Intrusion Detection System in UDP Protocol

K.Duraiswamy[1] G Palanivel[2]
Dean (Academic), Department of CSE, K.S.Rangasamy College of Technology[1]
Assistant Professor, Department of Information Tech, Kings College of Engineering[2]

Abstract - To face the growing trend of attack and other security challenges, Intrusion Detection System have to be addressed across the network. Each TCP/IP network layer has specific type of network attacks and hence it needs a specific type of IDS. So, depending upon the TCP / IP network model, we can categorize the IDS into AIDS, TIDS, NIDS, LIDS and each IDS type is specialized to a specific network device. In this paper, we focus on TIDS which detects the UDP layer attacks based on Fuzzy ESVDF (which select appropriate feature set) for overall improvement of performance and scalability especially in UDP model.
Keywords: - Intrusion detection systems, TCP/IP network model, UDP model, features ranking, support vector decision function.

1. INROUDUCTION

The field of information security has grown and evolved in recent years because of the rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet and other computer networks. Previous studies show a new categorization of IDS depending upon the TCP / IP model. It states that the choice of network features for IDSs was depend on the network attack type to be detected.

Network attacks can be categorized into four major types:

- Application Layer attacks,
- Transport Layer attacks,
- Network Layer attacks, and
- Link Layer attacks.

The IDSs also can be categorized into AIDS, TIDS, NIDS and LIDS.

Second, as it is known, firewalls operate at different TCP/IP network layers by using different criteria to restrict traffic, but this step is far from running an entirely secure network. Because of that, IDS must be allocated as a second line of defense. Third, the attacks usually gain access to the network through the network devices distributed through different TCP/IP network layers as entry points; and in order to be able to adequately address security, all possible avenues of entry must be evaluated and secured. So, IDS must be allocated at these entries or network devices.

Finally, categorizing IDS into different types depending on the TCP/IP layers becomes an essential issue for improving the overall system detection ability. In this paper, we focus mainly on developing a TIDS especially for UDP layer since TCP and UDP protocols are defined in the Transport layer of OSI/ISO model. Moreover, Transport layer attacks for TCP model and UDP model are not the same type and differs the feature set and hence separate TIDS is to be defined for the UDP model. In a nutshell, the AIDS, LIDS and NIDS remains the same as the TCP/IP model and only TIDS differs.

2. BACKGROUND

This section introduces a brief description of TCP/IP model, IDSs, classification of intrusions, UDP attacks and Fuzzy Enhanced Support Vector Decision Function (Fuzzy ESVDF).

2.1. TCP and UDP model:

TCP/IP model which are based on layered concept of networking as shown in Fig.1 was developed to accommodate changes in technology. Each layer of specific network model may be responsible for different functions of the network. The TCP/IP protocol enables computers to communicate over the network, specifying the processing information of a packet. The TCP/IP layer uses four layers which differ significantly from ISO/OSI layers even though they are very similar on the L3 and L4 layers.

In the TCP/IP model, each layer has its own functionality and service which means that each layer needs a specific protection process. Following is the major differences between UDP and TCP:

1. TCP can establish a Connection and UDP cannot.
2. TCP provides a stream of unlimited length, UDP sends small packets.
3. TCP guarantees that as long as you have a connection data sent will arrive at the

Manuscript received March 5, 2010
Manuscript revised March 20, 2010

destination, UDP provides not guarantee delivery.

4. UDP is faster for sending small amounts of data since no connection setup is required, the data can be sent in less time then it takes for TCP to establish a connection.

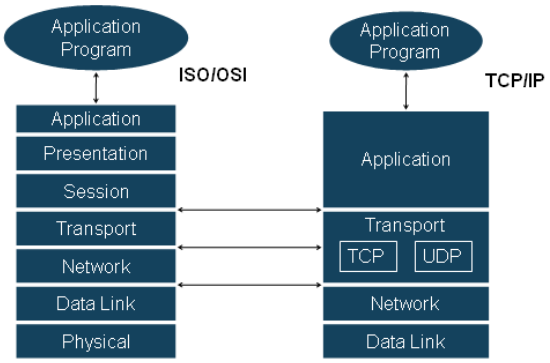

Fig.1 Comparison of TCP, UDP and ISO/OSI Model

2.2. Intrusion Detection System:

IDSs is responsible of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions. It takes the appropriate action to cut off network connections, record events, give alarm, and remind the system administrator to take the proper measures. Modern IDSs are extremely diverse in the techniques they employ to gather and analyze data.

The common architecture of IDS structure is shown in Fig.2

- A detection Model: It collects data that may contain signs of intrusion. It monitors Host IDS, Network IDS [7, 8, 13], Router IDS [3, 13], and Application IDS.
- An Analysis Engine: Once sign of intrusion is positive IDS
  analysis it and categorize into three types of detections: misuse detection [6], Anomaly detection [9], Specification detection [10].

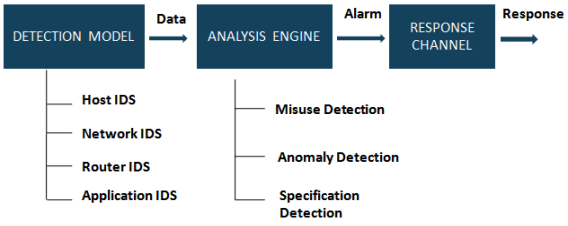

Figure 2: IDS Architecture

The Response Component: It reports intrusions and takes responsive action [11, 12, 13].

2.3. Classification of Intrusions:

An intrusion is generally defined as a set of actions that attempt to exploit vulnerabilities thereby gain access to confidential data.

- Normally, attacks can be categorize into four main categories [3, 4, 5, 13]

  – Probing
  – DoS
  – U2R
  – R2L

We, categorize the attacks into four types depending on the TCP/IP layer,

– Application layer attacks: These attacks are specific to the application layer in the network protocol stack such as back, pod, smurf, buffer overflow, load module, perl, guess password, satan, etc.

– Transport layer attacks: These attacks are specific to the transport layer in the network protocol stack such as land, Neptune, port sweep, and many others.

– Network layer attacks: These attacks are specific to the network layer in the network protocol stack such smurf, POD (Ping of Death), IP sweep attack, etc.

– Link layer attacks: These attacks are specific to the link layer in the network protocol stack such as MAC attacks, DHCP (Dynamic Host Configuration Protocol) attacks, ARP (Address Resolution Protocol) attacks, STP and VLAN-Related attacks.

Transport layer attacks in UDP model:

1. ICMP Attacks
2. Smurf Attacks
3. ICMP Tunneling
4. Port Scan attack
5. UDP Flood attack

ALGORITHM 1: The Fuzzy ESVDF

– Step 1 (calculating the global accuracy GA)
  - Calculating the accuracy and training time for all features.
    AA = accuracy of all features.
    ATT = training time of all features.
  - Calculating the accuracy and training time of s1
    AS1 = accuracy of s1
    ATTS1 = training time of s1
  - Pick the global accuracy(GA)

```
if (AA>=AS1)
        GA = AS1
else
        GA = AA
end if
```

– Step 2
  - Sort 's1' in descending order depends on its weight values.
  - Pick the first three features as initial features set (s2).
  - Calculating the accuracy and training time of s2.
    A1 = accuracy of s2.
    ATT1 = training time of s2.

```
if (GA< = A1)
   exit(0);
else
   continue loop=1;
    count loop=0;
   do
   {
        Add the next feature(f(i)) ;  /*from s1 to s2*/
       calculate  A2 and ATT2; /* corresponding to s2*/
        if (A2<A1)&&(ATT1>ATT2)
        {
            remove(f(i));          /* from s2*/
            count loop + = 1;
         }
         else
         {
              A1= A2; ATT1= ATT2; continue loop + = 1;
              if(GA < = A1)
                 count loop = 0;
              end if
         }
         end if
```

4. Fuzzy Enhanced Support Vector Decision Function(Fuzzy ESVDF):

- It is a simple and fast feature selection approach and an iterative algorithm.
- It is based on Support Vector Decision Function (SVDF) and Forward Selection (FS) approach with a fuzzy inferencing model.
- The Fuzzy ESVDF is an iterative algorithm, where each iteration consists of two steps:
  – Feature ranking (evaluated by SVDF)
  – Feature selecting (FS approach is applied with fuzzy inferencing model) to select these features based performance comparison.
- The general methodology of the Fuzzy ESVDF is based on the following algorithm:
  It starts by picking three features from the features set (S1) with the highest weight values (the weight value is calculated by using SVDF (1)) and name it as s2.
  – Then calculates the accuracy and training time for S2. The feature with the next highest weight value from S1 is added to S2 while calculating its performance.
  – During this process, 2 types of comparisons are made: a local fuzzy comparison and a global fuzzy comparison.
  - The local fuzzy comparison compares the performance of S2 with the performance from the previous iteration; if the first value is less than the second value, the added feature is ignored; otherwise, it is kept in S2.
  - In the global fuzzy comparison, the classification accuracy of S2 is compared with the global accuracy, which is equal to the minimum of two values: the accuracy of all the features and the accuracy of S1.
  – If the classification accuracy of S2 is equal to or greater than the global accuracy value, the algorithm will stop and S2 will be the selected features set; otherwise, it will continue execution.

4. PROPOSED MODEL

- Network security should be addressed at each TCP/IP network layer for different vulnerabilities and attack types. The choice of network feature for IDSs is dependent on the network attack pattern. Some features were good for detecting network attack traffic patterns while others were good at transport attack traffic pattern. So, it is necessary to study the nature of IDS environment for appropriate choosing of

features to analyze the traffic patterns. Moreover,

- Its able to combine the best characteristics of traditional router based, Network based, and Host based IDSs.

Splitting the detection process into different level reduces the computation load and increases the scalability and performance. To apply the Fuzzy ESVDF features selection approaches, there are two main steps.

First, we prepare dataset for the training and testing purposes. TIDS for UDP model has its own dataset since it is connectionless and doesn't have flow control when compared with TCP model. For this purpose, a brief study about the UDP attacks is required to define the dataset correctly.

ICMP Attacks - This occur by triggering a response from the ICMP protocol when it responds to a seemingly legitimate request (think of it as echoing). Ping for instance, that uses the ICMP protocol. sPing is a good example of this type of attack, it overloads te server with more bytes than it can handle, larger connections. Its ping flood.

Smurf Attacks - This attack uses IP spoofing and broadcasting to send a ping to a group of hosts on a network. When a host is pinged it sends back ICMP message traffic information indicating status to the originator. If a broadcast is sent to network, all hosts will answer back to the ping. The result is an overload of network and the target system. The only way to prevent this attack is to prohibit ICMP traffic on the router.

ICMP Tunneling - ICMP can contain data about timing and routes. A packet can be used to hold information that is different from the intended information. This allows an ICMP packet to be used as a communications channel between two systems. The channel can be used to send a Trojan horse or other malicious packet. The counter measure is to deny ICMP traffic on your network.

UDP Flood Attack: UDP is a connectionless protocol and it does not require any connection setup procedure to transfer data. A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

Port Scan Attack : A Port Scan is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a network run many services that use TCP or UDP ports. A port scan helps the attacker find which ports are available. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness.

- Second, we apply the features selection approach for the dataset to select the most effective features set for TIDS.

The Fuzzy ESVDF, as it is described in Algorithm, is based on a Support Vector Decision Function (SVDF) (and Forward Selection (FS) approach with a fuzzy inferencing model to select the best features as inputs for IDS. It is an iterative algorithm, where each iteration consists of two steps: feature ranking and feature selecting.

- First, features ranking, evaluated by SVDF to rank each specified candidate feature. Then, feature selecting, FS is applied with the fuzzy inferencing model to select the features according to a set of rules based on a comparison of performance;

The other features selection approach that is being used for designing the different types of IDS based on detectingDoS attack using SVM.

5. EXPERIMENT or IMPLEMENTATION METHOD

The experiment is divided in three modules.

- First, prepare different datasets for TIDS.
  - Prepare dataset such that it contains both the normal behavior patterns and the attack patterns (dataset contains some populated samples).
- Second, apply the feature selection approach on the dataset to select the most effective feature set for TIDS.
  - The Fuzzy ESVDF approach is used. The algorithm is performed for n times (e.g. 10 times) on TIDS over training and test data. At each time 30% samples were randomly

selected as the test data and remaining 70 as training data.

- Finally, evaluate the feature set results using Neural Networks (NNs) and Support Vector Machines (SVMs) as two different classifiers for AIDS, NIDS, TIDS and LIDS. Each experiment is repeated for some times for each dataset and by randomly selecting the training and the testing data using different splitting ratios.

6. CONCLUSION and FUTURE WORKS

A new categorization for IDS based on TCP/IP network model which focus on UDP Layer 4(UDP protocol) is designed that accommodates the three main form of security measure. This categorization improves the performance and scalability of the TIDS over the Transport layer. In the TCP/IP model each IDS type can be specialized to detect a specific category of attacks depending on the layer. Moreover, categorizing IDS will be supported by firewall since IDS is second level of defense after firewall. Our system proposes TIDS by selecting the appropriate features set the TIDS (Fuzzy ESVDF) and validate their performance by using NN and SVM classifiers. Future work will involve integrating the three IDS types (AIDS,NIDS, TIDS) into a single IDS(one multi IDS) in which the TIDS will detect both the TCP and UDP attacks in real time intrusion detection environments.

REFERENCES

[1] S. Zaman S., F. Karray. Fuzzy ESVDF approach for Intrusion Detection System. The IEEE 23rd International Conference on Advanced Information Networking and Applications (AINA-09).May 26-29, 2009. "to be published".

[2] I. Onut and A. Ghorbani. A Feature Classification Scheme for Network Intrusion Detection. International Journal of Network Security, Page(s): 1–15, July 2007.

[3] A. Tamilarasan, S. Mukkamala, A. Sung, and K. Yendrapalli. Feature Ranking and Selection for Intrusion Detection Using Artificial Neural Networks and Statistical Methods. 2006 International Joint Conference on Neural Networks (IJCNN'06), Page(s):4754 - 4761, July 16-21,2006.

[4] A.Sung, S.Mukkamala. Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks. Symposium on Application and Internet (SAINT'03), Page(s): 209-216, 27-31 Jan. 2003.

[5] V. Golovko, L. Vaitsekhovich, P. Kochurko and U. Rubanau. Dimensionality Reduction and Attack Recognition using Neural Network Approaches. International Joint Conference on Neural Networks, 2007, Page(s): 2734-2739, 12-17 Aug. 2007.

[6] L. Silva, A. Santos, J. Silva, and A. Montes. A Neural Network Application for Attack Detection in Computer Networks. IEEE International Joint Conference on Neural Network, 25-29, Page(s):1569 - 1574 Vol.2, July 2004.

[7] J. Lei and A. Ghorbani. Network Intrusion Detection Using an Improved Competitive Learning Neural Network. Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR'04), IEEE Computer Society, Page(s): 190 – 197, 2004.

[8] M. Moradi and M. Zulkernine. A Neural Network Based System for Intrusion Detection and Classification of Attacks. Unpublished technical report, this work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC). http://www.cs.queensu.ca/~moradi/148-04-MM-MZ.pdf.

[9] D. Novikov, R. Yampolskiy, and L Reznik.. Anomaly Detection Based Intrusion Detection. Third International Conference on Information Technology: New Generation, Page(s):420 – 425, April 2006.

[10] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang and S.Zhou. Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. Proceedings of the 9th ACM conference on Computer and communications security, Page(s): 265 – 274, 2002.

[11] A. Curtis, and J. Carver, "Intrusion Response Systems: A Survey", Department of Computer Science, Texas A&M University, Tech Report, 2000.

[12] H. Kai, H. Zhu, K. Eguchi, N. Sun, and T. Tabata. A Novel Intelligent Intrusion Detection, Decision, Response System. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences archive, Page(s): 1630-1637 Vol. E89-A, June 2006.

[13] Seovng-Bum Lee,Gahng-Seop Ahn, and Andrew T.Camphell, Columbia University.IEEE Communication magazine-June 2001,Page(s):156-165

Dr.K.Duraiswamy is currently a Professor & Dean (Academic) in the Department of Comp. Science & Engg, K.S.Rangasamy College of technology, S.India. He has more than 41 years of experience in Teaching and research. He has published more than 90 research papers in referred International journals and conference proceedings. His research interests include Computer Architecture and Network security. He is a member of the MISTE.

G Palanivel is currently working as an Assistant Professor in the Department of Information Technology, Kings College ofEngineering, Punalkulam – S.India.He has more than 8 years of experience in Teaching and research. He has published 5 research papers in referred conference proceedings. His research interests include Network security and Data Mining. He is a member of the CSI and MISTE.