A STUDY ABOUT THE CONSTRUCT AN INTRUSION DETECTION SYSTEM USING EFFECTUAL CLASSIFIER

*****

K.Sivasakthi,
Research Scholar,
Department Of Computer Science,
Christhu Raj College, Trichy.
Email: shaku.ngrkl@gmail.com
Mobile No:9894499088

Dr.RamalingamSugumar,
Professor&Head,
Department Of Computer Science,
Christhu Raj College,Trichy.
Email:rsugusakthi1974@gmail.com
Mobile No:9944221562

ABSTRACT: Unique with the massive development of the utilization of web and improvement in web applications running on different stages is turning into the significant focuses of attacks. New dangers are regularly making by people and associations that attack arrange frameworks. Intrusion is a vindictive, remotely instigated operational deficiency. Intrusion is utilized as a key to bargain the honesty, accessibility, and privacy of a pc attack. Consequently, the Intrusion Detection System (IDS) is turning into a critical piece of framework safeguard to recognize peculiarities and aggression in the system. Information mining based IDS can viably identify intrusions. In this paper, we propose an Effectual Classification Algorithm (ECA) to improve the accuracy rate of the classifier. To assess the presence of our proposed framework, we led probes KDD-CUP 99 informational index. Exact outcomes show that the proposed model dependent on ECA is active with the accuracy rate.

KEYWORDS: Intrusion Detection, Effectual Classification Algorithm (ECA), KDD-CUP 99,Feature selection.

INTRODUCTION: The Intrusion Detection System (IDS) manages an enormous measure of information and assumes a significant job in recognizing different sorts of attacks.

Intrusion Detection System (IDS) can be considered as characterization issue. Intrusion can be Characterized as malicious, remotely prompted, and operational flaw. Intrusion is a key to bargain accessibility, uprightness, and privacy of a PC framework. Subsequently, intrusion identification frameworks are turning into a key piece of framework resistance to distinguish abnormalities and attacks in the system. Information mining is the way toward extricating valuable data from immense stores. Intrusion Detection System (IDS) successfully recognizes these data and predicts the outcomes that can be utilized in the future. In information mining, characterization is one of the most significant procedures applied to interruption location. In this work, we proposed efficient IDS based on the ECA classifier. ECA enhances overall attack detection accuracy.

RELATED WORK: In writing, a few information-digging procedures are applied for Intrusion Detection System (IDS). Every strategy has its preferences and weaknesses. Execution of each model differs as far as DR, FAR, and precision**.** Arif & Waseem proposed IDS to identify the standard and attacked nodes using the ANN classification technique. They use the NSL-KDD dataset and find out the four attacks

(DOS,U2R,R2L,Probe) with the overall detection rate of 95.05. Basant & Santosh developed a network intrusion detection model based on data mining technology. They were using c4.5 decision tree algorithms and detected DOS (Denial Of Service) with a detection rate of 95.0%. Yanijie Zhao proposed an intrusion detection model using chi-square feature selection and multi-class support vector machine to identify the standard or multiple attacked classes. They use NSL-KDD data sets and achieve 96% detection accuracy. Sumaiyan & A.Aswani constructs an IDS using decision tree classification algorithm, and they achieve 89.95% detection accuracy. Mohammed A.Ambusaii build an intrusion detection system, and they find out the four attacks, with an overall accuracy rate of 97.33%.

DATASET DESCRIPTION: Since 1999, KDD'99 has been the most uncontrollably utilized informational collection for the assessment of inconsistency location strategies. This informational index is set up by Stolfo et al, and is fabricated dependent on the information caught in the DARPA'98 IDS assessment program and is generally applied to assess the exhibition of interruption recognition frameworks. It comprises five distinct classes, which are normal and four sorts of attacks (i.e., DOS, Probe, U2R, and R2L). It contains preparing information with roughly five mil-lion association records and test information with around 2,000,000 association records. Each file in these datasets is marked as either ordinary or an assault, and it has 41 diverse quantitative and subjective highlights.

Attacks in this dataset are categorized as four types

1) DOS attack
2) Probe attack
3) U2R
4) R2L

DENIAL OF SERVICE: DOS attack is an endeavor to make a machine (or) asset inaccessible to is proposed clients, for example, incidentally or uncertainly intrude (or) suspend administration of a host associated with the web.

PROBE: Probe is an attack, where the programmer checks a machine or a systems administration gadget to decide shortcoming or vulnerabilities that might be later abused.

USER TO ROOT ATTACK: U2R class distinguishes unapproved access to nearby super-user (root) benefits. These attacks are misuses in which the program begins on the framework with a typical client record and endeavors to mishandle vulnerabilities in the structure to pick up super-user benefits.

REMOTE TO LOCAL: R2L class distinguishes unapproved access from a machine. The attacker doesn't have a record on the unfortunate casualty machine, thus attempts to obtain entrance.

PERFORMANCE EVALUATION: The experiments have been conducted to evaluate the performance of the proposed work. The accuracy metric is defined by th

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

Where True Positive (TP) is the number of genuine attacks delegated attacks, True Negative (TN) is the quantity of real ordinary records named typical ones; False Positive (FP) is the quantity of actual conventional files titled attacks, and False Negative (FN) is the number of real attacks named typical records.

ECA (Enhanced Classification Algorithm)

The proposed intrusion identification framework utilizes the ECA calculation to distinguish the attacks. It is the ideal optimal choice of probability classifier. The previous work utilizes FMIFS+LS-SVM to recognize the five classes (normal, dos, probe, U2R, R2L). The FMIFS is used to evacuate the redundancies between the attributes. Utilizing FMIFS 19 features used just by the LS-SVM and identifies the attacks. LS-SVM isn't working well in the maximal number of features. The overall accuracy rate 97.33%, rather than lessening elements, the proposed work takes all the 41 functions of the KDD CUP 99 dataset and utilizations the ECA to detect the accuracy with 99.63%.

Method used for classifying the object into the different class is defined as

$P(X£Ci) = Max(\sum P(Fi)/P(Ci))$

X➔ Object has taken for classification.

Ci➔ No.of classes

Fi➔ No.of features

ALGORITHM

Step1: Read the training dataset T.

Step2: Calculate the probability for each class ei.

Step3: Calculate the probability of fi (each feature) with ei(each class).

Step4: Repeat step3 until the probability of all predictor variables(f1,f2,f3…fn) has been calculated.

Step5: Calculate the likelihood for each class.

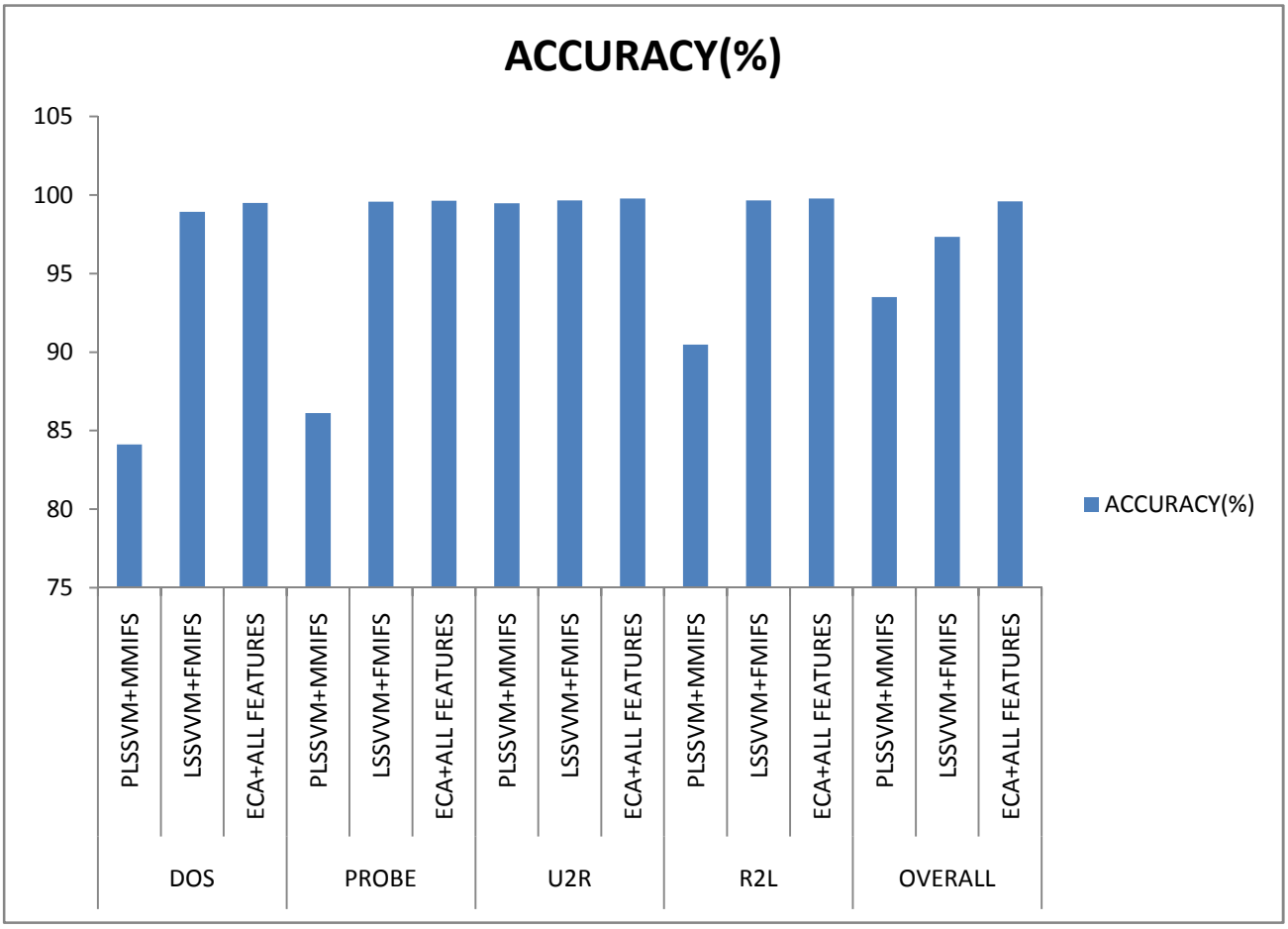
Step6: Get the highest likelihood.

EXPERIMENT RESULT: To exhibit the presentation of proposed work, the investigation directed on KDD CUP 99. The KDD CUP 99 is one the most mainstream far-reaching intrusion location datasets and is broadly applied to assess the exhibition of intrusion recognition frameworks. It contains five different classes regular and four various attacks (Dos,Probe,U2R, and R2L). It consists of millions of training data, and it has 41 features. To determined the execution of the ECA + ALL FEATURES, tests have been led to make correlations with different approaches.

.COMPARISON TABLE

CLASS NAME	MODEL	ACCURACY(%)
DOS	PLSSVM+MMIFS LSSVVM+FMIFS ECA+ALL FEATURES	84.11 98.93 99.50
PROBE	PLSSVM+MMIFS LSSVVM+FMIFS ECA+ALL FEATURES	86.12 99.57 99.64
U2R	PLSSVM+MMIFS LSSVVM+FMIFS ECA+ALL FEATURES	99.47 99.66 99.78
R2L	PLSSVM+MMIFS LSSVVM+FMIFS ECA+ALL FEATURES	90.47 99.66 99.78
OVERALL	PLSSVM+MMIFS LSSVVM+FMIFS ECA+ALL FEATURES	93.50 97.33 99.63

ACCURACY COMPARISON CHART WITH OTHER ALGORITHMS



The above table and chart summarizes the classification of the various techniques as to precision rate. It shows obviously that the classification model joined with MMIFS+PLS-SVM has accomplished the overall accuracy rate of 93.50%, the recognition model with FMIFS+LS-SVM has accomplished the overall accuracy rate of 97.33% and the proposed model with all features + ECA has accomplished the 99.63% overall accuracy rate individually. With respect to results acquired by different creators, it very well may be seen that the proposed approach appreciates the best exactness among all models.

CONCLUSION: In this paper, we proposed an effectual classifier algorithm (ECA) to detect four types of attacks DOS, Probe, U2R, and R2L. The proposed approach is compared and evaluated using KDD CUP 99 dataset. Experimental results prove that the proposed model (ECA) + all features produce an improved accuracy rate compared with other detection systems tested on the same dataset. Finally, based on the result achieved on the KDD CUP99 dataset, it can be concluded, the proposed detection model has achieved promising performance in detecting intrusion over computer networks.

REFERENCES

1. D.Powell and R.Stroud, “Conceptual model and architecture”, Deliverable D2, Project MAFTIA ISI-19993-11583,IBM Zurich research laboratory research report R23377 Nov(2011).
2. G V Nadiammai “Effective Approach Towards Intrusion Detection System Using Data Mining Techniques” Egyption Informatics Journal 15, pp 37-50(2014).
3. M.A Jabbar,B.LDeekshstulaePriti Chandra, ”Computational Intelligence Techniques for early diagnosis of heart disease”, ICETECH,IEEE(2015).
4. KDD Cup 1999. Available on: http://kdd.. ics.uci.edu/databases/kddcup 99/kddcup99.html, Ocotber 2007.
5. S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, “Cost-based modeling for fraud and intrusion detection: Results from the jam project,” discex, vol. 02, p. 1130, 2000.
6. R. P. Lippmann, D. J. Fried, I. Graf, J. W. Haines, K. R. Kendall, D. McClung, D. Weber, S. E. Webster, D. Wyschogrod, R. K. Cun-ningham, and M. A. Zissman, “Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation,” discex, vol. 02,
7. A. N. and M. Kahani, “A new approach to intrusion detec-tion based on an evolutionary soft computing model using neuro-fuzzy classifiers,” Comput. Commun., vol. 30, no. 10, pp. 2201–2212, 2007.
8. A. M. Ambusaidi, X. He, and P. Nanda, “Unsupervised feature selection method for intrusion detection system,” in Proc. Int. Conf. Trust, Security Privacy Comput. Commun., 2015, pp. 295–301.
9. A. M. Ambusaidi, X. He, Z. Tan, P. Nanda, L. F. Lu, and T. U. Nagar, “A novel feature selection approach for intrusion detection data classification,” in Proc. Int. Conf. Trust, Security Privacy Com-put. Commun., 2014, pp. 82–89.
10. Arif Jamal Malik, WaseemShahzad, FarrukhAslam Khan, "NetwordlD using hybrid binary PSO and RF algorithm", Security and Communication Network,(2012).
11. BasantSubba, SantoshBiswasSushanlaKarmakar, “ A Neural Network Based System for Intrusion Detection and Classification” 978-1-5090-2361-5/6/$31.00 C 2016 IEEE.
12. Yanjie Zhao, ”Network Intrusion Detection Systn Based on Data Mining”, 978-5090-2239-7/16/2016 IEEE.
13. SumaiyanThaseenIkram,A.Aswani Kumar Cherukuri, ”Intrusion Detection Model Using Fusion of Chi-square Feature Selection and Multiclass SVM”, Published on Science Direct on 3, December 2015.
14. LekhrajMehra, Harpreet Singh Gill, “ An Effectual & Secure Approach for the Detection And Efficient Searching of Network Intrusion Detection System”, Published on IEEE International Conference On Computer and Control 2015.
15. Bagheri,Wei Lu and Ali A.Ghorbani,”A Detailed Analysis of the KDD CUP 99 Data Set” IEEE On Computational Inelligence in Security and Defense Application 2009.
16. Mohammed A.Ambusaidi, Member IEEE,XiangianHe,Senior Member, “Building An Intrusion Detection System Using a Filter-Based Feature Selection Algorithm, IEEE Transaction On Computers, Vol 65, October 2016.
17. C.F.Tasi,Y.F.Hsu,C.Y.Lin and W.Y.Lin,”Intrusion detection by machine learning: A review”, Expert Syst with Appl.,vol 36,no.10.pp.11994-12000,2009.