Machine Learning Applications in
Engineering Education and Management

ISSN: ***Applied***

Volume ***01*** *Issue* ***02 Year 2021*** *Page* ***01:06***

Layered Intrusion Detection System Model for The Attack Detection with The Multi-Class Ensemble Classifier

Dr. Vivek Deshpande
Associate Professor, Department of Computer Engineering
Vishwakarma Institute of Information Technology Pune India
vivek.deshpande@viit.ac.in

Article History	***Abstract***
Received: 13 July 2021 Revised: 30 September 2021 Accepted: 11 November 2021	This paper presented a layered Intrusion Detection System (IDS) for attack detection in the network. The developed model comprises of the Multi-Class Hybrid Ensemble Learning in the IDS system termed the MCEL-IDS. The proposed MCEL-IDS perform ensemble learning for attack detection in the network. The MCEL-IDS system comprises multi-class features for the consideration of the attributes in the network. The experimental analysis expressed that the MCEL-IDS model achieves a higher False Positive Rate compared with the existing classifier. The MCEL-IDS achieves a higher FPR value of 0.86 which is ~12% performance improvement than the existing classifier. ***Keywords:*** ***Intrusion Detection System (IDS), Attack, Classification, False Positive Rate, Multi-Class, Ensemble classifier***

1. Introduction

Regardless of the extraordinary ability of abnormality location frameworks in identifying zero-day assaults, they endure with high misleading problem rate. To defeat this test and maintain the benefits of abuse identification, specialists have proposed a half breed interruption discovery framework. As indicated by the combination approach, current mixture IDSs can have equal or layered engineering [1]. In this approach a ultimate conclusion is made by combining the consequences of the singular frameworks. In [2] proposed a mixture IDS framework that joins an abuse recognition module and an irregularity location module in equal. The inconsistency discovery part of the half and half framework models ordinary conduct utilizing Self-Sorting out Guide (SOM). The abnormality recognition module thinks about any deviation from the ordinary way of behaving as assault. In the abuse identification module, the creators utilized J.48 choice tree calculation to order different kinds of recently known assaults. A choice emotionally supportive network was proposed for consolidating the recognition consequences of the two frameworks. The cross-breed framework was assessed with the KDD'99 benchmark interruption identification informational collection, and it is expressed that the proposed mixture approach beats independent individual methodologies.

Another mixture network interruption identification structure that consolidates abuse discovery and irregularity location frameworks in equal is proposed in [3]. In this approach Grunt and QRadar [4] are utilized as a mark-based finder and C4.5 choice tree is utilized as irregularity locator. Tavallaee utilized Dempster's standard of mix [5] alongside a bunching-based quantitation technique to foster a melding calculation that consolidates the outcomes from signature-based and irregularity-based identifiers. In [6] proposed a progressive half and half wise IDS approach (DT-SVM) that joins choice trees (DT) and support vector machines (SVM). In this approach the assessment informational collection is first gone through the choice tree and hub data is created. The terminal hub data produced by the choice tree alongside the first arrangement of highlights of the informational collection is then gone through the SVM for an ultimate conclusion of the progressive mixture IDS framework. However, the assessment made on the KDD'99 IDS informational index uncovered that the hub data worked on the exhibition of SVM, the half breed DT-SVM model did not give the normal presentation. The creators further consolidate choice tree, SVM and the mixture DT-SVM in lined up as free frameworks of group classifier. Contrasted with DT-SVM model, the gathering approach gives more exact interruption recognition frameworks (particularly for Test and R2L classes).

In [7] constructed a main level of this framework comprises of choice tree that isolates known assaults from typical cases. The subsequent level contains Grouping Based Affiliation irregularity recognition framework that gets thought deals (both ordinary and obscure assaults) and choice tree-based abuse indicator that gets known assaults from the primary level. The subsequent level abuse finder arranges known assaults into different assault subclasses. In [8] proposed a cross breed interruption location structure that joins abuse and oddity recognition frameworks. Irregular backwoods classifier is utilized to execute continuous abuse identifier. Associations which are named unsure by the abuse locator are taken care of to the disconnected peculiarity indicator. The inconsistency identifier additionally involved irregular backwoods classifier for exception recognition. Zhang et al. shown that arbitrary backwoods-based crossover IDS can accomplish high recognition rate with low misleading positive rate, and can identify already inconspicuous interruptions.

In [9] presented progressive crossover interruption identification technique that coordinates abuse location and a peculiarity discovery model. C4.5 choice tree and one-class support vector machine were utilized to execute the abuse discovery and abnormality location models separately. The abuse recognition module disintegrates the typical preparation information into more modest subsets. Then, at that point, for every one of these disintegrated subsets abnormality recognition model is created utilizing one-class SVM [10].

The framework is assessed utilizing NSL-KDD interruption identification informational collection. It is expressed that the half and half model has worked on the IDS concerning location execution for already concealed assaults and identification inertness. However, numerous interruption location structures and frameworks have been created by the exploration local area, IDS execution and zero-day assault identification are yet open examination issues and difficulties [11]. Subsequently, for tending to these difficulties in this part a layered half and half interruption recognition structure is proposed MCEL-IDS. As the proposed cross breed framework joins abuse and irregularity identifiers in consecutive way it will accomplish the upside of abuse location to have a high discovery rate on referred to assaults as well as the capacity of oddity finders in identifying obscure assaults. The created MCEL-IDS model shows the higher FPR 0.86 with the powerful exhibition.

2. Multi-Class Hybrid Ensemble Classifier for the Intrusion Detection System

In a layered hybrid system, each layer provides some new information to the higher level. Moreover, the layered approach is chosen instead of the parallel approach to reduce the overhead on the anomaly detector for detecting previously known attacks. In the layered approach if previously known attacks are detected by the misuse detector they will be blocked and will not be forwarded to the anomaly detector. The proposed hybrid IDS framework as shown in Figure 1 consists of four major components: Feature selection module, Misuse detector module, Data normalization module and Anomaly detector module.

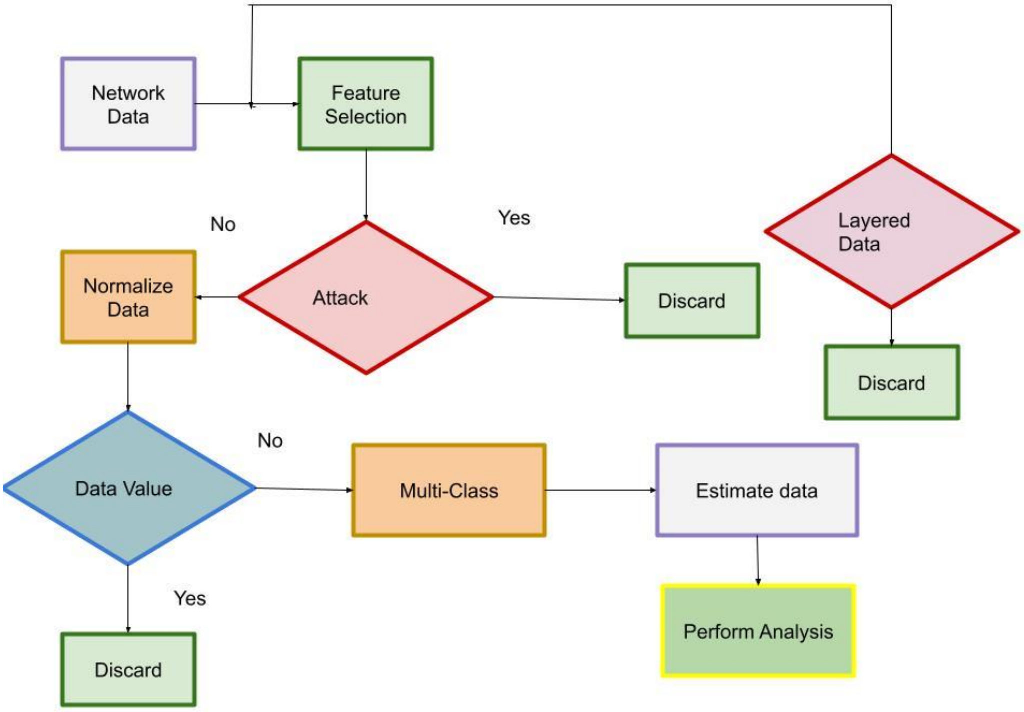


Figure 1: Flow Chart of MCEL-IDS

Because the intrusion detection dataset has a very large size, a normalization method should have simple rules and fast speed. Hence due to its simple rules and speed, the Min-Max-based linear data normalization technique is employed in the proposed hybrid IDS. The Min-Max based normalization can be done using the equation (1)

$$X = \frac{X-min}{\max - min} \tag{1}$$

In the above equation (1) the normalized attribute values are stated as the X and X' with the presence of the value minA and maxA for the attribute value maximum and minimum. Through the Multi-Class Ensemble Layered IDS (MCEL-IDS). The normalized function uses the kernel function for the estimation of the linear, Gaussian, Sigmoidal and Polynomial features. With the proposed MCEL-IDS scheme the anomaly detection is performed with the Gaussian radial basis function (RBF) for the computation of the features as presented in equation (2)

$$K(z,x) = e^{-\gamma} \tag{2}$$

The proposed MCEL-IDS comprises of the Gaussian radial basis function denoted in γ. The small value of γ comprises of the non-linear power and the decision boundary computation of the features. In case if the value of the γ is higher than the training data sensitivity is higher.

3. Experimental Analysis and Results

The proposed system is used to detect non-targeted attacks on SCADA network. As NSL-KDD intrusion detection dataset is collected on conventional IT infrastructure, it can used to represent non-targeted attacks on SCADA system. With NSL-KDD model the dataset comprises of the features in the data. As the NSL-KDD dataset comprises of the KDD99 dataset for the different data set. The dataset comprises of the 33 features with the defined set of the labels for the test data of 7679 and the 8457 for the features for the classification of the normal and attack classes presented in table 1.

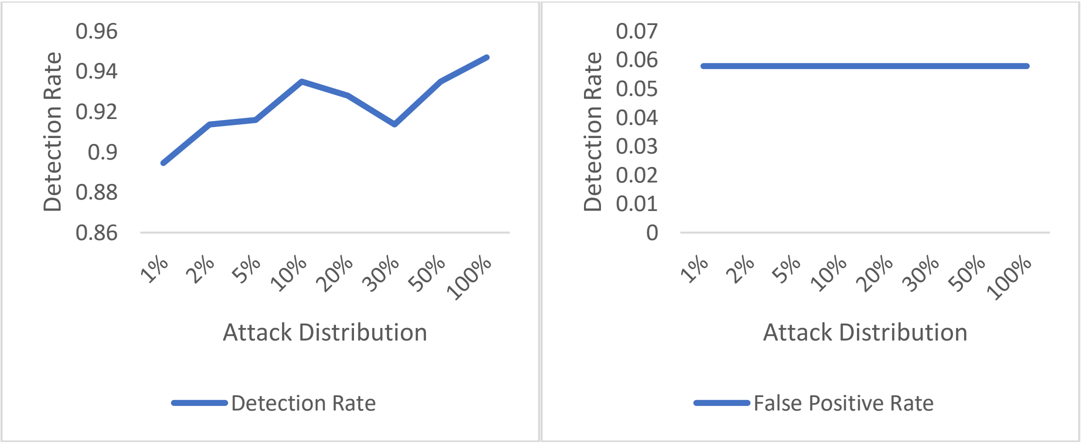
Table 1: Labelled Data

7833	0, udp, private data, SF, 103,103,1,1,1,1,0,0,0,0,1,1,0,0,0,0,0,0,1,2,2,0,0,0,2,1,1,237,237,2,0,1,1,0,0,1,0, normal
8467	0, udp, private, SF, 101,101,1,1,1,1,0,0,0,0,1,1,0,0,0,1,0,0,1,2,2,0,0,2,1,0,0,239,228,1,0,0,0,1,1,0,0, snmpgetattack
11695	0,udp,private,SF, 103,102,0,1,1,1,1,0,0,0,0,0,0,0,2,2,0,1,0,1,2,0,2,217,228,1,0,1,1,0,0,1,1,0,normal
1347	0,udp,private,SF, 103,101,1,1,1,1,2,2,21,1,10,0,0,0,0,0,0,3,3,0,0,0,0,1,0,0,255,255,1,0,0.01,1,1,0,0,0,snmpget attack

The developed MCEL-IDS model comprises the features comprised of the outbounds with zero value for the data training and testing. The features involved in the identification of the attacks in the network through consideration of the features. The proposed MCEL-IDS mode comprises of the NSL-KDD dataset for the processing the dataset for the attack classification. The dataset attributes considered for the analysis are presented in the table 2.

Table 2: Attributes values

Data	Normal	Attack
Training	66,456	58,478
Test	9,345	12,389



(a) (b)

Figure 2: (a) Detection Rate (b) False Positive Rate

Through the proposed MCEL-IDS model the features are evaluated for the computation of the multi-class ensemble features. The figure 2 provides the illustration of the detection rate and false positive rate for the different percentage of the attacks. In table 4 the comparative analysis of the proposed MCEL-IDS with the other classifier mode is presented.

With the proposed MCEL-IDS the multi-class features are estimated for the consideration of different attacks in the distribution of the attacks. In the table 3 the estimation of the detection rate and false positive rate are computed for the different attacks in the network. The multi-class ensemble classifier features are evaluated based on the consideration of the table 3.

Table 3: Estimation of the Features

Attack %	Detection Rate	False Positive Rate
1%	0.8945	0.0578
2%	0.9136	0.0578
5%	0.9157	0.0578
10%	0.9348	0.0578
20%	0.9278	0.0578
30%	0.9137	0.0578
50%	0.9349	0.0578
100%	0.9469	0.0578

Table 4: Comparative Analysis

Model	False Positive Rate (FPR)
Naive Bayes	0.034
J48	0.019
Rf	0.028
SVM	0.059
MCEL-IDS	0.086

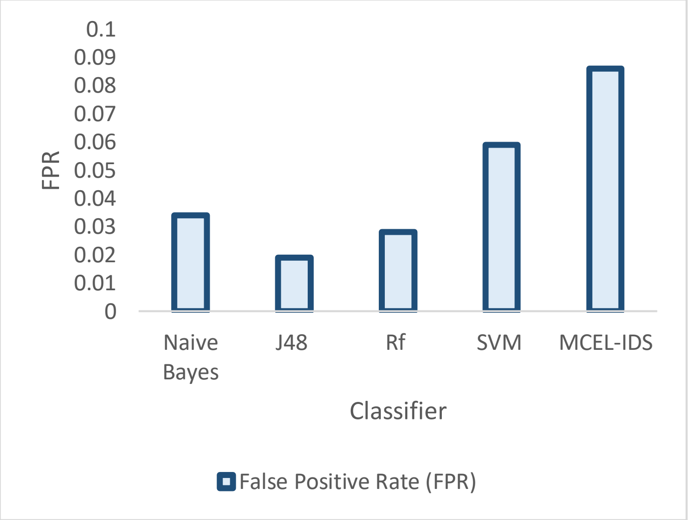


Figure 3: Comparison of FPR

In figure 3 the estimated FPR for the different classifier models with the proposed MCEL-IDS model is presented. The comparative analysis expressed that the proposed model achieves the FPR value of 0.086 which is significantly higher than the existing classifier model.

4. Conclusion

This paper developed an MCEL-IDS for attack detection in the network dataset in the IDS system. The developed MCEL-IDS comprises of the multi-class ensemble classifier for the classification of the attack in IDS. The evaluation of the dataset is based on the consideration of the estimated features for attack detection in the IDS system. The experimental evaluation of the proposed MCEL-IDS expressed that MCEL-IDS achieves a higher FPR compared with the existing classifier model. The MCEL-IDS model achieves the FPR value of 0.86 and the detection rate is 0.94.

References

[1] Marathe, N., & Shinde, S. K. (2019). ITCA, an IDS and trust solution collaborated with ACK based approach to mitigate network layer attack on MANET routing. *Wireless Personal Communications*, *107*(1), 393-416.

[2] Kaushik, I., Sharma, N., & Singh, N. (2019, March). Intrusion detection and security system for blackhole attack. In *2019 2nd International Conference on Signal Processing and Communication (ICSPC)* (pp. 320-324). IEEE.

[3] Kumari, R., & Sharma, K. (2018). Cross-layer based intrusion detection and prevention for network. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 38-56). IGI Global.

[4] Nyasore, O. N., Zavarsky, P., Swar, B., Naiyeju, R., & Dabra, S. (2020, May). Deep packet inspection in industrial automation control system to mitigate attacks exploiting modbus/TCP vulnerabilities. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)* (pp. 241-245). IEEE.

[5] Godala, S., & Vaddella, R. P. V. (2020). A study on intrusion detection system in wireless sensor networks. *International Journal of Communication Networks and Information Security*, *12*(1), 127-141.

[6] Alzahrani, S., & Hong, L. (2018). Generation of DDoS attack dataset for effective IDS development and evaluation. *Journal of Information Security*, *9*(4), 225-241.

[7] Lombardi, M., Pascale, F., & Santaniello, D. (2020, June). EIDS: Embedded Intrusion Detection System using Machine Learning to Detect Attack over the CAN-BUS. In *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, Venice, Italy* (pp. 21-26).

[8] Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., ... & Idris, N. B. (2020). Intrusion detection system for the internet of things based on blockchain and multi-agent systems. *Electronics*, *9*(7), 1120.

[9] Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, *20*(13), 3625.

[10] Mohapatra, H., Rath, S., Panda, S., & Kumar, R. (2020). Handling of man-in-the-middle attack in wsn through intrusion detection system. *International journal*, *8*(5), 1503-1510.

[11] Kao, Y. C., Liu, J. C., Wang, Y. H., Chu, Y. H., Tsai, S. C., & Lin, Y. B. (2019). Automatic Blocking Mechanism for Information Security with SDN. *J. Internet Serv. Inf. Secur.*, *9*(1), 60-73.

[12] Kore, A., & Patil, S. (2020). IC-MADS: IoT enabled cross layer man-in-middle attack detection system for smart healthcare application. *Wireless Personal Communications*, *113*(2), 727-746.