Research Article

ACCENTS Transactions on Information Security, Vol 5(20)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2020.517003

An efficient intrusion detection mechanism based on particle swarm optimization and KNN

Anand Vijay[1*], Kailash Patidar[2], Manoj Yadav[2] and Rishi Kushwah[2]
M.Tech Scholar, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[1]
Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[2]

Abstract

In this paper an efficient intrusion detection mechanism based on particle swarm optimization and KNN has been presented. In our approach experimentation has been performed for the intrusion detection considering NSL-KDD dataset. Then the selected weights have been added directly to the final classification which has been received safely. Then the remaining selected weights have been added for the classification. These nodes are originally safe but received unsafe. It has been input for the classification process. KNN has been used for the classification of the initial features and the content features. The remaining features have been transferred to the particle swarm optimization. PSO has been used for the classification of the traffic and host features. It has been classified based on 50% threshold value. The results show that by using our approach the average classification accuracy is approximately 98%. The attack considered here are Denial of Service (DoS), User to Root (U2R), Remote to User /Login (R2L) and Probe.

Keywords

Intrusion detection system, DoS, U2R, R2L and Probe.

1.Introduction

Intrusion detection is an important aspect where there is the need of computational techniques like data mining, artificial intelligence and machine learning [1−4] for the improvement in detection system. It has been found that different algorithms have already been applied in the same direction for the improvement [3−8]. But there are several areas where there is the need of improvement including detection, identification along with the attack types.

Based on the literature it has been found that the intrusion detection is an important aspect in different areas of data sharing and communication [9]. It may be helpful in the identification of malicious and suspicious behavior. It has been done through intrusion detection system (IDS) [10]. These systems have been developed to identify suspicious activities which may be attack prone or it may increase the chances of vulnerable activities [11−14].

Other important aspects are types of intrusion, types of attacks, identification process and the detection process. Detection process includes network, configuration, IP, signature, host, anomaly and configuration. The main objective of this paper is to develop an efficient intrusion detection system.

2.Literature survey

In 2020, Razimi et al. [15] discussed about the surveillance technology. They have proposed an intelligent home surveillance system. IT has been proposed based on the use of Raspberry Pi. It has been triggered when an intruder is captured through the video surveillances.

In 2020, Zoppi et al. [16] discussed about the anomaly detection techniques. It has been discussed in terms of identifying patterns. Their main aim is to instruct the anomaly-based techniques considering unsupervised algorithms. It has been used for the classification of normal and anomalous behaviors.

In 2020, Dang [17] discussed about intrusion detection system. The main task of the detection system is to differentiate benign and malicious

[*] Author for correspondence

network flows. They have discussed the active learning usage. It has been discussed in terms of active learning for the online configuration. It has been discussed for the reduction of labeling cost.

In 2020, Chen et al. [18] discussed about the 5G application and the chances of intrusion detection. They have suggested that the traditional method is relatively insufficient. They have proposed a RLA intrusion detection system for the hybrid network. For the classification support vector machine algorithm has been used. They have achieved 98% accuracy approximately.

In 2020, Jin et al. [19] discussed about the applicability of big data and machine learning algorithms in case of intrusion detection. They have proposed a K-nearest neighbors (KNN) and categorical boosting (CatBoost) for the imbalanced data. For experimentation they have used KDD99 dataset. By this method they have achieved better detection performance.

In 2019, Halimaa and Sundarakantham [20] dicusses about malicious activity and intrusion detection system. They have suggested that the intrusion detection may plays an important role in the network. Hey have suggested the need of classification methodologies. They have applied support vector machine (SVM) and naïve Bayes (NB) algorithm for the classification problem. For experimentation NSL-KDD dataset has been used. Their result suggest that the support vector machine outperforms.

In 2020, Taghavinejad et al. [21] discussed the use of Internet of Things. They have discussed regarding the prevention from the cyber-attack through intrusion detection system. They have used the combination of SVM, KNN and decision tree (DT). Their result shows that the proposed method is found to be better.

In 2020, Mu et al. [22] discussed about the internet intrusion detection. They have discussed the applicability in terms of IP matching and network monitoring. They have also discussed unauthorized access due to various tags.

In 2020, Dawit et al. [23] discussed about cyber security. They have investigated several methods for the intrusion detection collaboration. They have also studied the integration of intrusion detection. They have also studied and discussed the major vulnerabilities in case of blockchain application.

In 2020, Park et al. [24] discussed a prediction model which is based on recurrent neural network. They have discussed this in terms of IoT environment. They have used long short-term memory model. They have used cosine similarity for the scoring function. They have considered a normal packet for the same.

In 2020, Iman and Ahmad [25] discussed about the intrusion detection system development. They have analyses and estimated the use of random forest algorithm. They have considered Boruta algorithm. Their results show that the proposed method is capable of preventing the infinite loop. It is capable in the improvement of the performance.

3.Methods

Our approach is divided into following parts:

Feature preprocessing

In our approach experimentation has been performed for the intrusion detection considering NSL-KDD dataset. There are total 42 nodes in the dataset. 41 nodes have been used for the classification. The complete records in the dataset are 1025973. The initial elements are shown in 1-9. The content features are shown in 10-22. The traffic features are shown in 23-31. The host features are shown in 32-41. These data are first preprocessed based on the feature values.

Selected weight (Direct add)

Then the selected weights have been added directly to the final classification which has been received safely. These nodes do not participate in the classification process as these are already safely received nodes.

Selected weight (Validation)

Then the remaining selected weights have been added for the classification. These nodes are originally safe but received unsafe. These nodes do participate in the classification process.

K-nearest neighbor (KNN)

The validation weights have been transferred to the KNN classifier. It has been used for the classification of the weighted segment. KNN has been used for the classification of the initial features and the content features. The first part has been used for the classification of segregated data from these features. It has been classified based on 50% threshold value.

PSO

The remaining features have been transferred to the particle swarm optimization. It has been used for the classification of the weighted segment. PSO has been used for the classification of the traffic and host features. The second part has been used for the classification of segregated data from these features. It has been classified based on 50% threshold value. Then the aggregated accuracy has been calculated for the final output. *Figure 1* shows the complete process flowchart.

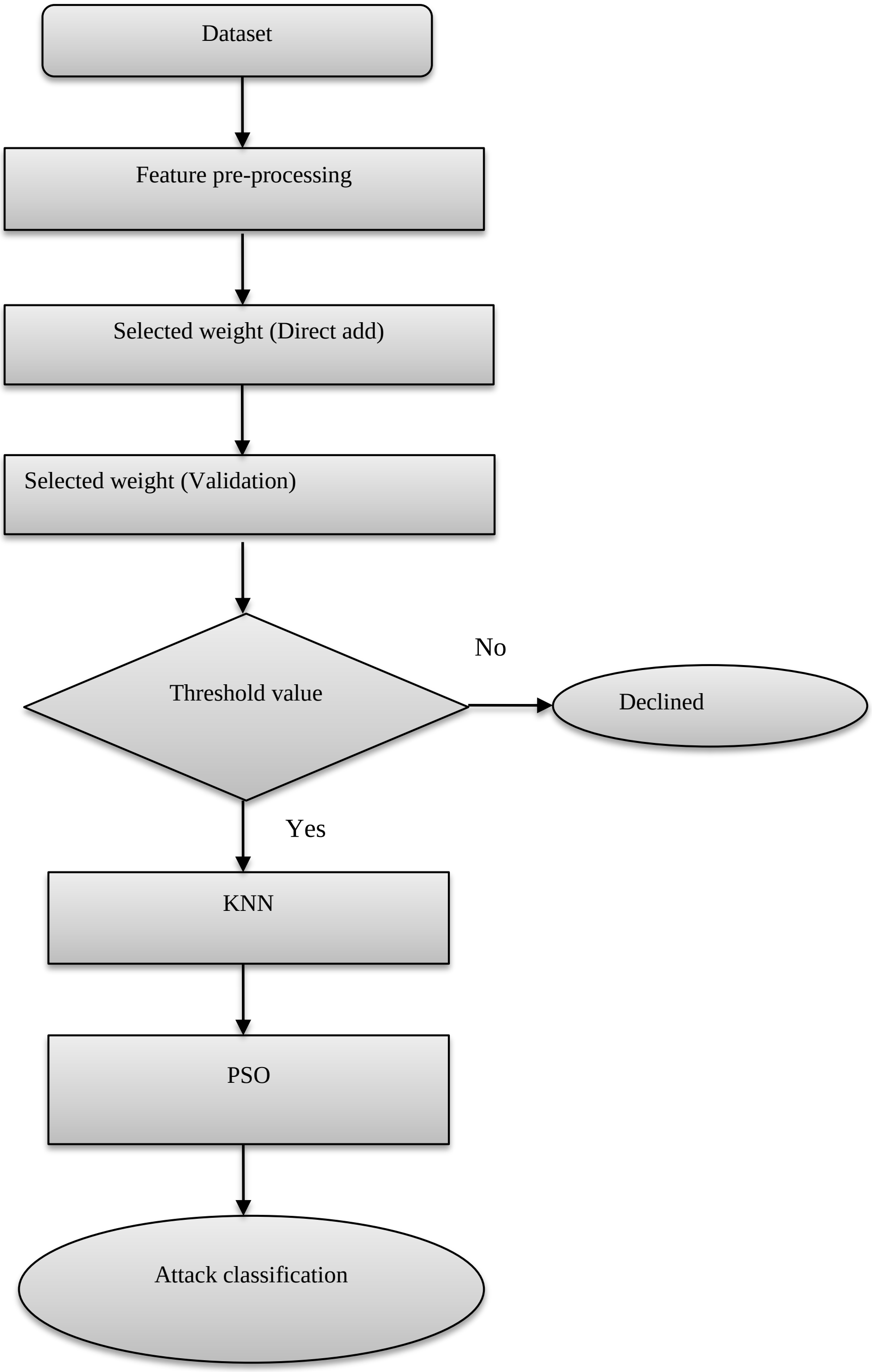

Figure 1 Flowchart of the KNN-PSO approach

4.Results

Figure 2 shows the average classification accuracy with random set 1. *Figure 3* shows the average classification accuracy with random set 2. *Figure 4* shows the average classification accuracy with random set 3. The results clearly indicate that by using our approach the average classification accuracy is approximately 98%. The attack considered here are Denial of Service (DoS), User to Root (U2R), Remote to User /Login (R2L) and Probe.

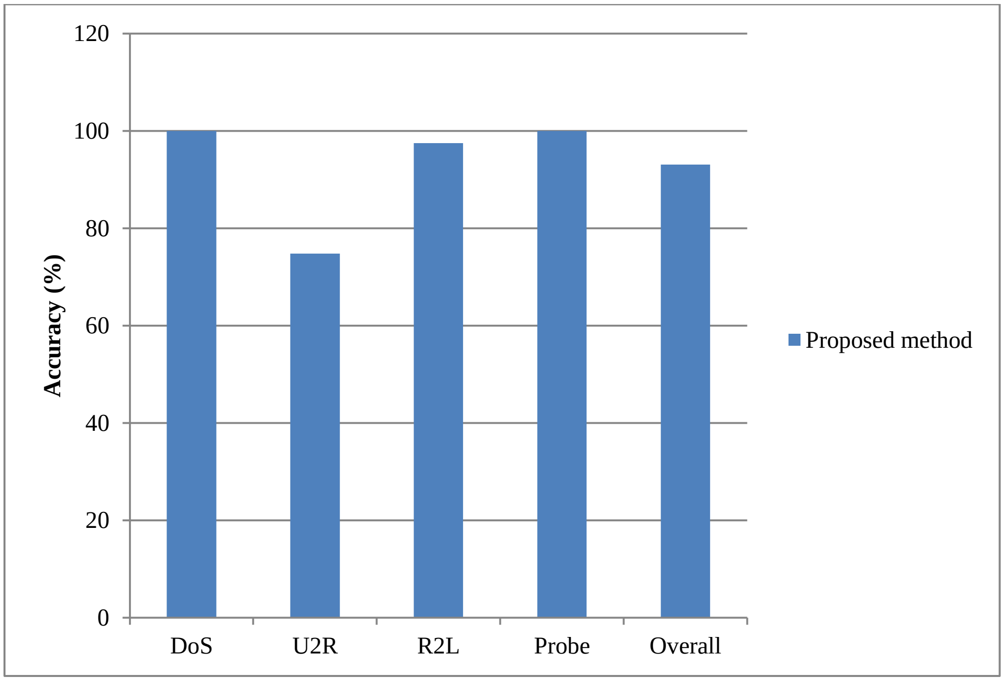

Figure 2 Average classification accuracy with random set 1

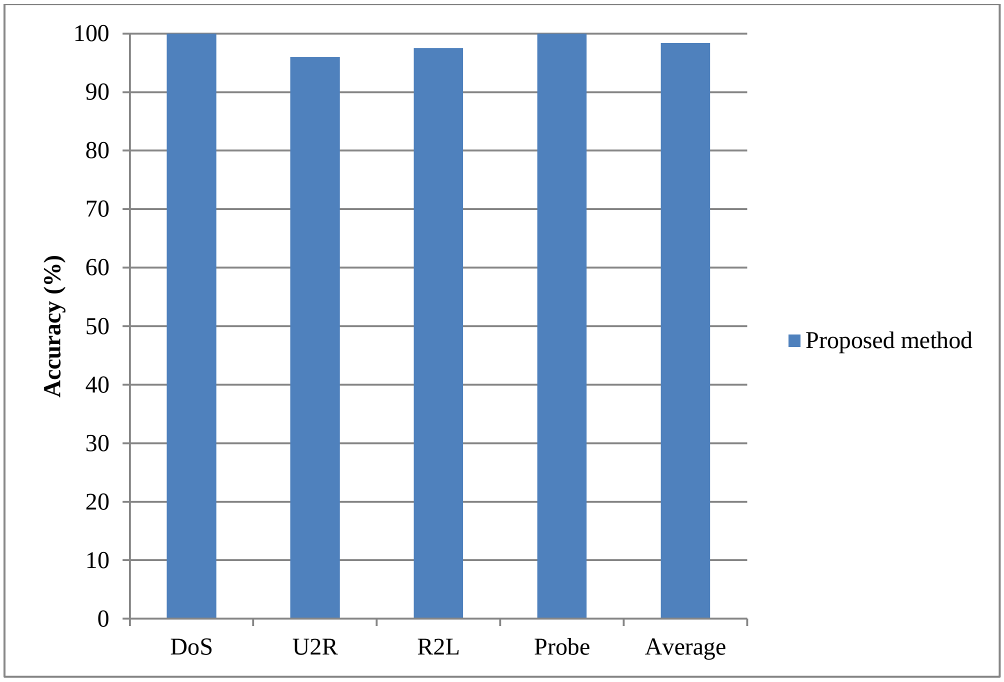

Figure 3 Average classification accuracy with random set 2

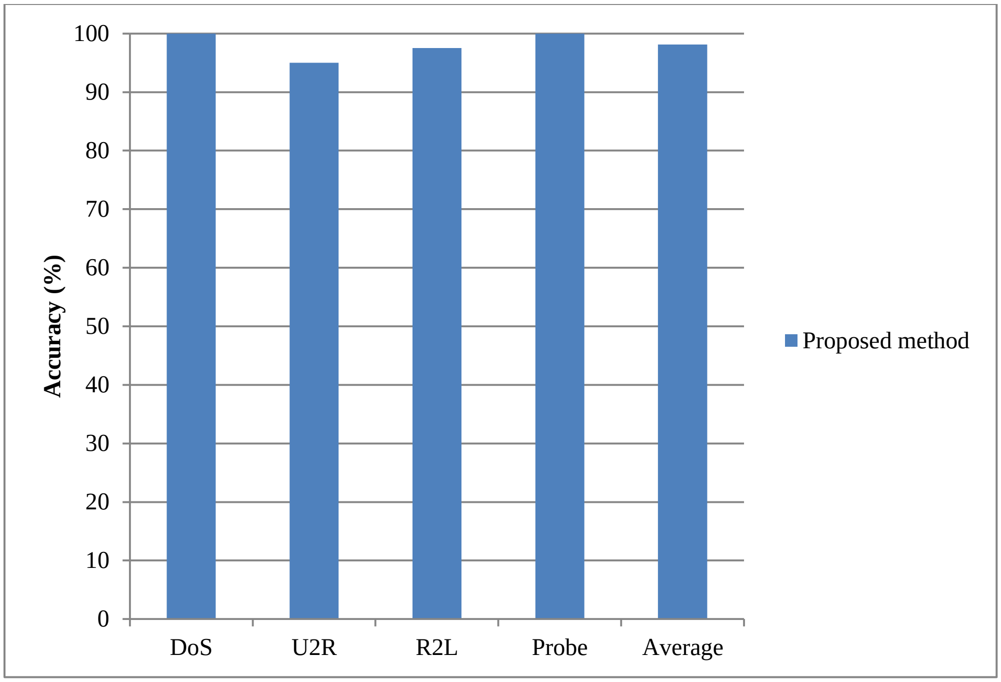

Figure 4 Average classification accuracy with random set 3

5.Conclusion

In this paper an efficient intrusion detection system has been presented and discussed with the comparison with different random set. KNN based PSO algorithm has been applied for the classification. First feature based preprocessing has been performed. Then an input set has been created based on the nodes which are not received safe. These nodes are preprocessed with KNN and PSO. The attack considered here are DoS, U2R, R2L and Probe. The average accuracy obtained is 98%.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] McLaughlin S, Konstantinou C, Wang X, Davi L, Sadeghi AR, Maniatakos M, Karri R. The cybersecurity landscape in industrial control systems. Proceedings of the IEEE. 2016; 104(5):1039-57.

[2] Ani UP, He H, Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology. 2017; 1(1):32-74.

[3] Gupta R, Singh S. A review on intrusion detection system based on data mining and evolutionary algorithms. International Journal of Advanced Technology and Engineering Exploration. 2018; 5(46):356-61.

[4] Kim S, Kim B, Kim HJ. Intrusion Detection and Mitigation System Using Blockchain Analysis for Bitcoin Exchange. In proceedings of the 2018 international conference on cloud computing and internet of things 2018 (pp. 40-4).

[5] Ren W, Yardley T, Nahrstedt K. EDMAND: edge-based multi-level anomaly detection for SCADA Networks. In international conference on communications, control, and computing technologies for smart grids (SmartGridComm) 2018 (pp. 1-7). IEEE.

[6] Kumar KN, Sukumaran S. A survey on network intrusion detection system techniques. International Journal of Advanced Technology and Engineering Exploration. 2018; 5(47):385-93.

[7] Yang J, Shen C, Chi Y, Xu P, Sun W. An extensible Hadoop framework for monitoring performance metrics and events of OpenStack cloud. In 3rd international conference on big data analysis (ICBDA) 2018 (pp. 222-6). IEEE.

[8] Foroushani ZA, Li Y. Intrusion detection system by using hybrid algorithm of data mining technique. In proceedings of the 2018 7th international conference on software and computer applications 2018 (pp. 119-23).

[9] Farhaoui Y. How to secure web servers by the intrusion prevention system (IPS)?. International Journal of Advanced Computer Research. 2016; 6(23):65.

[10] Sicard F, Zamaï É, Flaus JM. An approach based on behavioral models and critical states distance notion

for improving cybersecurity of industrial control systems. Reliability Engineering & System Safety. 2019; 188:584-603.

[11] Anwer HM, Farouk M, Abdel-Hamid A. A framework for efficient network anomaly intrusion detection with features selection. In international conference on information and communication systems (ICICS) 2018 (pp. 157-62). IEEE.

[12] Alexopoulos N, Vasilomanolakis E, Ivánkó NR, Mühlhäuser M. Towards blockchain-based collaborative intrusion detection systems. In international conference on critical information infrastructures security 2017 (pp. 107-18). Springer, Cham.

[13] Kaushik M, Ojha G. Attack penetration system for SQL injection. International journal of advanced computer research. 2014; 4(2):724.

[14] Lopez-Martin M, Carro B, Sanchez-Esguevillas A. Application of deep reinforcement learning to intrusion detection for supervised problems. Expert Systems with Applications. 2020; 141:112963.

[15] Razimi UN, Alkawaz MH, Segar SD. Indoor intrusion detection and filtering system using raspberry Pi. In IEEE international colloquium on signal processing & its applications (CSPA) 2020 (pp. 18-22). IEEE.

[16] Zoppi T, Ceccarelli A, Bondavalli A. Into the unknown: unsupervised machine learning algorithms for anomaly-based intrusion detection. In annual IEEE-IFIP international conference on dependable systems and networks-supplemental volume (DSN-S) 2020 (pp. 81-81). IEEE.

[17] Dang QV. Active learning for intrusion detection systems. In Research, Innovation and Vision for the Future 2020.

[18] Chen W, Cao H, Lv X, Cao Y. A hybrid feature extraction network for intrusion detection based on global attention mechanism. In international conference on computer information and big data applications (CIBDA) 2020 (pp. 481-5). IEEE.

[19] Jin D, Lu Y, Qin J, Cheng Z, Mao Z. KC-IDS: Multi-layer intrusion detection system. In international conference on high performance big data and intelligent systems (HPBD&IS) 2020 (pp. 1-5). IEEE.

[20] Halimaa A, Sundarakantham K. Machine learning based intrusion detection system. In international conference on trends in electronics and informatics (ICOEI) 2019 (pp. 916-20). IEEE.

[21] Taghavinejad SM, Taghavinejad M, Shahmiri L, Zavvar M, Zavvar MH. Intrusion detection in IoT-based smart grid using hybrid decision tree. In international conference on web research (ICWR) 2020 (pp. 152-6). IEEE.

[22] Mu Z, Liu H, Liu C. Design and implementation of network intrusion detection system. In international conference on intelligent transportation, big data & smart city (ICITBS) 2020 (pp. 494-7). IEEE.

[23] Dawit NA, Mathew SS, Hayawi K. Suitability of blockchain for collaborative intrusion detection systems. In annual undergraduate research conference on applied computing (URC) 2020 (pp. 1-6). IEEE.

[24] Park SH, Park HJ, Choi YJ. RNN-based prediction for network intrusion detection. In international conference on artificial intelligence in information and communication (ICAIIC) 2020 (pp. 572-4). IEEE.

[25] Iman AN, Ahmad T. Improving intrusion detection system by estimating parameters of random forest in boruta. In international conference on smart technology and applications (ICoSTA) 2020 (pp. 1-6). IEEE.