for example, record attack data, store captured data, send emails and messages to the manager, it can also take some active dynamic preventive measures, cut off the intruded connection and modify the access control of router, for instance. It mainly includes patrol agent and host mobile agent two types [7]. The former is to carry out host behavior detection and response, and the latter is mainly to respond to the invasion information in the intrusion detection module and report the invasion logs to the control server, as well as store in the database. The system is only to achieve log storage, and the database storage will be achieved until the system expansion and improvement. Generally, the system mainly includes three very important functions [1], namely Alert () function is to give real-time warning of intrusion behaviors, logtoTable() is to set up a log of high danger class intrusion behaviors in database and TraceInstrusion is to trace and take evidence of intrusion behaviors if it proves necessary.

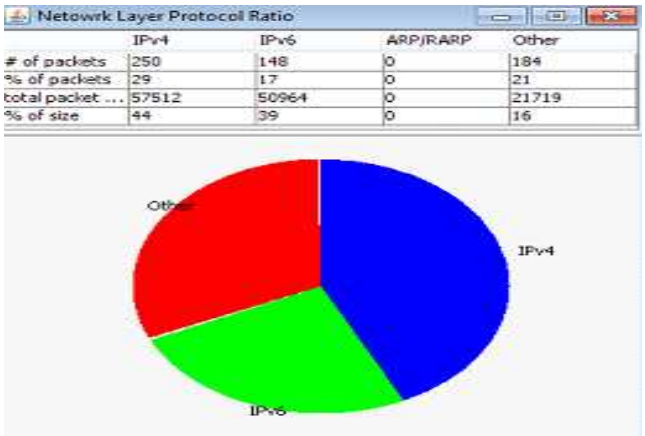


Fig. 4: Network Layer Protocol Ratio

IV. CONCLUSION

In the Present technology many attack features are in accordance with the idiomatic usage of natural English and the appearance probability of English letters varies very much, according to the above characteristics, a new pattern matching algorithm is proposed in this paper, first sequence letters in the pattern string from low appearance probability to high appearance probability in natural English, and then match one by one according to the algorithm, in this way, you can find as many mismatches as you can, thereby reducing the comparison times. *Intrusion* prevention *system (IPS)* is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents; this can be put forward as a Future work [7]. The current generations of IDS (HIDS and NIDS) are quite effective already; as they continue to improve they will become the backbone of the more flexible security systems we expect to see in the not-too-distant future. Finally, on the basis of BM algorithm, an intrusion detection system model is put forward.

REFERENCES

[1] ZHANG Hu "Design of Intrusion Detection System Based on a New Pattern Matching Algorithm".

[2] Ulf lindvist, Phillip Brentano and Doug Mansur, "IDS Motivation, architecture, and an Early Prototype", Computer Security Laboratory, US Davis: 160-171.

[3] Robert Graham," Protocol Analysis and Command Parsing vs. Pattern Matching in Intrusion Detection System", http://www.networkice.com

[4] Neil Desai, "Increasing Performance in High Speed NIDS".

[5] Moore, Strother J. "The Boyer_Moore Fast String Searching Algorithm. Texas University".

[6] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, Diego Zamboni, "An Architecture for intrusion detection using autonomous agents".

[7] Shivaji P. Mirashe, N. V. Kalyankar, Reliance Communication. Koparkharine, "Why We Need the Intrusion Detection Prevention Systems (IDPS) In IT Company".

[8] www.robertgraham.com/pubs/network-intrusion-detection.html.