IJCSC International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 247-250

# Machine Learning Approach for Attack Prediction and Classification using Supervised Learning Algorithms

G. MeeraGandhi

Research Scholar, Department of Computer Science and Engineering, Sathyabama University, Chennai -119
Email: meeragopi@hotmail.com

## ABSTRACT

Due to the large volumes of data as well as the complex and dynamic properties of intrusion behaviors, data mining based Intrusion Detection techniques have been applied to network-based traffic data. With recent advances in computer technology large amounts of data could be collected and stored. Machine Learning techniques can help the integration of computer-based systems in the network environment providing opportunities to facilitate and enhance the work of network security experts. It ultimately improves the efficiency and quality of data and information. Network Intrusion Detection aims at distinguishing the behavior of the network. This paper presents the implementation of four supervised learning algorithms, C4.5 Decision tree Classifier (J48), Instance Based Learning (IBK), Naive Bayes (NB) and Multilayer Perceptron (MLP) in WEKA environment, in an Offline environment. The classification models were trained using the data collected from Knowledge Discovery Databases (KDD) for Intrusion Detection. The trained models were then used for predicting the risk of the attacks in a web server environment or by any network administrator or any Security Experts. The Prediction Accuracy of the Classifiers was evaluated using 10-fold Cross Validation and the results have been compared to obtain the accuracy.

*Keywords:* Machine Learning, Intrusion Detection, C4.5, MLP, NB, IBK, WEKA

## 1. INTRODUCTION

A major focus of machine learning research is to automatically learn to recognize complex patterns and make intelligent decisions based on data. Its difficulty lies in the fact that the set of all possible behaviors are difficult to describe. IDSs may complement other preventive controls (e.g. ûrewalls) as the next line of defense within the organization (Pûeeger and Pûeeger, 2003). An IDS is a device that is placed inside a protected network to monitor what occurs within the network.

The major objective of intrusion detection systems is:

- To accurately detect anomalous network behaviour or misuse of resources.
- To Sort out the true attacks from false alarms.
- To notify the Network administrators of the activity.

Many organizations now use Intrusion Detection Systems to help them determine if their systems have been compromised (Carnegie Mellon University, 2001)

## 2. MACHINE LEARNING METHODS AND THEORETICAL BASIS

Machine learning methods (Pradeep Singh 2005) have been successfully applied for solving classification problems in many applications. In machine learning, algorithms (learners) try to automatically filter the knowledge from example data (datasets). This knowledge can be used to make predictions about original data in the future and to provide insight into the nature of the target concept(s).The example data typically consists of a number of input patterns or examples to be learned. Each example is described by a vector of measurements or features along with a label which denotes the category or class the example belongs to. Machine learning systems typically attempt to discover regularities and relationships between features and classes in *learning or training* phase. A second phase called *Classification* uses the model induced during learning to place new examples into appropriate classes.

For analyzing the data and classification of network attacks from a network environment, the four machine learning algorithms [4], C4.5 Decision tree classifier, Multilayer Perceptron and Naïve Bayes Classifier and Instance Based Learning (IBK) were adopted here. Multilayer Perceptron (MLP) network is the most widely used neural network classifier. MLPs are Universal approximators. MLPs are valuable tools in problems when one has little or no knowledge about the form of the relationship between input vectors and their corresponding outputs.

J48 algorithm is an implementation of the C4.5 decision tree learner. This implementation produces decision tree models. It recursively splits a data set according to tests on attribute values in order to separate the possible predictions. The algorithm uses the greedy technique to induce decision trees for classification. A decision-tree model is built by analyzing the training data and the model is used to classify the trained data. J48 generates decision trees. The node of the J48 decision trees evaluates the existence and the significance of every individual feature.

The Naive Bayes Classifier (Probabilistic Learner) technique is based on Bayesian theorem and is used when the dimensionality of the inputs is high. Naïve Bayes classifiers assume that the variable value on a given class is independent of the values of other variable. The Naive-Bayes inducer computes conditional probabilities of the classes given the instance and picks the class with the highest posterior. Depending on the precise nature of the probability model, Naive Bayes classifiers can be trained very efficiently in a supervised learning mode.

Instance-based knowledge representation uses the instances themselves to represent what is learned, rather than inferring a rule set or decision tree and storing it instead. Once a set of training instances has been memorized, on encountering a new instance the memory is searched for the training instance. This is known as instance-based learning.

## 3. EXPERIMENTAL SETUP

The data analysis and attack classification was carried out using WEKA software environment for machine learning.The Weka, Open Source, Portable, GUI-based workbench is a collection of state-of-the-art machine learning algorithms and data pre processing tools.

In the experiments, the original data set A 1998 [1] DARPA intrusion detection evaluation program, an environment was set up to acquire raw TCP/IP dump data for a network by simulating a typical U.S. Air Force LAN[2] The LAN was operated like a real environment, but being blasted with multiple attacks. For each TCP/IP connection, 41 various quantitative and qualitative features were extracted. Of this database a subset of 494021 data were used in our experiments reported in this paper, of which approximately 20% represent normal patterns, the rest 80% of patterns are attacks belonging to four different categories. It consists of 65534 instances with 41 features. As the risk of the network environment has to be predicted, the categorical attribute of the attack category is selected as the class label. The instances in the dataset are pertaining to the five attack categories – Normal, Denial of Service (DOS), R2L (Unauthorized access from remote machines), Probe, U2R (User to Root attacks).

## 4. RESULTS AND DISCUSSION

The results of the experiments are summarized in Table 2, 3 and 4.

**Table 1**
**Predictive Performance of the Classifiers**

| *Evaluation criteria* | *Classifiers*<br>***J48*** | ***IBK*** | ***NB*** | ***MLP*** |
|---|---|---|---|---|
| Time to build the model (in Secs) | 419.75 | 0.09 | 13.75 | 27382.63 |
| Correctly Classified Instances | 65341 | 65158 | 56419 | 64599 |
| Incorrectly Classified Instances | 193 | 376 | 9115 | 935 |
| Prediction Accuracy | 99.705 % | 99.4263% | 86.0912 % | 98.5733% |

The performances of the four models were evaluated based on the three criteria, the prediction accuracy, learning time and error rate and illustrated in Figures 1, 2 and 3.

**Table 2**
**Comparison of Estimates**

| *Evaluation criteria* | *Classifiers*<br>***J48*** | ***IBK*** | ***NB*** | ***MLP*** |
|---|---|---|---|---|
| Kappa Statistic | 0.9949 | 0.99 | 0.7716 | 0.9751 |
| Mean Absolute Error(MAE) | 0.0017 | 0.0028 | 0.0557 | 0.0065 |
| Root Mean Squared Error (RMSE) | 0.0335 | 0.0426 | 0.2308 | 0.0713 |
| Relative Absolute Error (RAE) | 0.7465% | 1.2009% | 24.2277% | 2.846% |
| Root Relative Squared Error (RRSE) | 9.88% | 11.9782% | 68.0942% | 21.0205% |

**Table 3**
**Comparison of Evaluation Measures by Classifiers**

| *Classifier* | *TP Rate* | *FP Rate* | *Precision* | *Recall* | *Class* |
|---|---|---|---|---|---|
| J48 | 0.998 | 0.003 | 0.997 | 0.998 | Normal |
| | 0.999 | 0.001 | 0.999 | 0.999 | DOS |
| | 0.929 | 0 | 0.959 | 0.929 | R2L |
| | 0.992 | 0 | 0.995 | 0.992 | Probe |
| | 0.5 | 0 | 0.667 | 0.5 | U2R |
| IBK | 0.996 | 0.006 | 0.994 | 0.996 | Normal |
| | 0.998 | 0.002 | 0.996 | 0.998 | DOS |
| | 0.885 | 0.001 | 0.91 | 0.885 | R2L |
| | 0.986 | 0.001 | 0.993 | 0.986 | Probe |
| | 0.429 | 0 | 0.75 | 0.429 | U2R |
| NB | 0.825 | 0.063 | 0.937 | 0.878 | Normal |
| | 0.948 | 0.02 | 0.965 | 0.948 | DOS |
| | 0.423 | 0.016 | 0.181 | 0.254 | R2L |
| | 0.762 | 0.043 | 0.648 | 0.7 | Probe |
| | 0.821 | 0.042 | 0.008 | 0.016 | U2R |

*Contd..*

| | | | | | |
|---|---|---|---|---|---|
| MLP | 0.995 | 0.022 | 0.981 | 0.995 | Normal |
| | 0.983 | 0.001 | 0.998 | 0.983 | DOS |
| | 0.692 | 0.002 | 0.737 | 0.692 | R2L |
| | 0.977 | 0.001 | 0.99 | 0.977 | Probe |
| | 0.179 | 0 | 0.5 | 0.179 | U2R |

**Table 4**
**Confusion Matrix of the Classifiers**

| *Classifiers* | *Normal* | *DOS* | *R2L* | *Probe* | *U2R* |
|---|---|---|---|---|---|
| J48 | 34750 | 22 | 16 | 27 | 6 |
| | 18 | 24009 | 0 | 2 | 0 |
| | 37 | 1 | 509 | 0 | 1 |
| | 38 | 5 | 6 | 6059 | 0 |
| | 13 | 1 | 0 | 0 | 14 |
| IBK | 34666 | 69 | 47 | 36 | 3 |
| | 48 | 23975 | 0 | 6 | 0 |
| | 61 | 1 | 485 | 0 | 1 |
| | 69 | 19 | 0 | 6060 | 0 |
| | 15 | 0 | 1 | 0 | 12 |
| NB | 28731 | 597 | 1036 | 2345 | 2112 |
| | 997 | 22780 | 4 | 152 | 96 |
| | 29 | 8 | 232 | 34 | 245 |
| | 896 | 232 | 6 | 4653 | 321 |
| | 0 | 0 | 4 | 1 | 23 |
| MLP | 34632 | 45 | 86 | 54 | 4 |
| | 361 | 23616 | 46 | 5 | 1 |
| | 169 | 0 | 379 | 0 | 0 |
| | 133 | 8 | 0 | 5967 | 0 |
| | 20 | 0 | 3 | 0 | 5 |

Confusion matrices are very useful for evaluating classifiers. The columns represent the predictions, and the rows represent the actual class. To evaluate the robustness of the classifier, the normal methodology is to perform cross validation on the classifier. In general, ten fold cross validation has been proved to be statistically good enough in evaluating the performance of the classifier.

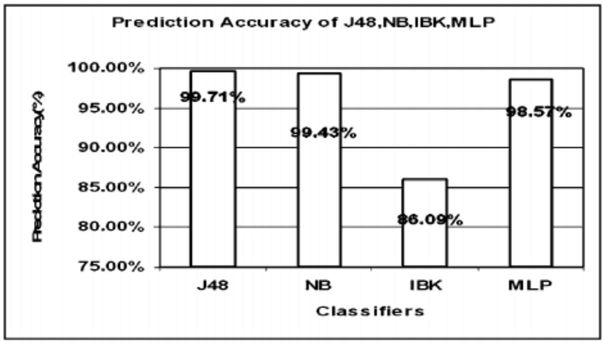

**Fig. 1: Prediction Accuracy**

As shown in Fig. 1 J48 a Decision Tree Classifier predicts better than other algorithms. Among the four classifiers used for the experiment, the decision tree induction algorithm (J48) and NB makes a little difference in the Prediction Accuracy. Multilayer perceptron algorithm provides more or less the same prediction accuracy. The accuracy rate of Instance Based classifier is the lowest among the four machine learning techniques.

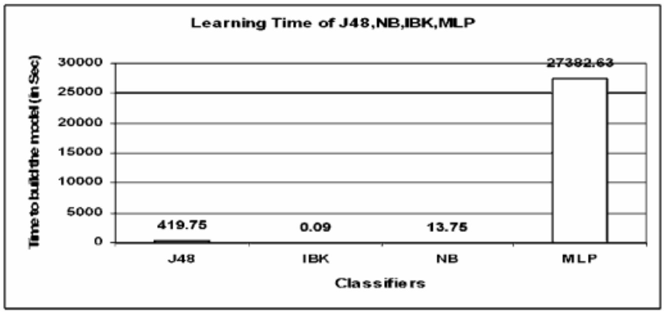

**Fig. 2: Learning Time of Four Classifiers**

Figure 2 illustrates the learning time of the four schemes under consideration. Multilayer perceptron, the neural network classifier consumes more time to build the model. The Naïve Bayes, the probabilistic classifier tends to learn more rapidly for the given dataset. There is a little statistical difference in the time taken to build the decision tree model and probabilistic model. Figure 3 show the Correctly Classified Instances Vs Incorrectly Classified Instances.

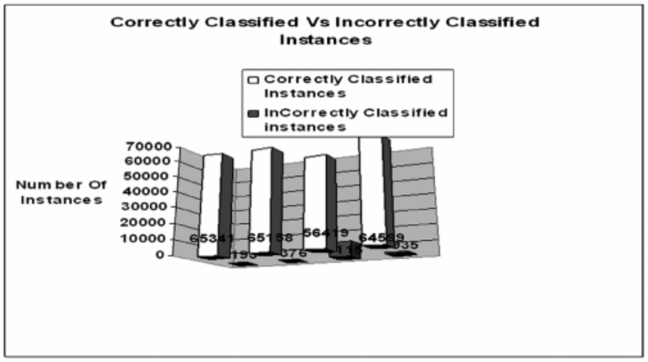

**Fig. 3: Error Rate of Correctly Classified Instances Vs Incorrectly Classified Instances**

The machine learning techniques weka.classifier. bayes.NaïveBayes, weka.classifiers .functions. Multilayer perceptron, weka.classifiers. trees. J48, weka. classifiers.lazy.IBk were used for training the dataset. The 10-fold cross validation was performed to test the performance of the four models. The prediction accuracy of the models was compared.

Good results correspond to large numbers down the main diagonal and small, ideally zero, off-diagonal elements. From the confusion matrix given in Table IV, it is observed that J48, IBK and MLP produce relatively good results. The Naïve Bayes classifier's confusion matrix has large numbers down the off-diagonal elements. The results strongly suggest that machine learning can aid in the prediction of attack categories.

## 6. CONCLUSION

In the research work, four supervised machine learning schemes were applied on the intrusion datasets e assessment data to predict the attack risk of the network environment and the performance of the learning methods were evaluated based on their predictive accuracy and ease of learning. The results indicate that the C4.5 decision tree Classifier outperforms in prediction than Multilayer Perceptron classifier, Instance Based Learning and Naïve Bayes methods. Although the Classification Accuracy between J48 of 99.70 % and IBK of 99.42 % makes little difference, the Computational Performance differs significantly. As the nature of the application demands more accurate prediction than the learning time, it is suggested that the C4.5 the Decision Tree Classifier may be practically used by the Network Security Professional or the Administrators to assess the risk of the attacks.

## REFERENCES

[1] The 1998 Intrusion Detection Off-line Evaluation Plan. MIT Lincoln Lab., Information Systems Technology Group., 25 March 1998. http://www.11.mit.edu/IST/ideval/docs/1998/id98-eval-11.txt

[2] Knowledge Discovery in Databases DARPA archive. Task Description. http://www.kdd.ics.uci.edu/databases/kddcup99/task.htm

[3] Ian H.Witten, et al, “Weka: Practical Machine Learning Tools and Techniques with Java Implementations,” Working Paper 99/11, Department of Computer Science, The University of Waikato, Hamilton, 1999.

[4] Ian H.Witten, Eibe Frank (2005), “Data Mining – Practical Machine Learning Tools and Techniques,” 2nd Edition, Elsevier, 2005.

[5] Sabhnani, M. and G. Serpen (2003), “Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context”, *Proceedings of the International Conference on Machine Learning, Models, Technologies and Applications (MLMTA 2003)*, Las Vegas, NV.

[6] Mark A. Hall (2008), “Practical Feature Subset Selection for Machine Learning.

[7] Pradeep Singh (2009), “Comparing the Effectiveness of Machine Learning Algorithms for Defect Prediction“, *International Journal of Information Technology and Knowledge Management*, July-December 2009, **2**, No. 2, pp. 481-483.