Intrusion detection Systems in networks

Shubham Kumar (170101064)

A B.Tech Project report submitted in Partial Fulfilment of the requirements for the degree Bachelor of Technology in the guidance of

Dr. Manas Khatua

Computer Science and Engineering
Indian Institute of Technology, Guwahati

Contents

Abstract

Advancements in communication fields hugely increased the network size which ultimately gives rise to more intrusions(attacks). Intrusion detection system (IDS) are designed to protect networks from such attacks by monitoring the state of software and hardware present in the network. Implementing an IDS is a challenging task and an acceptable IDS should have high detection accuracy, low false detection rate and should be able to detect new attacks. Recently many researchers are working on using machine learning and deep learning methods to solve above issues in IDS efficiently. In this report we first detail about IDS and what are the traditional methods that we have used in IDS and why they are not good in current times. Then we will see need of AI based methods to develop IDS and understand various ML based methods that can be used in IDS. Finally we will evaluate some algorithms and see how they perform in real life based on some evaluating metrics. Finally we will discuss about future work in the second phase of the project.

1 Introduction

Recently, due to advancements in internet and communication fields, many organizations are moving their platform to internet, which ultimately increasing network sizes. Networks are prone to various attacks as they contain sensitive information, So network security is a vital research domain. Network security domain deals with the detection and prevention of various novel attacks on the system. Firewall, antivirus software and intrusion detection system are some tools that are used to secure networks.

1.1 IDS

Intrusion detection system (IDS) is a security mechanism that continuously monitors the host and network traffic to detect any illegal(unauthorized) activity that do not adhere with security policy and if found alerts the detected suspicious behaviour to network or host administrators.

1.1.1 Classification of IDS

As depicted in Figure 1, IDS can be classified with the perspective of its deployment or detection methods.

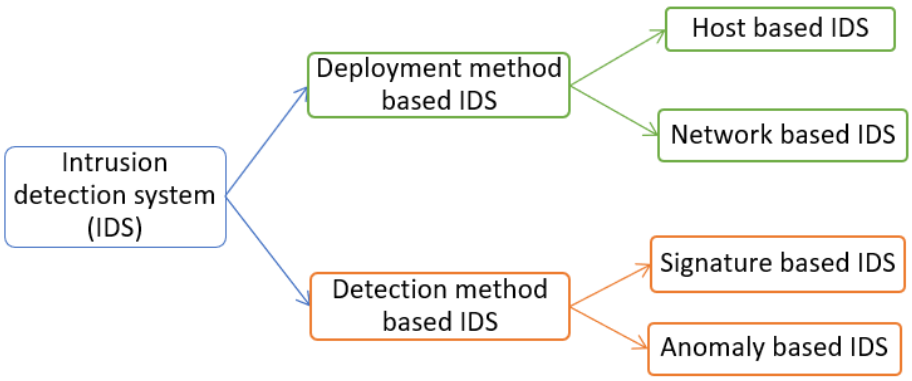

Figure 1: Classification of IDS

- **Deployment Method based IDS** - IDS can be differentiated by their deployment in the secure network. Deployment based perspective IDS can be further sub classified as:-
  - **Host based IDS (HIDS)** - It is deployed on each single information device in the network. It monitors traffic on the single device and detect violations in the security policy on single device only. It should be deployed on each device in the network, so this method is not good.

  - **Network based IDS (NIDS)** - This is deployed on the network and monitors traffic of entire devices in the network. It detects intrusions on the network level and protect all devices in the network.

- **Detection Method based IDS** - IDS can be differentiated by the detection method used by IDS to detect intrusions. Detection based perspective IDS can be further sub classified as:-

  - **Signature based IDS (SIDS)** - Idea behind this method is to look for specific patterns such as number of 1's or 0's in the network traffic. It stores patterns (known as signature) used by intrusions and match these patterns with the incoming and outgoing traffic's pattern to detect intrusions. It gives high accuracy for known intrusions but lacks accuracy against unknown attacks.
  - **Anomaly detection based IDS (AIDS)** - **Anomaly** can be defined as deviation from normal behaviour. These IDS try to estimate the normal behaviour of the system to be secured and report intrusion if any anomaly found in the traffic. They have benefit over signature method based IDS these IDS as they can detect unknown attacks.

In this project we will see ML models that can be used in NIDS (Deployment method perspective) and AIDS (Detection methods perspective). A deployment of NIDS is depicted in Figure 2. NIDS copy all the incoming and outgoing network traffic for performing traffic monitoring to detect intrusions in the trusted network.

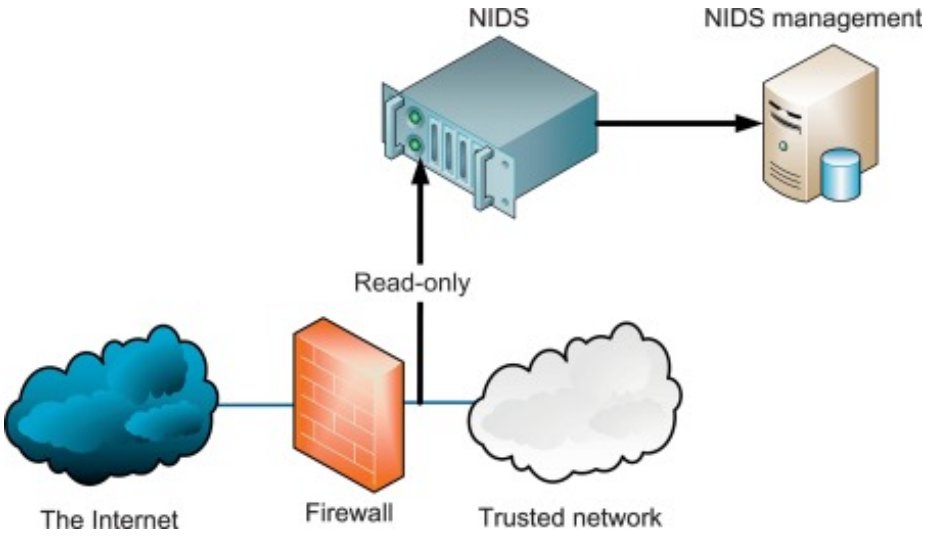

Figure 2: Deployment of NIDS

1.2 Traditional IDS and need of machine learning in IDS

Traditional IDS use mechanism based on Signature based methods or anomaly based methods, which has some limitations:-

- Real attacks are often far less in number than false detection in traditional IDS.
- Network suffers from noise and it increases false alarm rate.
- Signature method based IDS can only detect known attacks they are not much useful against new attacks. Due to above reason they need software updates frequently.
- Anomaly based IDS can only detect deviation from normal behaviour which limits the variety of attacks that they can detect.

To address the above problems there should be a model which can automatically learn like human to differentiate between Normal traffic and Intrusion traffic. Machine learning and deep learning methods are based on the idea of learn automatically based on the events. With this idea we can use them in the IDS..

2 Related Work

IDS came into existence in 1980 when Jim Anderson[1] proposed the idea of IDS. Since then many systems and models were proposed by researchers to secure networks. Due to shortcomings of traditional IDS, recently researchers are focusing on using ML and DL algorithms in IDS. Some researchers [2] [3] focused on building IDS for accuracy and timely detection but they lack robustness. Zanero and Savaresi [4] developed a two-tier anomaly-based architecture for IDS in TCP/IP networks based on unsupervised learning. Lee and Solfo [5] build a classifier to detect anomalies in networks based on data mining techniques. Sommer and Paxson [6] studied lack of deployment of ML-based IDS. They identified various challenges to create ML-based IDS. Training ML-models is also challenging as training data is limited and available ones are for only bench-marking purposes. KDD dataset [7] is one of the datasets that can be used for training models. This dataset was used in the KDDCup contest of 1999. Task was to create model that can classify data into 5 classes of attacks and normal. In this report we will try to recognize problems with traditional IDS and test ML methods for some ML methods. [8] and [9] explained various ML methods that can be used in IDS.

3 Machine Learning in IDS

Machine learning (ML) algorithms gives computer models capability to learn from experience and improve upon them without explicit programming. ML models learn from observations or training data and predict the output for

given input. These models modify themselves to estimate correct values without any human Intervention.
Machine learning algorithms used in IDS can be classified as:-

- **Supervised algorithms** - These type of models work with labelled data. They use labelled training data set to build a function, which can predict outcomes of input.
- **Unsupervised algorithms** - These are used with unclassified or unlabelled data. These algorithms try to build a function to represent hidden structure of the unlabelled data. Data is grouped on the basis of similarities, patterns and differences.

3.1 Overview of some ML algorithms in IDS

Decision tree Decision tree is one of the basic supervised ML algorithms. These algorithm classifies data based on series of rules. The model uses normal tree structure with nodes (represents attribute or feature), branches (represents decision or a rule) and leaf (represents class outcome). These algorithms processes by selecting best features to build tree and then perform tree pruning to remove branches that are irrelevant to avoid overfitting.

K-Nearest Neighbour (KNN) These type of algorithms are one of the simplest supervised algorithm. These algorithms are based on the hypothesis that a sample has higher chance to belong to the class, which most of the neighbours (nearest k neighbours) belong. Thus these models are highly influenced by the value of k.

Support vector machine (SVM) These class of algorithms based on the idea of finding a max-margin separation hyperplane in the n-dimensional feature space. These can be used for linear as well as non-linear problems although for solving non-linear problems they usually use kernal functions. These models can achieve high accuracy even with small-size training sets as separation hyperplane is determined by only small number of support vectors.

Clustering - These unsupervised algorithms are based on the idea of dividing data into different clusters or groups by putting highly similar data into same cluster and less similar data into different cluster. Since these are unsupervised algorithms, no prior labelling of data is needed. **K-means clustering** is a clustering algorithm, where K represents number of clusters and means is the mean of the attributes. It uses distance to measure similarity between two data points. Data points having short distance have high chances of being in same group. K-means algorithm is highly influenced by the value of K.

Naïve Bayes These type of algorithm is based on the idea of conditional probability and the hypothesis of attribute independence. For each data, these classifiers calculates the conditional probabilities for different classes and classified into the class having maximum probability. Conditional probability of sample is calculated as in Formula(1).

$$P(X = x|Y = c_k) = \prod_{i=1}^{n} P(X^{(i)} = x^{(i)}|Y = c_k) \tag{1}$$

In reality attribute independence hypothesis is tough to satisfy, so this algorithm does not perform well in reality.

Linear Regression (LR) The LR is a type of logarithmic linear model. It uses parametric logistic distribution to compute the probabilities of different classes. Probability Calculation formula is shown in Formula(2)

$$P(Y = k|x) = \frac{e^{w_k * x}}{1 + \sum_{k}^{K-1} e^{w_k * x}} \tag{2}$$
$$k \in 1, 2, 3, ..., K - 1.$$

This model can be built easily.

Artificial neural network (ANN) - These supervised models are inspired by the working system of human brain. ANN has input layer, many hidden layers and an output layer. The adjacent layer units are fully connected. Though training ANN models is not easy due to their complex structure.

Ensemble methods Every individual classifiers has strengths and weaknesses. Idea behind these models is to use several weak classifiers to create a single strong classifier by selecting using a voting algorithm.

4 Evaluation of some ML algorithms in IDS

In this section we will see performance of some ML based models in the detection of IDS.

4.1 Dataset

In this report for evaluation purpose we will be using KDD dataset, which was used in the UCI KDD1999 competition. Task of the competition was to develop IDS to detect various attacks. Dataset has total of 4898430 different data instances. Dataset has 23 different classes of data with 22 types of attack. Each data has 41 features. Table 1 shows instances of various data classes in the dataset.

In this Report for experiments we will be using 90% data to train the model and 10% to test the model.

Attack class	Attack name	Instances
DOS	SMURF	2807886
	NEPTUNE	1072017
	BACK	2203
	POD	264
	TEARDROP	979
	LAND	21
U2R	Buffer Overflow	30
	Load Module	9
	PERL	3
	Rootkit	10
R2L	FTP Write	8
	Guess Password	53
	IMAP	12
	MultiHop	7
	PHF	4
	SPY	2
	Warez client	1020
	Warez master	20
PROBE	IPSWEEP	12481
	NMAP	2316
	PORTSWEEP	10413
	SATAN	15892
Normal	-	972780

Table 1: Various attacks with their instances

4.2 Evaluation metrics

In this report we will be using **Precision**, **Recall**, **F-Measure** and **Confusion Matrix**. Confusion Matrix provides information about predicted and actual classes of unlabelled data. For example let's take confusion matrix with n rows and m columns. Then value in cell (i,j) can be seen as the total instances of class i in unlabelled data which are predicted to be in class j.

- **Precision** - Ratio of correctly predicted instances in the class to the total instances predicted to be in that class.
- **Recall** - Ratio of correctly predicted instances in the class to the total instances in the class.
- **F-Measure** - It is the harmonic mean of Precision ans Recall.

4.3 ML algorithms used for Analysis

In this report we will analyse performance of ML model based on the accuracy. There are some techniques known as 'Evaluation metrics' are used in this report to compare performance of various models. Evaluation metrics used in this report are explained in next subsection.

We have used **K-means**, **Random Forest** and **Naïve Bayes** to evaluate ML Models. We will first see results for 5 classes of attacks and normal. Then we will treat all intrusions in a single class.

K-means This is unsupervised model so we can not evaluate performance with metrices discussed above. but we can get some idea from the various cluster value counts. Some conclusions from the results-

- On both cluster size 5 and 2, most of the data is clustered into single cluster while training model.
- On testing data this models fails badly and maps all values of testing data to single cluster.
- Some feature selection technique can help to overcome this problem.

Random forest It is an ensemble method type classifier. It combines many other algorithm classifiers. Classifiers create many trees on any random subset of data and then combines the total votes of each tree to give class of the test data. Evaluation Metrics of this model is described below for both the classifications.

Class	DOS	NORMAL	PROBE	R2L	U2R
DOS	388263	2	0	0	0
Normal	0	97321	0	0	0
PROBE	0	3	4140	0	0
R2L	0	4	0	104	0
U2R	0	5	0	0	1

Table 2: Random Forest algorithm Confusion matrix for cluster size = 5

Class	Precision	Recall	F-Measure	Support
DOS	1.00	0.99	1.00	388265
NORMAL	0.99	1.0	1.00	97321
PROBE	1.00	0.99	1.00	4143
R2L	1.00	0.96	0.98	108
U2R	1.00	0.17	0.29	6
Accuracy			1.00	489843
Macro avg	1.00	0.83	0.85	489843
Weighted avg	1.00	1.00	1.00	489843

Table 3: Random Forest algorithm evaluation metrics for cluster size = 5

Class	Intrusion	Normal
Intrusion	392509	13
Normal	0	97321

Table 4: Random Forest algorithm Confusion matrix for cluster size = 2

Class	Precision	Recall	F-Measure	Support
Intrusion	1.00	0.99	1.00	392522
Normal	0.99	1.00	1.00	97321
Accuracy			1.00	489843
Macro avg	1.00	1.00	1.00	489843
Weighted avg	1.00	1.00	1.00	489843

Table 5: Random Forest algorithm evaluation metrics for cluster size = 2

Naïve Bayes As discussed in Section 2 this approach is based on probabilistic graphical model. Here is evaluation of this approach in IDS.

Class	DOS	NORMAL	PROBE	R2L	U2R
DOS	387935	262	0	0	68
NORMAL	27294	66590	787	98	2552
PROBE	2626	1158	98	0	261
R2L	5	43	19	0	41
U2R	1	1	0	0	4

Table 6: Naïve Bayes algorithm Confusion matrix for all attack types

Class	Precision	Recall	F-Measure	Support
DOS	0.93	0.99	0.96	388265
NORMAL	0.98	0.68	0.81	97321
PROBE	0.11	0.02	0.04	4143
R2L	0.00	0.00	0.00	108
U2R	0.00	0.67	0.00	6
Accuracy			0.93	489843
Macro avg	0.40	0.47	0.36	489843
Weighted avg	0.93	0.93	0.92	489843

Table 7: Naïve Bayes algorithm evaluation metrics for all attack types

Class	Intrusion	Normal
Intrusion	347174	45348
Normal	769	96552

Table 8: Naïve Bayes algorithm Confusion matrix for all intrusion and normal traffic

Class	Precision	Recall	F-Measure	ROC Area
Intrusion	0.99	0.88	0.94	392522
Normal	0.68	0.99	0.81	97321
Accuracy			0.91	489843
Macro avg	0.84	0.94	0.87	489843
Weighted avg	0.93	0.91	0.91	489843

Table 9: Naïve Bayes algorithm evaluation metrics for intrusion and normal traffic

4.4 Conclusion of the experiment

From Evaluation metrics for both the algorithms we can deduce some conclusions about using ML in IDS:-

- An algorithm can be better in terms of precision but it may not be best one due to false rate. No single algorithm can handle all types of attacks.
- ML techniques in IDS should be applied according to the requirements of the network.
- Models can differentiate between Normal traffic and intrusion traffic but lacks accuracy in differentiating various attacks.
- A good model should have high precision and low false positive and false negative rate.

5 Future work

- In this we have used 3 ML algorithms for performance comparison. We will compare some more ML models in next phase.
- In this report we have used some subset of data to train and to test. So these algorithms will be tested on some other data also.
- Deep learning models can be used to handle big data and they can automatically learn from feature representation from data to give output. So we will try to analysis some DL algorithms that can be used in IDS.

References

[1] James P. Anderson Co. Computer Security Threat Monitoring and Surveillance. *Technical report*, 1980.

[2] Yongguang Zhang, Wenke Lee, and Yi-an Huang. Intrusion detection techniques for mobile wireless networks. *ACM Wireless Networks Journal*, 9, 04 2003.

[3] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslaw Szymanski, and M. Embrechts. Network-based intrusion detection using neural. *Intell. Eng. Syst. Artif. Neural Networks*, 12 2002.

[4] Stefano Zanero and Sergio Savaresi. Unsupervised learning techniques for an intrusion detection system. *Proceedings of the ACM Symposium on Applied Computing*, 1, 12 2003.

[5] Wenke Lee and Salvatore Stolfo. Data mining approaches for intrusion detection. 7, 02 1998.

[6] Robin Sommer and Vern Paxson. Outside the closed world: On using machine learning for network intrusion detection. pages 305–316, 01 2010.

[7] *http://kdd.ics.uci.edu/databases/kddcup99/task.html*, 1999.

[8] Hongyu Liu and Bo Lang. Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9:4396, 10 2019.

[9] Zeeshan Ahmad, Adnan Khan, Cheah Shiang, and Farhan Ahmad. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 10 2020.