2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)

Enhancing Hybrid Intrusion Detection and Prevention System for Flooding Attacks Using Decision Tree

Mofti Rafie Abdel-Ghani Ahmed
Sudan University of Science and Technology
College of Graduated Studies
College of Computer Science and Information Technology
Khartoum, Sudan
(E-mail: mofte.cn93@gmail.com)

Faisal Mohamed Abdalla Ali
Karary University
College of Computer Science and Information Technology
Khartoum, Sudan
(E-mail:fabdalla@hotmail.com)

Abstract **- Computer networks are being attacked every day. Intrusion detection systems (IDS) are used to detect and reduce effects of these attacks. The currently used of hybrid intrusion detection systems that was base on signature and anomaly based detection techniques were became inefficient for detecting attacks because it have nearly less than or equal to 95.5% for the detection rate and 1.8% for false positive rate, nowadays these values are unsatisfied for the detection so that the needs to enhanced hybrid intrusion detection system has became the most important issues.**

In this study, the enhanced hybrid intrusion detection system has been proposed to provide better results with high accuracy of the detection rate and reduce the value of false positive rate that will done by proposing new method based on decision tree of data mining techniques that is based on C4.5 algorithm to show that the proposed model is more efficient and it gives better optimum results.

. ***Keywords – Network, Intrusion, Signature based detection, A anomaly based detection, Attack.***

I. INTRODUCTION

As a result of the technological advances in recent years, we have become increasingly dependent on global networks on our daily life, then the explosive use of computer networks make a number of security issues on the internet and in computer systems have been raised and this made the intrusion detection and prevention system (IDPS) play a critical role in the internet to maintain data integrity, confidentiality, and system availability against possible threats vi using intrusion detection techniques [1].

-Types of intrusion detection techniques:

a. Signature Based Detection:

The signature is a pattern that corresponds to a known threat. In signature based detection, observed events are compared against the pre-defined signatures in order to identify possible unwanted traffic. It's is very fast, easy to configure and it's very effective at detecting known threats but largely ineffective at detecting previously unknown threats [2].

b. Anomaly Based Detection:

This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time ,then the IDS will compares the characteristics of current activity to thresholds related to the profile if it's anomalies mean that there are abnormal activities of attacks. It's can be very effective at detecting previously unknown threats, but the common problems with it' establishing profiles that are not sufficiently complex and it leads to generating many false positives alerts [3].

II.Related Works

In the recent years, various hybrid IDS systems have been developed to achieve the best possible performance. In this section, we will review some of these methods.

L. Khalvati, M. Keshtgary and N. Rikhtegar [4] have proposed intrusion detection system that is based on novel hybrid learning approach that combine the K-Medoids clustering and selecting feature using the support vector machine method. The experimental results on the KDDCUP'99 dataset have shown that this method is capable of achieving 91.5 % for the accuracy, 90.1% for detection rate and 6.36 for False alarm rate.

Özge C epheli1Saliha Büyükçorak, and Güneg Karabulut Kurt [5] have build hybrid intrusion detection system using expectation maximization algorithm. The results show that the proposed hybrid model of intrusion detection system has a 92.1% TPR and 1.8% FPR, and with signature-based detector we get 64.7% TPR and 13.2% FPR.

Aliya Ahmad , Bhanu Pratap Singh Senga [6] were developed intrusion detection system (IDS) based on support vector machine using BAT algorithm to increase the performance of the system. The experimental results have shown that the proposed IDS had accuracy reaches up to 94.309% with minimum FPR and FNR whereas classification rate for Existing Method (IG-ABC SVM) is 89.799%.

III. PROBLEM STATEMENT

The increasing number of cyber threats likes flooding attacks in the networks of the organization and there were various approaches to intrusion detection are currently being used, but they are relatively ineffective for detecting flooding attacks and it will cause many problems such as:

a. May detect and prevent only known or unknown attacks.

b. Making a resource (e.g. CPU, memory, bandwidth, disk space) unavailable to its legitimate users, by exhausting it [7].

978-1-7281-1006-6/19/$31.00 ©2019 IEEE

c. The detection rate nearly is less than or equal to 95.5% and 1.8% for false positive rate, but in nowadays these values are not satisfied.

1V. OBJECTIVES OF THE RESEARCH

This study aim to:

1. Collect dataset about the normal behaviors for valid users.
2. Build secure and robust enhanced hybrid IDS/IPS to provide high detection rate and low false alarm.
3. Demonstrate how some types of or flooding attacks that will occur.
4. Analysis and evaluate the performance of proposed intrusion detection and prevention system.

V. Proposed Solution

For this research, will trying to find a method that provides the best way to detect malicious activities and to solve the shortage of existing intrusion detection system and this done by building enhanced hybrid intrusion detection system by using decision tree of data mining classification techniques to make deep packets inspection that help in detecting of known and unknown attacks and providing better results of detection accuracy rate and false alarm rate than existing results after passing the observed data or a traffics.

VI. Proposed System

The observed traffics are passed to hybrid IDS (Signature and Anomaly) detection system as seen in figure 1. In signature based detection, The detector(Engine) will compare the observed traffics against the pre-defined signatures in order to identify possible unwanted traffic then it will generate attacks alert messages to the administrator as shown in the top part in the below "Fig .1":

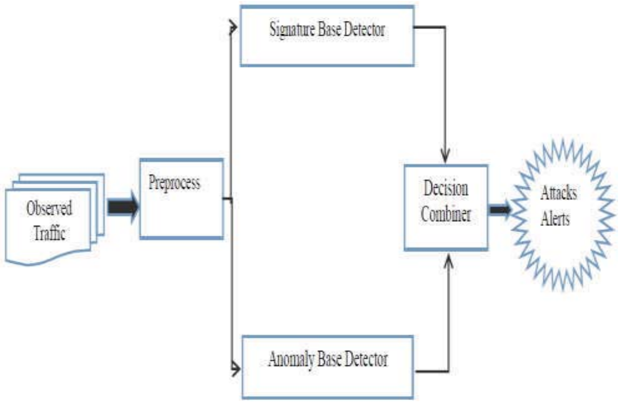


Fig. 1. Architecture of the proposed Hybrid IDS

From the above "Fig 1", In Anomaly based detection engine, the anomaly base detector must receive processed dataset so that will need to preprocess it by extracting the important features (e.g. duration and protocol,.., etc) and cleaning data-set from any irrelevant values by using Info gain feature selection technique then will reduce the features by remove similarity attributes of the data-sets as represented steps in "Fig. 2":

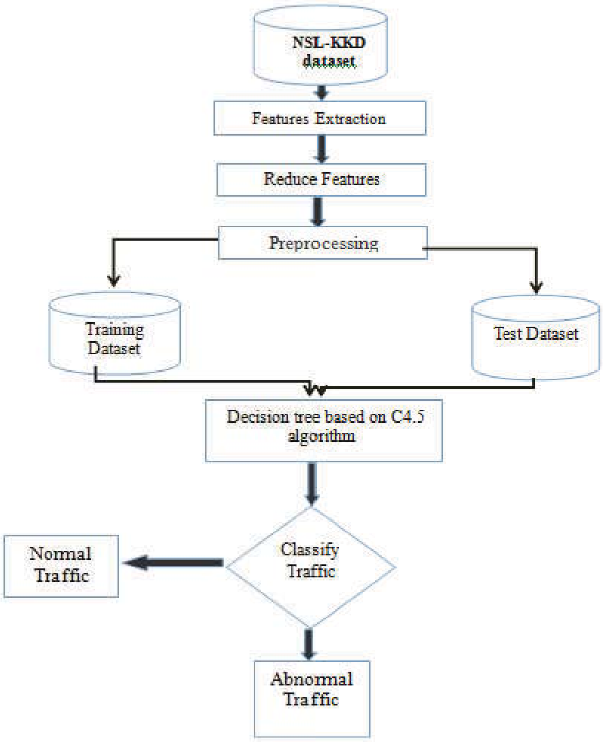


Fig. 2. Steps of building proposed Anomaly detection model

After that, the prepossessed dataset are passed to the classifier to classify it as normal and abnormal traffics according to predefined classification as it's represented in "Fig. 2".

As it saw in "Fig. 1", the hybrid techniques with their methods will work together by using decision combiner to work as logical module that generate decision for detecting attacks to provide high accuracy of detection rates to help administrators to choose and configure the appropriate protection mechanism.

- Reasons of using classification techniques:

Because the **c**lassification techniques are useful to handle large amount of data. Classification is used to predict categorical class labels. The classification models are used for classifying newly available data into a class label.

- Reasons of using decision tree based on C4.5:

A decision tree is the data mining method technique that can be represented as form of tree structure. It's can be very fast, power efficient and easy to understand and programming it's with using IF, THEN, ELSE statements.

The C4.5 algorithm has many features such as it can dealing with both continuous and discrete attributes, missing values and it produce more accurate model [8].

After the building the proposed system then will test it with many behaviors of attacks such as nmap scanning attacks, TCP, UDP, ICMP and HTTP flooding attacks.

VII.Testing Attacks behaviors

The following attacks are tested to check the efficiency of the proposed system:

1 ICMP Flooding Attacks :

This type of attack flood the target with many echo request and echo replay messages with the different packet size to cause high load as in “Fig 3”:

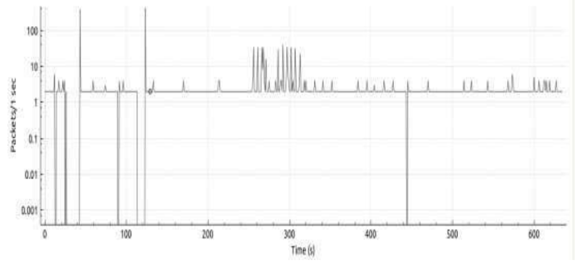
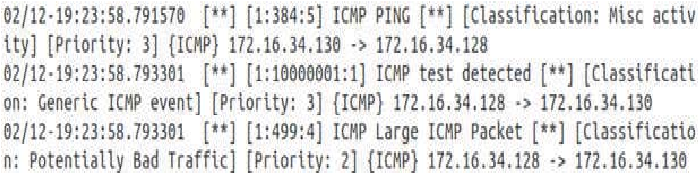


Fig. 3. Effection of icmp flooding attacks on the resources

The detection of the attacks will done by running snort in intrusion detection mode and it give this result:

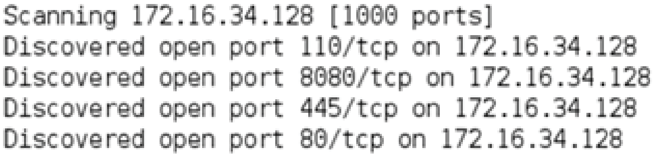


```
02/12-19:23:58.791570  [**] [1:384:5] ICMP PING [**] [Classification: Misc activ
ity] [Priority: 3] {ICMP} 172.16.34.130 -> 172.16.34.128
02/12-19:23:58.793301  [**] [1:10000001:1] ICMP test detected [**] [Classificati
on: Generic ICMP event] [Priority: 3] {ICMP} 172.16.34.128 -> 172.16.34.130
02/12-19:23:58.793301  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificatio
n: Potentially Bad Traffic] [Priority: 2] {ICMP} 172.16.34.128 -> 172.16.34.130
```

Fig. 4. Result of detection ICMP flooding attacks

2 Nmap scanning attacks:

This type of attacks attempt to obtain information about the target device such as the information of the used of operating system and open and closed ports as in “Fig 5” after using the nmap –A –v 172.16.34.128 command :



```
Scanning 172.16.34.128 [1000 ports]
Discovered open port 110/tcp on 172.16.34.128
Discovered open port 8080/tcp on 172.16.34.128
Discovered open port 445/tcp on 172.16.34.128
Discovered open port 80/tcp on 172.16.34.128
```

Fig. 5. Output of scanning process

“Fig. 5” illustrate that there are many open tcp ports such as 445 and 80.When the traffics of scanning process come to the IDS then it compare the observed traffics with the signature in IDS system

3 TCP/SYS flooding attacks:

The behavior of this type of attacks was done by sending many SYN messages to the target and fill it’s buffers to effect’s to the resources as represented it in “Fig. 6”:

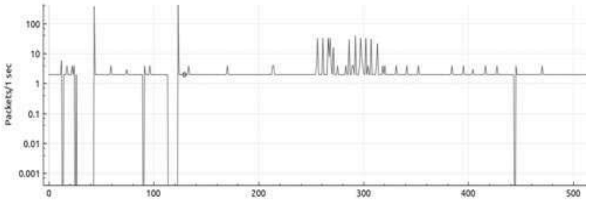
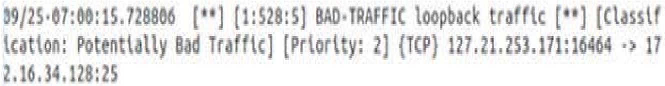


Fig. 6. Effection of sys attacks on the resources

The target (HIDS) system cause alerts message after it receive abnormal traffics of sys flooding attacks and cause the following results of detection as in “Fig. 7”:’



```
09/25-07:00:15.728806  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.21.253.171:16464 -> 17
2.16.34.128:25
```

Fig. 7: Result of detection TCP/SYS flooding attacks

“Fig. 7” notify that, there are bad traffics of tcp or sys messages that can reduce the performance of the network and make the resources unavailable to the valid users. Also, the UDP flooding attack are occurs by sending many udp packet to the target to slow the system by filling it storage capacity such as RAM and that effect to resources.

4 HTTP Flooding attacks:

This types of attacks was done by sending many requests to target to open session that carry many inbound traffics this was occurs by running this command: (ab -c 1000 –n 10000 http:// 172.16.34.128/) to send packet with the size 1000 to cause high load as in “Fig. 8” :

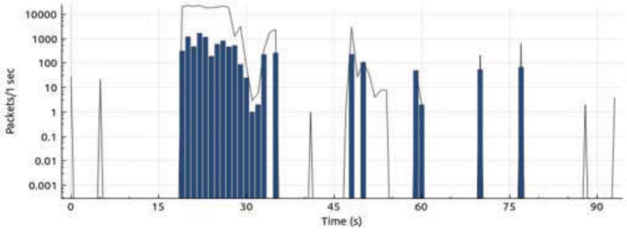
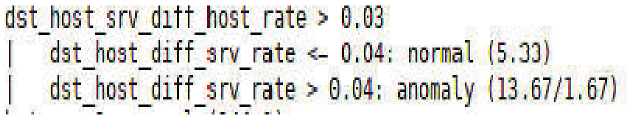


Fig. 8. Load on the target device

“Fig. 8” show that the target device receive many inbound traffics that coming from unauthorized users and it cause high load with the large amount of packets that increasing with the changing of the time (s).

In anomaly base detection method, the processed data set will passed to enhanced decision tree algorithm to classify traffic to normal and abnormal, such as the following “Fig. 9”:



```
dst_host_srv_diff_host_rate > 0.03
|   dst_host_diff_srv_rate <= 0.04: normal (5.33)
|   dst_host_diff_srv_rate > 0.04: anomaly (13.67/1.67)
```

Fig. 9. Classification of traffics base on no of packets

The previous “Fig. 9” differentiates the behavior of valid users form invalid users according to number of packet that are sent. If there are .04 (4) packets or less than it as inbound traffic this mean the normal traffic for valid user else this is abnormal traffics that is sent by attacker that act as ICMP flooding attacks so that will take appropriate mechanism to prevent it by intrusion prevention system like firewall, pefsense , and iptables .....etc.

“Fig. 10” illustrate that the status of the target before it flooded and the status of its after the flooding it with the large amount of inbound traffics that represented with high curve as it see in ” Fig. 11”:

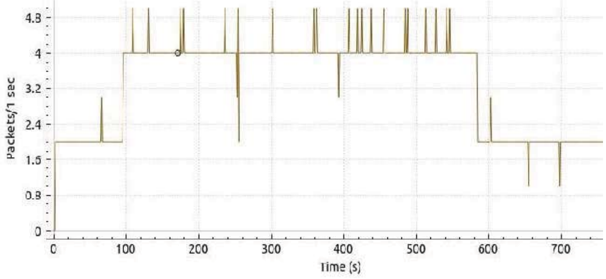
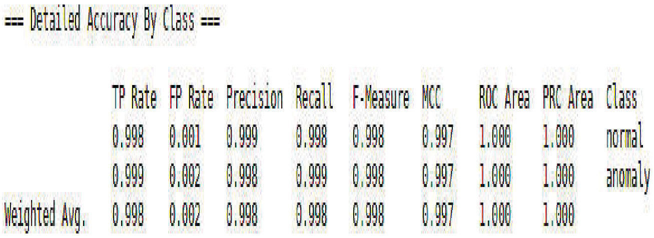


Fig. 10. Effecting of prevention mechanism after the flooding

In “Fig. 10”, after the monitoring process would notify that there is a huge amount of traffics that need to prevent or drop it. Then after the dropping process, the performance of the network was enhancing as it shown the curve that was going to down.

VIII. Evaluation of proposed model

The proposed model make enhancement of accuracy of detection rate to become 99.8 % and it reduce the values of true and false positive to these values for normal and anomaly traffics when it based on decision tree algorithm:



```
=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
               0.998    0.001    0.999      0.998    0.998      0.997    1.000     1.000     normal
               0.999    0.002    0.998      0.999    0.998      0.997    1.000     1.000     anomaly
Weighted Avg.  0.998    0.002    0.998      0.998    0.998      0.997    1.000     1.000
```

Fig. 11. Results of classification

Simple accuracy comparison between the proposed algorithm and many other algorithms as seen in “TABLE 1”:

TABLE 1. COMPARISONS WITH THE PREVIOUS RESULTS

Algorithm	Accuracy rate
Genatic algorithms + Neural Network	80%
K-Medoids + Support Vector Machine	91.5
BAT Algorithm	94%
Proposed algorithm	99.8%

IX. CONCLUSION

In this study, a new hybrid intrusion detection method that integrates a signature detection model and an anomaly detection model is introduced. The results show that the proposed hybrid intrusion detection system has a ability of detection attacks with the faster time and higher detection rate that reach to 99.8% and also it reduces the number of false positives on the detection system to 0.001 when it compared with previous IDS as it saw in figure 11 and table 1.

X.ACKNOWLEDGMENT

I would like to thank my teachers and the sincerely thank to Faisal Mohamed Abdallah for their support and guidance

REFERENCES

[1]William Stallings, “Network security essentials: application and standards”, in Pearson Education, -Inc person highered, ISBN 10: 0-13-610805-9 ISBN 13: 978-0-13-610805-4, 4 edition, 2011.

[2] B.Santos Kumar, T.Chandra Sekhara Phani Raju, M.Ratnakar, Sk.Dawood Baba, N.Sudhaka, “Intrusion Detection System- Types and Prevention ” ,in International Journal of Computer Science and Information Technologies , Vol. 4 (1) , 77 -82.2013.

[3] J. David Irwin, Chwan-Hwa Wu ,”Introduction to Computer Networks and Cyber security” ,in CRC Press , ISBN: 9781466572133 , foburth edition ,
April 2016.

[4] L. Khalvati , M. Keshtgary and N. Rikhtegar , “Intrusion detection based on a novel hybrid learning approach “ , in Journal of AI and data mining , Vol. 6, No 1,157-162, 2018.

[5] Özge cepheli1, Saliha Büyükçorak, and Güneg Karabulut Kurt,” Hybrid intrusion detection system for DDoS Attacks” in Journal of electrical and computer engineering, Vol. 2016, 2016.

[6] Aliya Ahmad, Bhanu Pratap Singh Senga.” Instruction detection system based on support vector machine using BAT algorithm” in international journal of computer applications, Vol.158 – No 8, January 2017.

[7] From interview of IT employee in the organization, and related papers.

[8] Jiawei Han, Micheline Kamber, Jian Pei,”Data mining: concepts and techniques”, Morgan Kaufmann , ISBN: 978-0-12-381479-1 ,3rd Edition, 2011.