REVIEW PAPER ON INTRUSION DETECTION BASED ON ANN BY NETWORK TRAFFIC PARAMETER

Rahul R. Bhoge¹ and Dr. M. A. Pund²
¹²CSE Department, PRMIT&R Badnera, Amravati, Maharashtra, India

Abstract—The Network Intrusion Detection is depending on different parameter of network, which is selected based on either signature or anomaly. In this paper we have review performance of anomaly based intrusion detection parameter like SYN flood attack, TCP/UDP flood attack, nMap scanning attack, and also for non-malicious communication. The paper try to examine the different parameter of ID based result on the benchmark NSL-KDD dataset shows that the performance (accuracy and detection rate) of the ANN based IDS model is at par or in some cases even better than other IDS models based on parameter of Network.

Keywords—Intrusion detection system (IDS), Artificial Neural Network (ANN), NSL-KDD dataset, SYN flood, TCP/UDP flood, nMap.

I. INTRODUCTION

The intrusion detection is use particular mechanism to protect the network from attacker. The NIDS management server and management console often are unknown from the rest of the network, which preferably means that an attacker would not be able to find these mechanisms are placed [1]. Attackers are gradually finding their way around first level preventive mechanisms to gain unauthorized access to the network and system to attacks. Therefore, moreover this preventive measure, Intrusion Detection Systems (IDSs) which acts as a corresponding second line of network resistance is a crucial component for defense against network Attackers [2]. Intrusion detection monitors network traffic or different system for malicious activities to identification of suspicious activities that may indication of a network or system rule violations.

Signature based (Knowledge based) IDS - references a database of previous attack signatures and known system vulnerabilities. The signature is a recorded evidence of an attack or intrusion. Each intrusion leaves a footprint behind (e.g., files and folder access, user intervention, attempt to run a software, etc.)[3]. these footprints are stored in database called signature database and can be used to identify and prevent the same attacks in the future. For each intercepted packet there is verification against stored signatures and the IDS evaluates whether the packet consists malicious communication or not. The disadvantage of signature based IDS is that signature database must be continually updated and maintained. If not, signature based IDS may fail to identify unique attacks. Anomaly based IDS - references a baseline or learned pattern of normal system activity (TCP-UDP-ICMP ratio, packets per second, connections per second, etc.) to identify active intrusion attempts [4]. Deviations from this baseline cause an alarm to be triggered.

The main advantage of an anomaly-based system is its ability to detect previously unknown (or variants of known) attacks when they appear [5]. The major drawback of anomaly detection is defining its rule set. The efficiency of the system depends on how well it is implemented and tested on all protocols. Nevertheless, these systems typically suffer from high rates of false positives.

In this paper we provide a review of attacks detection in run time and also based on either signature or anomaly based detection of attacked going to find by network. There is a different type of parameter which we have to identify by network where attacks detection is possible.
II. RELATED WORK

This were we compare work made done to develop IDE which already done by many researchers which is more about to implementing idea about IDE and Defense mechanism they already have with system.

Why the Artificial neural network has been made in use to make Intrusion detection system, it’s quite easy to answer that this question because we have to make such system which can be find out the different future scope of attacks available with the system. So might have never compromising with the system while attacks going on. The paper on Artificial network already said that the IDE should be depend on the cumulative data which can we collect at the different host of networks gather to one placed or we can shared data between different host might have taking advance futuristic approach given to the system by making analysis of different data set available with the system. NSL KDD dataset have most of the solutions [6], [7], [8] deals with the "off-line and on-line" analysis of the system data. This dataset contains a set of network communication signatures representing standard and malicious communication. In more detail, the KDD Cup 1999 contains:

- Training dataset of the size more than five million records.
- Testing dataset of the size five million records, each entry of the dataset is characterized by different forty two parameters describing network communication (e.g. the amount of bytes sent, number of bytes received, number of node available, etc.).
- The dataset consists the signatures for:
  - Denial of Service attack (DOS), e.g. sync flood.
  - Probing Attack (PROBE), surveillance and other probing, e.g., port scanning.
  - Users to Root Attack (U2R), unauthorized access to local super user (root) privileges, e.g., various “buffer overflow” attacks.
  - Remote to Local Attack (R2L), unauthorized access from a remote machine, e.g. guessing password.
  - Standard communication.
  - N map attacks.
  - Node introduction to the router.

For more detailed analysis of the KDD Cup 1999, see [9].

There is some more general attacks can we find out in KDD dataset while it is most of the time to learning by such attacks we can have system inbuilt decision making to counter attacks of all types which can related or near to our dataset, which can we used to train the network. The decision tree of the neural network has to make the decision in time being frame [10].

Most of the time the attackers have to find out the new solution to the IDE, by unknowingly makes the attacks on the system where the IDE not ability to find out an attackers.

III. NUERAL NETWORK BAESD IDS

![Figure 1. Network based IDS](image-url)
The ANN based IDS have a solution make the attacks counterfoil by training the ANN with NSL KDD dataset while doing so there might have the system to make self assessment while doing such reference value updating so might have possible find out the limitation overrules by itself diagnosing a solution on the attacks[11].

It is always important to parameter selection while detecting attacks, even its every network parameter having substantial role find out attacks, but it is not possible consider all parameter of network traffics as the list of parameter is already provided with standard dataset NSL KDD, so might have possible to select a parameter based on requirement of situation arises in network.

We also how some example which can specified in different paper so might have we can conclude with what parameter should be consider,

![Figure 2. Example of TCP packet](image)

The above example has TCP packets which can have different parameter that can possible to analyze.
- Destination port
- Flag
- DestIP Ratio,
- DestPort Ratio,
- DestIP&Port Ratio,
- SynAckRatio,
- NumDestIps,
- NumDestPorts,
- InputRate,
- TCP Rate,
- UDP Rate,
- ICMP Rate.

The analysis of this parameter store into the database of network packet [12][13]. Even we have compare data with old data and construct new set of data so we can try to find out a prediction of attacks based on result so might have consider attacks should be not going incorporated with host. We have to match dataset find out by our IDS with already trained dataset of ANN, to make the dataset train against particular types of attacks and then take the necessary action on behavior of system to counterfoil, even ANN with initial 20% training given with premature dataset already available with the NSL KDD. The important aspect to match the given reference traffic parameter values with new generated data for exclusion of attacks in same manner as real time data acquisition going to take from different network node and try to make integrated approach to immune the host as by IDS with Neural Network. The attacks are to find out in different manner so it might have shows unwanted behavior of network parameter. We have small list of attacks that can be classify on the base of NSL KDD dataset [1].

| S/N | Name             | Type  |
|-----|------------------|-------|
| 1.  | Back             | Dos   |
| 2.  | buffer_overflow  | u2r   |
| 3.  | ftp_write        | r2l   |
| 4.  | guess_passwd     | r2l   |
5. imap  r2l
6. ipsweep  probe
7. land  Dos
8. loadmodule  u2r
9. multihop  r2l
10. neptune  Dos
11. nmap  probe
12. perl  u2r
13. phf  r2l
14. pod  Dos
15. portsweep  probe
16. rootkit  u2r
17. satan  probe
18. smurf  Dos
19. spy  r2l
20. teardrop  Dos
21. warezclient  r2l
22. warezmaster  r2l

This above attacks might have uncertainty in network parameter as we find out already while considering a small example of TCP packet. On that basis we can able find out the resultant IDS which can find out attacks more specifically even in some parameter are consider but not even without comparing with nearby traffic flow in the network.

IV. CONCLUSION

By these paper we can find out with some fact about network parameter and how to find out specific parameter in the networks so we manage to recognize which types of attacks going to happen on network, by simulating such analysis of such parameter we can find out the actual parameter affecting to the network while applying any type of defense against attacks.

It also gives us a brief introduction about ANN system can be best solution we might have to apply so we can easily integrated the data even in subsequent stages of network while transferring a data from one host to another host. The network based IDE is make integrated collection of data while performing a defense against attacks.

REFERENCES

[1] Norbert Adam, Branislav Mados, Anton Balaz, Tomas Pavlik, “Artificial Neural Network based IDS”, SAMI 2017, IEEE 15th International Symposium on Applied Machine Intelligence and Informatics, January 26-28, 2017, Herlany, Slovakia, pp 159-163.
[2] Basant Subba, Santosh Biswas, Sushanta Karmakar, “A Neural Network Based System for Intrusion Detection and Attack Classification”, 978-1-5090-2361-5/16, 2016, IEEE.
[3] H. Kaur, G.K. Bhalia, “A Review on IDS By Correlation & KPCA with Neural Network Optimized By Genetic Algorithm”, in IRACST - International Journal of Computer Science and Information Technology & Security (IJCITS), vol.6, no.2, 2016. Pp 237-239.
[4] L. Vokorokos, A. Baláž, B. Madoš, “Anomaly and Misuse Intrusions Variability Detection” in Acta Electrotechnica et Informatica, Vol. 10, No. 4, 2010, pp. 5-9.
[5] L. Vokorokos, A. Baláž, N. Adam, “Events Planning in Intrusion Detection Systems” in Acta Electrotechnica et Informatica, Vol. 7, No. 4, 2007, pp. 82-86.
[6] S. Devaraju, S. Ramakrishnan, “Performance Comparison for Intrusion Detection System Using Neural Network with KDD Dataset”, in Ictact Journal on Soft Computing, April 2014, vol. 04, issue 03, pp.743-752.
[7] L.L. Ray, “Training And Testing Anomaly-Based Neural Network Intrusion Detection Systems”, in International Journal of Information Security Science, vol. 2, no. 2, pp. 57-63.
[8] S. Kumar, A. Yadav, “Increasing performance of intrusion detection system using neural network”, in IEEE International Conference on Advance Communication, Control And Computing Technologies (ICACCT), May 8th-10th, 2014, pp. 546-550.
[9] M. K. Siddiqui, S. Naahid, “Analysis of KDD CUP 99 Dataset using Clustering based Data Mining”, International Journal of Database Theory and Application, Vol.6, No.5 (2013), pp.23-34.

[10] Gajanan P. Bherde, M. A. Pund, “Recent attack prevention techniques in web service applications”, 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 9-10 Sept. 2016, pp 1174 – 1180.

[11] M. A. Pund, S. V. Athawale, “NGIPS: The road map of next generation intrusion prevention system for wireless LAN”, 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), Year: 2017, pp 276 – 280.

[12] Akshat Ajabrao Uike, M. A. Pund, Sangram S. Dandge, “An Overview of Cloud Computing: Platforms, Security Issues and Applications”, International Journal of Science Technology Management and Research, Volume 2, Issue 5, May 2017, pp 17-20.

[13] Shwetambari G. Pandkar, G. R. Bamnote, “Analysis of Firewall Technology in Computer Network Security”, International Journal of Computer Science and Mobile Computing (IJCSMC), Vol 3 Issue 4, April-2014, pp 841-846.