*International Journal of Master of Engineering Research and Technology, 2394-6172-(O)*
*Volume-6, Issue-9, September 2019*

# A Review of Intrusion Detection Techniques Based on Feature Selection and Feature Optimization using Swarm Intelligence

**SAGAR PANCHTILAK**
sagarpanchtilak89@gmail.com

**Prof. BHAWANA PILLAI**
bhawnap@lnct.ac.in

**Abstract**

Feature selection and optimization of features is important area of research in intrusion detection system. The optimization and selection of features enhanced the process of detection of unknow types of attack in intrusion detection. Now a day's various features optimization and selection algorithms used such as filter based, wrapper based, and hybrid based. In series of feature selection and optimization filter-based selection technique did not require any optimization algorithms, its directly select the features without optimization. The swarm intelligence play an important role in selection of features and optimization of features. In this paper present the review of features selection and feature optimization based on swarm intelligence. The swarm intelligence offers various algorithms such as ant colony optimization, particle swarm optimization, glow warm optimization, ABC and many more bio-inspired algorithms for the processing of features optimization.

**Keywords: -** intrusion detection, feature selection, optimization, swarm intelligence, data mining, KDD CUP99.

## Introduction

The intrusion detection system came highlight in 1991 by Anderson. After that the process of intrusion detection carry long journey for the prevention and detection of cyber-attack. Due to variation of time and data capacity the nature of cyber- attack is also change and generates dynamic features-based attacks over the network [1, 2]. The conventional methods of intrusion detection cannot capable for the detection of intrusion detection. The complex features of intrusion data handling are big issue for detection of intrusion. The complex features decrease the detection rate and increase the complexity of cost. In current decade the researcher focuses on the feature's optimization and feature selection. The process of features optimization and features selection speedup the process of detection and prevention of intrusion detection. The process of features detection classified into three basic section one is filter based feature selection, wrapper-based feature selection and finally hybrid-based features selection. The filter-based features selection methods cannot require any optimization algorithms for the process of optimization and selection of irrelevant features [3-5]. The hybrid and wrapper methods of features selection incorporate the swarm and bio-inspired function for the optimization of features [7]. The swarm-based features optimization used various optimization algorithms such as ant colony optimization, particle swarm optimization, ABC algorithm and many more agent-based algorithms inspired by natural swarm. The swarm-based optimization algorithms maintain the basic content of features and reduces the unwanted features sub-set of intrusion data and increases the speed of detection and classification of intrusion [8, 9]. Data mining also play an important role in detection and classification of intrusion detection. The optimized data proceed for the process of detection used classification and clustering algorithms for the grouping of data. The grouping of data categorized the different categories of attack available in the family of intrusion. The family of intrusion data classified into five major classes, DOS attack, prob attacks, U2R attacks, R2L attacks and normal categories of data. The major content of attack of data is DOS attack. The DOS attacks are major family of cyber-attack. The family of DOS attack consist of static as well as dynamic features attribute for the capturing the data without any legal permission [10]. The detection and prevention of DOS attacks is major challenge. Validation of methods and design algorithms is big challenge due to inability of large network and huge amount of attackers group. For the crises [12]. The MIT institute develop the laboratory experimental data is called KDDCUP99 dataset. The KDDCUP99 dataset consist of 7 lacks instant data, these 7 lacks instant data have 42 features attributes. The rest of paper discuss as in section II related work.



*Paper ID:- 2019/06/IJMERT/09/365*

In section III discuss the Feature Selection process. In comparative algorithms compression of feature selection and finally conclude in section V.

## II. Related Work

The fast and accurate detection of intrusion using features optimization and selection cum in frame of research. The various researchers and authors used conventional and bio-inspired swarm-based optimization and selection techniques of features for the detection of intrusion. Some related work in features optimization discuss here.

| Et al. | Author | Title | Approach | Result | Publication |
|---|---|---|---|---|---|
| [1] | Zhang Y, Chen X, Jin L, Wang X, Guo D | Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data. | They first discussed a new network intrusion detection model named the deep hierarchical network, which integrates the improved LeNet-5 and LSTM neural network structures, while learning the spatial and temporal features of flow. By designing a reasonable network cascading method, they can train our discussed hierarchical network at the same time instead of training two networks separately. | The experimental results show that the performance of the discussed hierarchical network model is significantly better than other network intrusion detection models, which can achieve the best detection accuracy. | IEEE Access. 2019 |
| [2] | Ahmed M, Mahmood AN, Hu J. | A survey of network anomaly detection techniques. | Anomaly detection is an important data analysis task which is useful for identifying the network intrusions. This paper presents an in-depth analysis of four major categories of anomaly detection techniques which include classification, statistical, information theory and clustering. | The survey of literature reported in this paper has categorized the network anomaly detection methods on four major categories. For each category, they described the assumptions for segregating normal data instances from anomalous. This paper provided a discussion on network traffic dataset issues which are of significant concern to the research community in the area of network traffic analysis. | Journal of Network and Computer Applications. 2016 |
| [3] | Kim J, Kim J, Thu HL, Kim H. | Long short-term memory recurrent neural network classifier for intrusion detection. | They construct an IDS model with deep learning approach. They apply Long Short Term Memory (LSTM) architecture to a Recurrent Neural Network (RNN) and train the IDS model using KDD Cup 1999 | They implemented the IDS classifier based on LSTM-RNN and evaluated the IDS model. They have the highest DR and Accuracy even though the FAR is slightly above the other ones. | International Conference on Platform Technology and Service 2016 |

| | | | | | |
|---|---|---|---|---|---|
| | | | dataset. Through the performance test, they confirm that the deep learning approach is effective for IDS. | | |
| [4] | Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y. | N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. | They discussed and empirically evaluate a novel network-based anomaly detection method which extracts behavior snapshots of the network and uses deep autoencoders to detect anomalous network traffic emanating from compromised IoT devices. To evaluate our method, they infected nine commercial IoT devices in our lab with two of the most widely known IoT-based botnets, Mirai and BASHLITE. | They observed that the Philips B120N/10 baby monitor demonstrated the highest FPR relative to the other devices; it also produced the largest amount of traffic, so one could expect that the abundance of training instances would result in more robust machine learning models. | IEEE Pervasive Computing. 2018 |
| [5] | Wang L, Xiong Y, Wang Z, Qiao Y, Lin D, Tang X, Van Gool L. | Temporal segment networks: Towards good practices for deep action recognition. | This paper aims to discover the principles to design effective ConvNet architectures for action recognition in videos and learn these models given limited training samples. Our first contribution is temporal segment network (TSN), a novel framework for video-based action recognition. | They presented the Temporal Segment Network (TSN), a video-level framework that aims to model long-term temporal structure. As demonstrated on two challenging datasets, this work has brought the state of the art to a new level, while maintaining a reasonable computational cost. | European conference on computer vision 2016 |
| [6] | Zarpelao BB, Miani RS, Kawakani CT, de Alvarenga SC. | A survey of intrusion detection in Internet of Things. | They present a survey of IDS research eï¬€orts for IoT. Our objective is to identify leading trends, open issues, and future research possibilities. they classified the IDSs discussed in the literature according to the following attributes: detection method, IDS placement strategy, security threat and validation strategy. | They discussed a taxonomy to classify these papers, which is based on the following attributes: detection method, IDS placement strategy, security threat, and validation strategy. They observed that the research of IDS schemes for IoT is still incipient. The discussed solutions do not cover a wide range of attacks and IoT technologies. | Journal of Network and Computer Applications. 2017 |
| [7] | Diro AA, Chilamkurti N. | Distributed attack detection scheme using deep | This research is aimed at adopting a new approach, deep learning, to cybersecurity to enable the detection of attacks in | The experiments have shown that our distributed attack detection system is superior to centralized | Future Generation Computer Systems. 2018 |

| | | | | | |
|---|---|---|---|---|---|
| | | learning approach for Internet of Things. | social internet of things. The performance of the deep model is compared against traditional machine learning approach, and distributed attack detection is evaluated against the centralized detection system. | detection systems using deep learning model. It has also been demonstrated that the deep model is more effective in attack detection than its shallow counter parts. | |
| [8] | Li G, Dong M, Ota K, Wu J, Li J, Ye T. | Deep packet inspection-based application-aware traffic control for software defined networks. | They discussed an application-aware traffic control scheme, in which both network states and traffic behaviors are exploited cooperatively. Deep Packet Inspection (DPI) is introduced into SDN controller. Meanwhile, a mechanism for packet classification and behavior matching is designed. | They adopt some mathematical models to quantitatively evaluate the performances of discussed architecture by comparing the throughput of network one node, latency time of the end-to-end communication. Simulation results shows that the discussed architecture can reduce latency time and fine-grained traffic control improves network load capability. | IEEE Global Communications Conference (GLOBECOM) 2016 |
| [9] | Liu W, Wang Z, Liu X, Zeng N, Liu Y, Alsaadi FE. | A survey of deep neural network architectures and their applications. | They discuss some widely used deep learning architectures and their practical applications. An up-to-date overview is provided on four deep learning architectures, namely, autoencoder, convolutional neural network, deep belief network, and restricted Boltzmann machine. | They have reviewed the latest developments of deep neural networks. Some widely used deep learning architectures are investigated and selected applications to computer vision, pattern recognition and speech recognition are highlighted. | Neurocomputing. 2017 |
| [10] | Bhuyan MH, Bhattacharyya DK, Kalita JK. | A multi-step outlier-based anomaly detection approach to network-wide traffic. | They present a multi-step outlier-based approach for detection of anomalies in network-wide traffic. They identify a subset of relevant traffic features and use it during clustering and anomaly detection. | They have presented a fast-distributed framework for extracting and preparing feature data from raw network-wide traffic. The clustering algorithm arranges the data in a depth-first manner before applying our network anomaly detection algorithm. The main attraction of our approach is its ability to successfully detect all outlier cases they have come up | Information Sciences. 2016 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | with. It can also use any proximity measure for score computation. | |
| [11] | Chen PY, Zhang H, Sharma Y, Yi J, Hsieh CJ. | Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models. | They discussed an effective black-box attack that also only has access to the input (images) and the output (confidence scores) of a targeted DNN. | This paper discussed a new type of black-box attacks named ZOO to DNNs without training any substitute model as an attack surrogate. By exploiting zeroth order optimization for deploying pseudo back propagation on a targeted black-box DNN, experimental results show that our attack attains comparable performance to the state-of-the-art white-box attack. | ACM Workshop on Artificial Intelligence and Security 2017 |
| [12] | Papernot N, McDaniel P, Wu X, Jha S, Swami A. | Distillation as a defense to adversarial perturbations against deep neural networks. | They introduce a defensive mechanism called defensive distillation to reduce the effectiveness of adversarial samples on DNNs. They analytically investigate the generalizability and robustness properties granted by the use of defensive distillation when training DNNs. | It reduces the success of adversarial sample crafting to rates smaller than 0.5% on the MNIST dataset and smaller than 5% on the CIFAR10 dataset while maintaining the accuracy rates of the original DNNs. | IEEE Symposium on Security and Privacy (SP) 2016 |
| [13] | Wang C, Zhao Z, Gong L, Zhu L, Liu Z, Cheng X. | A distributed anomaly detection system for in-vehicle network using HTM. | They improved the abnormal score mechanism to evaluate the prediction. They manually synthesized field modification and replay attack in data field. | Moving the redundant fields in the data domain. In addition, they must integrate ID with data dependencies and improve the combination evaluation of multiple ID to achieve better overall detection performance, because the ID of each monitor increases the possibility of false alarm. This is to avoid the greater impact of a single special ID judgment on the whole system. | IEEE Access 2016 |
| [14] | Yu Y, Long J, Cai Z. | Network intrusion detection through stacking | Intentions automatically and efficiently from large amounts of unlabeled raw network traffic data by using deep learning | they compared our deep learning method with other similar approaches. The effects of various important | Security and Communication Networks. 2017 |

| | | | | | |
|---|---|---|---|---|---|
| | | dilated convolutional autoencoders. | approaches. They discussed a novel network intrusion model by stacking dilated convolutional autoencoders and evaluate our method on two new intrusion detection datasets. Several experiments they're carried out to check the effectiveness of our approach. The comparative experimental results demonstrate that the discussed model can achieve considerably high performance which meets the demand of high accuracy and adaptability of network intrusion detection systems (NIDSs). | hyperparameters are further analyzed. The experimental results show the superiority of our model by effectively detecting com-plex attacks from lots of unlabeled data. | |
| [15] | Yuan Z, Lu Y, Xue Y. | Droiddetector: android malware characterization and detection using deep learning. | They discussed to associate the features from the static analysis with features from dynamic analysis of Android apps and characterize malware using deep learning techniques. They implement an online deep-learning-based Android malware detection engine (DroidDetector) that can automatically detect whether an app is a malware or not. | The results show that deep learning is suitable for characterizing Android malware and especially effective with the availability of more training data. DroidDetector can achieve 96.76% detection accuracy, which outperforms traditional machine learning techniques. | Tsinghua Science and Technology. 2016 |

**III. Feature Selection (FS)**

The process of machine learning says that the greater number of features enhanced the performance of system and data. But some cases it's not true, because the size of data and large number of features decreases the process of classification and detection[5, 7]. In case of intrusion detection, the reduction of features play an important role for the detection algorithms. In the process of features selection, the intrusion detection techniques used three methods. Filter based methods, wrapper-based methods and hybrid methods. The filter-based methods directly decide the successive nature of features for the process of classification and detection. The successive nature of features is very effective but not scale the process of intrusion detection[13, 14]. The drawback of filter-based approach is that cannot the justify the performance of selected features for the process of detection and classification. The wrapper models used the concept of variable integration with the swarm intelligence and improve the performance of classification algorithms of data mining and neural network. The process of feature optimization and selection used swarm-based optimization techniques here discuss some swarm-based algorithms[15].

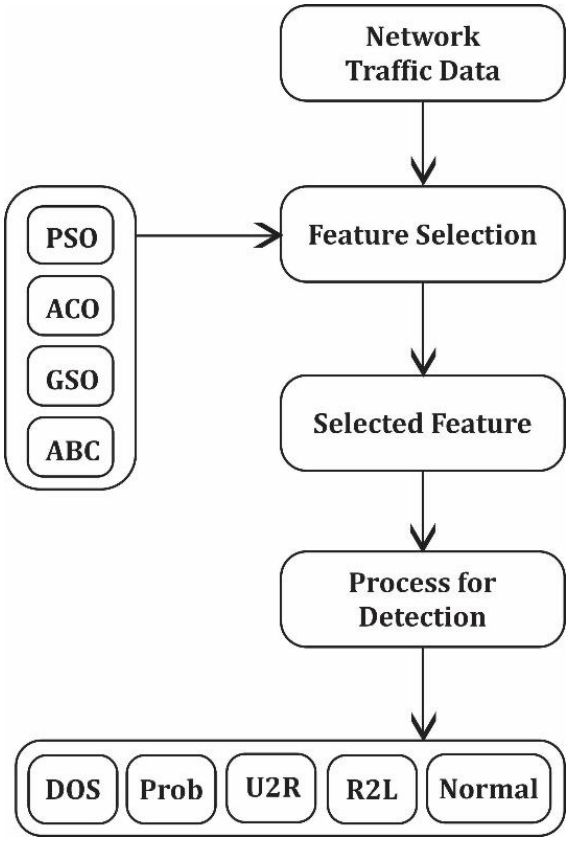


Figure 1: Block diagram of feature selection and optimization based on swarm intelligence.

Particle swarm optimization (PSO): - particle swarm optimization is memory based iterative algorithm. These algorithms work on the principle of fly birds in sky. The principle of birds gives the concept of function of acceleration and constant velocity. The acceleration and constant velocity define the two function in PSO is called Gbest and Pbest. The value of Pbest is local optimal value of set and the value of Gbest gives the optimal value of complete process of data.

Ant colony optimization (ACO): - ant colony optimization inspired by the biological ants and design the artificial ant colony optimization algorithms. By the virtue of nature, the biological ants always find the smallest distance between source to food location. The smallest paths trace by the ants, here used as the principle of features dissimilarity. The dissimilar feature is selected, and similar features are rejected for the processing of data. The ant colony process of algorithms depends on the value of pheromone. The value of pheromone maintains the path of data. In artificial ants the value of pheromone measures the constant value of given features set.

Glow swarm optimization (GSO): - The glow swarm optimization algorithms is new bio-inspired algorithms based on the working behaviors of glowworm. The glowworm work on the principle of lubrification. The process of lubrification generates a smell and collect all glowworm in single point of location and in light that location. The principle of that used here for the collection of similar features.

ABC (BEE algorithms): - in the process of features optimization in any discipline the BEE algorithm gives better result in process of sought location of Bee. The function process of Bee indirect process of features optimization. Bee perform the collective movement without any collision.

## IV. Comparative Performance of Features Optimization & Classification

| S. No. | Dataset | Method | Classifier | Feature Length | Measure | | | | | Ref. |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | AC | DR | FAR | FPR | TPR | |
| 1. | KDD CUP'99 | Bees Algorithm | SVM | 15 | 94.62 | - | 0.07 | - | 97.01 | [2] |
| 2. | KDD CUP'99 | ABC Optimization | SVM | 40 | 96.57 | | 0.0013 | - | 93.65 | [3] |
| 3. | KDD CUP'99 | PSO | Decision tree | | - | - | - | 2.61 | - | [5] |
| 4. | KDD CUP'99 | Cattle fish algorithm | Feed-forward neural network classifier | 12 | - | | - | 1.87 | 98.64 | [6] |
| 5. | KDD CUP'99 | Bat algorithm | SVM | 8 | 97.22 | - | - | 1.21 | - | [7] |
| 6. | KDD CUP'99 | PSO+SVM | SSO with weighted local search | 38 | - | - | 1.02 | 0.98 | - | [8] |
| 7. | KDD CUP'99 | Swarm based rough set | Decision tree | - | 92.97 | 96.23 | 0.07 | - | 87.24 | [9] |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8. | KDD CUP'99 | Bat algorithm | Decision tree | 12 | - | 99.46 | - | - | 86.31 | [11] |
| 9. | KDD CUP'99 | Bees Algorithm | SVM | 26 | - | 93.07 | - | 0.961 | 96.95 | [12] |
| 10 | KDD CUP'99 | PSO | SVM | - | - | - | 1.29 | 2.87 | 96.90 | [13] |
| 11. | KDD CUP'99 | ACO | Feed-forward neural network classifier | - | 89.14 | - | 1.611 | - | - | [14] |
| 12. | KDD CUP'99 | ACO + Feature weighting SVM | SVM | 12 | 88.50 | - | - | - | - | [15] |

## V. Conclusion & Future Work

The detection and prevention of intrusion is great challenge in diverse of network and growth of data. For the detection and prevention used various data mining, machine learning and swarm optimization-based algorithms are used. The conventional intrusion detection algorithms cannot the used of feature selection and feature optimization. In this paper present the review of features optimization and features selection of network traffic data for the detection of intrusion. In the process of survey finds that the performance of feature optimization and detection based on optimization and classification algorithms. In future used the hybrid swarm algorithms for the selection of features.

## References

[1] Zhang Y, Chen X, Jin L, Wang X, Guo D. Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data. IEEE Access. 2019 Mar 20;7:37004-16.

[2] Ahmed M, Mahmood AN, Hu J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016 Jan 1;60:19-31.

[3] Kim J, Kim J, Thu HL, Kim H. Long short-term memory recurrent neural network classifier for intrusion detection. In2016 International Conference on Platform Technology and Service (PlatCon) 2016 Feb 15 (pp. 1-5). IEEE.

[4] Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Computing. 2018 Jul;17(3):12-22.

[5] Wang L, Xiong Y, Wang Z, Qiao Y, Lin D, Tang X, Van Gool L. Temporal segment networks: Towards good practices for deep action recognition. InEuropean conference on computer vision 2016 Oct 8 (pp. 20-36). Springer, Cham.

[6] Zarpelao BB, Miani RS, Kawakani CT, de Alvarenga SC. A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications. 2017 Apr 15;84:25-37.

[7] Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems. 2018 May 1;82:761-8.

[8] Li G, Dong M, Ota K, Wu J, Li J, Ye T. Deep packet inspection-based application-aware traffic control for software defined networks. In2016 IEEE Global Communications Conference (GLOBECOM) 2016 Dec 4 (pp. 1-6). IEEE.

[9] Liu W, Wang Z, Liu X, Zeng N, Liu Y, Alsaadi FE. A survey of deep neural network architectures and their applications. Neurocomputing. 2017 Apr 19;234:11-26.

[10] Bhuyan MH, Bhattacharyya DK, Kalita JK. A multi-step outlier-based anomaly detection approach to network-wide traffic. Information Sciences. 2016 Jun 20;348:243-71.

[11] Chen PY, Zhang H, Sharma Y, Yi J, Hsieh CJ. Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models. InProceedings of the 10th ACM Workshop on Artificial Intelligence and Security 2017 Nov 3 (pp. 15-26). ACM.

[12] Papernot N, McDaniel P, Wu X, Jha S, Swami A. Distillation as a defense to adversarial perturbations against deep neural networks. In2016 IEEE Symposium on Security and Privacy (SP) 2016 May 22 (pp. 582-597). IEEE.

[13] Wang C, Zhao Z, Gong L, Zhu L, Liu Z, Cheng X. A distributed anomaly detection system for in-vehicle network using HTM. IEEE Access. 2018;6:9091-8.
[14] Yu Y, Long J, Cai Z. Network intrusion detection through stacking dilated convolutional autoencoders. Security and Communication Networks. 2017;2017.
[15] Yuan Z, Lu Y, Xue Y. Droiddetector: android malware characterization and detection using deep learning. Tsinghua Science and Technology. 2016 Feb;21(1):114-23.