International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-6 Issue-1, June 2016

An Efficient Random Iterative Based Particle Swarm Optimization for Intrusion Detection

Sonal M. Wange, Shiv K. Sahu, Amit Mishra

Abstract— In this paper, an efficient intrusion classification has been proposed by the help of association rule and random iterative based particle swarm optimization NSL-KDD dataset has been used for the experimentation. This is done by the separation of nodes by receiving and sending. Then it is examined for malicious behavior. RIPSO is applied then to examine the approved threshold value for the detection of different intrusion types defined. If the value obtained after RIPSO iteration passed the threshold assigned, then it will be categorized as the specific intrusion and type will identified. Denial of Service (DoS), User to Root (U2R), Remote to User (R2L) and Probing (Probe) attacks is considered in this paper for intrusion detection. The results show the improvement in detection as compared to the previous method. The average accuracy obtained by our approach is 91.3 %.Index

Keywords— RIPSO, Intrusion Detection, DoS, U2R, R2L and Probe.

I. INTRODUCTION

Now a days there are special focus is on the detection of malicious behavior in the network as all the business processing are relies on any type of network. The Association for Computing Machinery (ACM) has been gathered different network malicious and non-malicious behavior data in a Knowledge Discovery and Data mining (KDD) platform [1] for the data mining understudies and experts. They have provided a set KDD Cup99 data sets for network intrusion detection [2]. This gathering is use for intrusion recognition and a few specialists had considered this as the benchmark dataset for result examination.

As of late, various specialists are focusing to use data burrowing thoughts for Intrusion Detection [3]. This is a strategy to think the undeniable information and learning. Interruption disclosure is the philosophy of malignant ambush in the structure and framework when we are in no time correspondence or isolating data in the steady environment [4][5]. Since its development, interference area has been one of the key segments in fulfilling information security. It goes about as the second-line obstruction which supplements the passage controls. Exactly when the controls failed, the intrusion ID systems should have the ability to remember it consistent and alert the security officers to take incite and suitable exercises [5] [6]. Interference acknowledgment structure oversee managing the scenes happening in PC structure or framework circumstances and taking a gander at them for signs of possible events, which are infringement or certain perils to PC security, or standard security sharpens Intrusion recognizable proof systems (IDS) have ascended to recognize exercises which imperil the uprightness, protection or availability of are source as a push to give a response for existing security issues [7-10]. So in the above course we ponder a couple of points of view in the subsequent sections. We similarly discuss data mining and headway procedures, in light of the fact that it can be used as a piece of forming the structure which conveys better distinguishing proof system. As we are inspected this study toward a prevalent framework with the blend of data mining and streamlining .These systems are useful and has been used as a piece of differing procedures like [11-14]. So the use of these estimations can enhance an impact.

II. LITERATURE SURVEY

In 2012, P. Prasenna et al. [15] suggested that in standard framework security just relies on upon numerical computations and low counter measures to taken to turn away intrusion recognizable proof system, but the lion's share of this approachs to the extent theoretically tried to execute. Makers recommend that instead of delivering generous number of standards the progression change methods like Genetic Network Programming (GNP) can be used .The GNP is in perspective of composed chart. They focus on the security issues related to send a data mining-based IDS in a consistent circumstance. They total up the issue of GNP with connection standard mining and propose a feathery weighted association rule mining with GNP framework suitable for both consistent and discrete qualities.

In 2011, LI Han [16] focuses on interference disclosure in light of collection examination. The fact of the matter is to improve the acknowledgment rate and decrease the false alert rate. A balanced component K-suggests count called MDKM to recognize irregularity activities is proposed and relating reenactment investigations are presented. Firstly, the MDKM figuring channels the upheaval and isolated spotlights on the data set. Additionally by finding out the divisions between all illustration data centers, they secure the high-thickness parameters and gathering part parameters, using component iterative strategy we get the k clustering concentrate exactly, then a peculiarity revelation model is shown. They used KDD CUP 1999 data set to test the execution of the model.

Manuscript published on 30 June 2016.
***Correspondence Author(s)
Sonal M. Wange, Technocrats Institute of Technology, Bhopal (M.P). India.
Dr. Shiv K. Sahu, Technocrats Institute of Technology, Bhopal. (M.P). India.
Prof. Amit Mishra, Technocrats Institute of Technology, Bhopal (M.P). India.

Their results exhibit the structure has a higher acknowledgment rate and a lower false alert rate, it accomplishes confident point.

In 2011, Z. Muda et al. [17] discuss the issue of current anomaly recognizable proof that it not ready to recognize an extensive variety of ambushes viably. To beat this issue, they propose a crossbreed learning approach through mix of K-Means bundling and Naïve Bayes portrayal. The proposed philosophy will be gathering all data into the looking at assembling before applying a classifier for request reason. An examination is done to evaluate the execution of the proposed technique using KDD Cup '99 dataset. Come about exhibit that the proposed philosophy performed better in term of precision, area rate with sensible false alert rate.

In 2014, Deshmukh et al. [18] introduces a Data Mining framework in which distinctive preprocessing procedures will be incorporated, for example, Normalization, Discretization and Feature decision. With the assistance of these strategies the data will be preprocessed and obliged highlights are picked. They used NaIve Bayes framework in coordinated learning methodology which assembles distinctive framework events for the KDD cup'99 Dataset.

In 2014, Benaicha et al. [19] show a Genetic Algorithm (GA) approach with an upgraded beginning masses and decision executive, to capably distinguish diverse sorts of framework intrusions. They used GA to improve the look of ambush circumstances in audit reports, on account of its awesome balance examination/abuse; according to the makers it gives the subset of potential attacks which are show in the survey archive in a sensible get ready time. The testing time of the Network Security Laboratory Knowledge Discovery and Data Mining (NSL-KDD99) benchmark dataset has been used to recognize the mishandle works out. Their system of IDS with Genetic estimation increases the execution of the recognizable proof rate of the Network Intrusion Detection Model and declines the false positive rate.

In 2014 Kiss et al. [20] suggest that Modern Networked Critical Infrastructures (NCI), including advanced and physical systems, are introduced to sharp computerized attacks concentrating on the unfaltering operation of these structures. To ensure variation from the norm care, their watched data can be used as a piece of concurrence with data mining methods to make Intrusion Detection Systems (IDS) or Anomaly Detection Systems (ADS). They proposed a gathering based philosophy for recognizing advanced strikes that cause idiosyncrasies in NCI. Distinctive clustering methodologies are examined to pick the most suitable for gathering the time-course of action data highlights, hence portraying the states and potential computerized attacks to the physical structure. The Hadoop execution of Map Reduce standard is used to give a suitable planning environment to broad datasets.

In 2014, Thaseen et al. [21] proposed a novel procedure for organizing crucial fragment examination (PCA) and support vector machine (SVM) by overhauling the piece parameters using customized parameter determination framework. Their procedure diminishes the arrangement and testing time to recognize interferences therefore upgrading the precision. Their proposed methodology was attempted on KDD data set. The datasets were carefully parceled into planning and testing considering the minority ambushes, for instance, U2R and R2L to be display in the testing set to recognize the occasion of cloud strike. Their results demonstrate that the proposed procedure is viable in perceiving interferences. Their exploratory results exhibit that the request precision of the proposed framework defeats other course of action methodologies using SVM as the classifier and other dimensionality lessening or highlight decision frameworks.

In 2014, Wagh et al. [22] proposed Network security is a key a portion of web enabled systems in the present world circumstance. According to the makers as a result of confusing chain of PCs the open entryways for intrusions and strikes have extended. Along these lines it is need of extraordinary significance to find the best courses possible to secure our structures. So the makers propose intrusion distinguishing proof structure is expecting essential part for PC security. The best methodology used to handle issue of IDS is machine learning. Thy watched that the rising field of semi managed learning offers an ensured course to correspond investigation. So they proposed a semi-oversaw framework to reduce false ready rate and to improve revelation rate for IDS.

In 2014, Masarat et al. [23] displayed a novel multistep structure considering machine learning methodology to make a capable classifier. In initial step, the highlight decision strategy will execute considering get extent of highlights by the makers. Their system can upgrade the execution of classifiers which are made considering these highlights. In classifiers blend step, we will show a novel soft assembling method. Along these lines, classifiers with more execution and lower cost have more effect to make the last classifier.

In 2015,Yan et al. [24] focusing at false negative rate and false alarm rate which exist generally in the intrusion detection system. They have proposed an intelligent intrusion detection model. Based on the characteristics of global superiority of genetic algorithm and locality of nerve, the model optimizes the weights of the neural network using genetic algorithm. Their experiment results show that the intelligent waycan improve the efficiency of the intrusion detection.

III. PROPOSED METHOD

In our approach we have considered the dataset of NSL-KDD. It is a data set which does not include redundant record and test sets. Then we consider equal proportion 10,000 dataset from the whole dataset. We first separation it into two sections taking into account normal establishment and termination. At that point we consider the ordinary information set and for discovering the interruptions we compute the intrusions in light of the coordinating component. At that point we apply random PSO system for the intrusion classification. In the event that the worth crosses the farthest point esteem then the node will be included into the attack class. At last taking into account the attack class of Denial of Service (DoS), User to Root (U2R), Remote to User (R2L) and Probing (Probe) we find the final classification.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Our results support better classification in comparison to the previous techniques used in several research papers as per our study. Figure 1 shows the flowchart of my proposed technique. Data separation is completely based on the fourth field. The data is categorized based on the two different data properties that are normal entry and termination. The normal data is checked for the final receiving adequacy that the data is received finally with success or not. If yes then the data comes in the normal category otherwise that data lies in the attack category. This data is first classified by the association rule mining and support value obtained. Then the below algorithm is applied for the checking the maximum threshold so that data can be checked for the minimum qualification criteria. Random Iterative Particle Swarm Optimization (RIPSO) RIPSO is applied for checking the maximum threshold so that data it can be checked for the minimum qualification criteria. The applied algorithm is shown below.

Input:

IPS(ips1,ips2….ipsn)

OPS(ops1,ops2….opsn)

Output:

DT1…….DTn

IPS: Input particle set

OPS: Output particle set

DT: Distributed trails

VT: Velocity trails

RVT: Random velocity trails

PRVT: Previous random velocity trails

N: Number of iterations

DAC: Detection accuracy

DTP: Previous distributed trail

Step 1: Input selected NSL KDD dataset

Step 2: Particle value is initialized by the associated rule dataset

Step 3: Random velocity calculation and assigned in each iterations

for i=0 ; i<=n; i++

RVT =Math. random();

Step 4: Data Assignement

for i=0 ; i<=n; i++

DT=(ips1*RVT1 + ips2*RVT1 + ips3*RVT1 +…. + ipsn*RVT1)/n

If (Vt1 > Vtn-1)

Vt1 = Vtn-1

PRVT1=RVT1

DTP=DT1

For above than 2

DTi=DTi-1 + (ips1*RVTi + ips2*RVTi + ips3*RVTi +…. + ipsn*RVTi)/n- PRVT

If (Vt1 > Vtn-1)

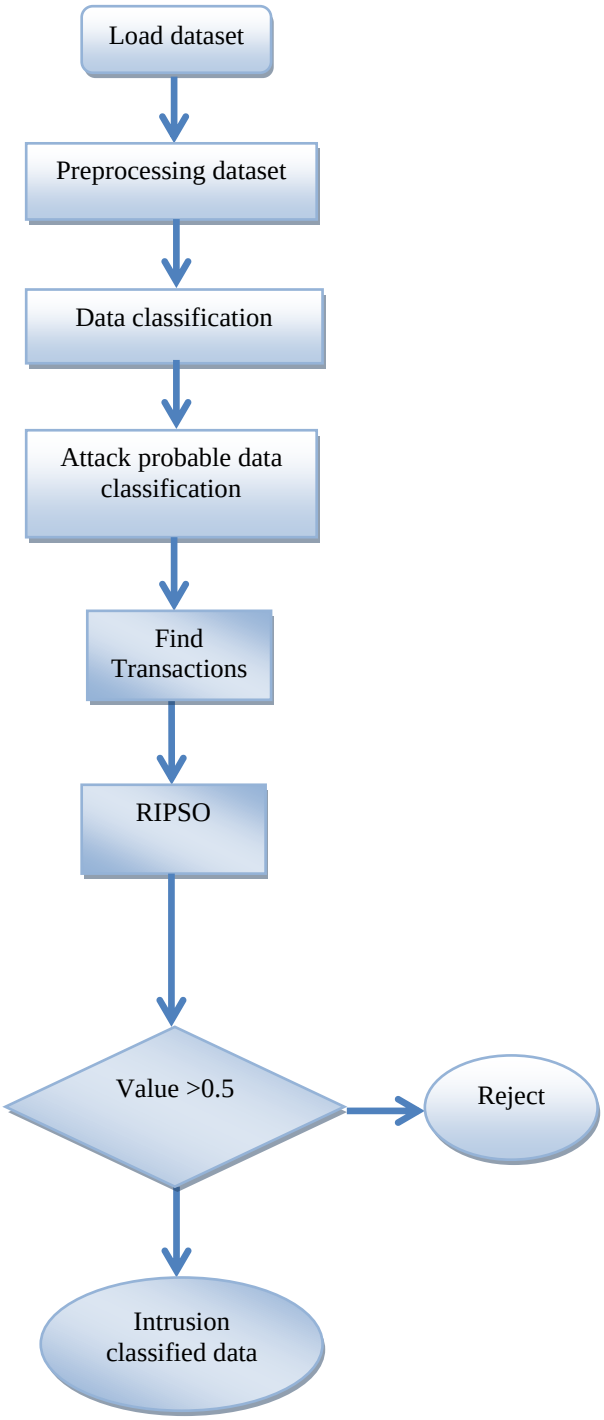
Vtn = Vtn-1

PRVTn = RVTn

Step 5: Detection accuracy

DAC=$\sum DT_i / n$

Step 6: Finish



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV. RESULT

For result evaluation normal data set has been considered for final data refinement. It is based on the receiving data node if it is not received as the normal then it should be checked for attack node. Associated data is first refined based on the content features, traffic features and hot features. Then we have applied RIPSO for checking the maximum threshold classification of each attribute presented in the database. The threshold value is 50 % means all the attributes which can cross this validation will be abstracted and contributed in any type of attack. Different ranges are considered for result evaluation and comparison. In which three ranges are considered for result evaluation. The results are shown in Table 1 to 4. The comparison showed in figure 2 shows that our results are improved from traditional approach in DOS, U2R and Probe.

Table 1: Detection Result Total

Model	Average Accuracy
Proposed Approach	**91.3 %**
Previous Accuracy [34] (%)	**85.87 %**

Table 2: Attack Type Comparison [Range: 98113-106591]

Attack Type	Proposed Accuracy (%)	Previous Accuracy [34](%)
DOS	100	97.1
R2L	66.66	80.5
U2R	98.66	83.9%
Probe	100	82

Table 3: Attack Type Comparison [Range: 98112-105377]

Attack Type	Proposed Accuracy (%)	Previous Accuracy [34] (%)
DOS	100	97.1
R2L	66.66	80.5
U2R	98.48	83.9%
Probe	100	82

Table 4: Attack Type Comparison [Range: 90846-102955]

Attack Type	Proposed Accuracy (%)	Previous Accuracy [34](%)
DOS	100	97.1
R2L	75	80.5
U2R	98.91	83.9%
Probe	100	82

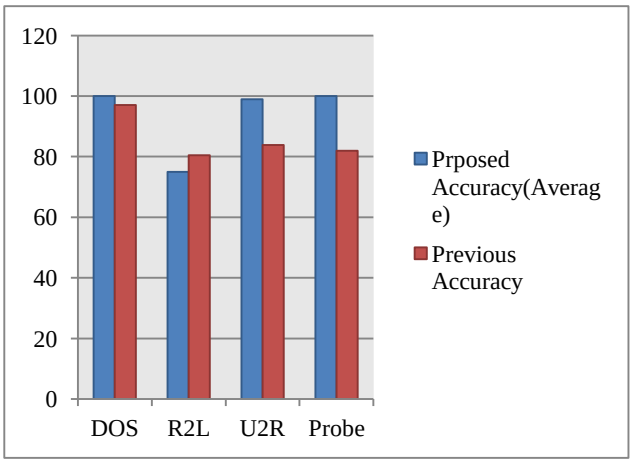


Figure 2: Classification accuracy.

V. CONCLUSION

In this paper, we have applied random iterative based particle swarm optimization (RIPSO) with random iteration support. For this we are using NSL-KDD dataset. This is done by the separation of nodes by receiving and sending. Then it is examined for malicious behavior. RIPSO is applied then to examine the approved threshold value for the detection of different intrusion types defined. If the value obtained after RIPSO iteration passed the threshold assigned, then it will be categorized as the specific intrusion and type will identified. Denial of Service (DoS), User to Root (U2R), Remote to User (R2L) and Probing (Probe) attacks is considered in this paper for intrusion detection. The results show the improvement in detection as compared to the previous method.

REFERENCES

1. Alexander O. Tarakanov, Sergei V. Kvachev, Alexander V. Sukhorukov ," A Formal Immune Network and Its Implementation for On-line Intrusion Detection", Lecture Notes in Computer Science Volume 3685, pp 394- 405, 2005.
2. Ranjna Patel, DeepaBakhshi and TriptiArjariya, " Random Particle Swarm Optimization (RPSO) based Intrusion Detection System " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-5, April-2015 ,pp.60-66.
3. MengJianliang,ShangHaikun,Bian Ling," The Application on Intrusion Detection Based on K-means Cluster Algorithm", International Forum on Information Technology and Applications, 2009.
4. Lundin, E. and Jonsson, E. "Survey of research in the intrusion detection area", Technical Report, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden. January 2002.
5. R.Venkatesan, R. Ganesan, A. Arul Lawrence Selvakumar, " A Comprehensive Study in Data Mining Frameworks for Intrusion Detection " , International Journal of Advanced Computer Research (IJACR), Volume-2, Issue-7, December-2012 ,pp.29-34.
6. S.Devaraju, S.Ramakrishnan:,"Analysis of Intrusion Detection System Using Various Neural Network classifiers, IEEE 2011.
7. Moriteru Ishida, Hiroki Takakura and Yasuo Okabe," High-Performance Intrusion Detection Using OptiGrid Clustering and Grid-based Labelling", IEEE/IPSJ International Symposium on Applications and the Internet, 2011.
8. S. T. Brugger, "Data mining methods for network intrusion detection",pp. 1-65, 2004.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

9. W. Lee, S. J. Stolfo, "Data Mining Approaches for Intrusion Detection",Proceedings of the 1998 USENIX Security Symposium, 1998.
10. KaminiNalavade, B.B. Meshram, "Mining Association Rules to Evade Network Intrusion in Network Audit Data" , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.560-567.
11. W. Lee, S. J. Stolfo, "Data mining approaches for intrusion detection" Proc. of the 7th USENIX Security Symp.. San Antonio, TX, 1998.
12. ReyadhNaoum, Shatha Aziz, FirasAlabsi, "An Enhancement of the Replacement Steady State Genetic Algorithm for Intrusion Detection", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014, pp.487-493.
13. AdityaShrivastava, MukeshBaghel, Hitesh Gupta, " A Review of Intrusion Detection Technique by Soft Computing and Data Mining Approach " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-12, September-2013 ,pp.224-228.
14. LI Yin–huan , "Design of Intrusion Detection Model Based on Data Mining Technology", International Conference on Industrial Control and Electronics Engineering, 2012.
15. P. Prasenna, R. Krishna Kumar, A.V.T RaghavRamana and A. Devanbu "Network Programming And Mining Classifier For Intrusion Detection Using Probability Classification", Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012.
16. LI Han, "Using a Dynamic K-means Algorithm to Detect Anomaly Activities", Seventh International Conference on Computational Intelligence and Security, 2011.
17. Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir," Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification", 7th International Conference on IT in Asia (CITA), 2011.
18. Deshmukh, D.H.; Ghorpade, T.; Padiya, P., "Intrusion detection system by improved preprocessing methods and Naïve Bayes classifier using NSL-KDD 99 Dataset," Electronics and Communication Systems (ICECS), 2014 International Conference on , vol., no., pp.1,7, 13-14 Feb. 2014.
19. Benaicha, S.E.; Saoudi, L.; BouhouitaGuermeche, S.E.; Lounis, O., "Intrusion detection system using genetic algorithm," Science and Information Conference (SAI), 2014 , vol., no., pp.564,568, 27-29 Aug. 2014.
20. Kiss, I.; Genge, B.; Haller, P.; Sebestyen, G., "Data clustering-based anomaly detection in industrial control systems," Intelligent Computer Communication and Processing (ICCP), 2014 IEEE International Conference on , vol., no., pp.275,281, 4-6 Sept. 2014.
21. Thaseen, I.S.; Kumar, C.A., "Intrusion detection model using fusion of PCA and optimized SVM," Contemporary Computing and Informatics (IC3I), 2014 International Conference on , vol., no., pp.879,884, 27-29 Nov. 2014.
22. Wagh, S.K.; Kolhe, S.R., "Effective intrusion detection system using semi-supervised learning," Data Mining and Intelligent Computing (ICDMIC), 2014 International Conference on , vol., no., pp.1,5, 5-6 Sept. 2014.
23. Masarat, S.; Taheri, H.; Sharifian, S., "A novel framework, based on fuzzy ensemble of classifiers for intrusion detection systems," Computer and Knowledge Engineering (ICCKE), 2014 4th International eConferenceon , vol., no., pp.165,170, 29-30 Oct. 2014.
24. Yan C. Intelligent Intrusion Detection Based on Soft Computing. InMeasuring Technology and Mechatronics Automation (ICMTMA), 2015 Seventh International Conference on 2015 Jun 13 (pp. 577-580). IEEE.