Intrusion Detection System using Hybrid SVM-RF and SVM-DT in Wireless Sensor Networks

S. Prithi, S. Sumathi

Abstract—Intrusion detection system (IDS) is one of the essential security mechanisms against attacks in WSN. Network intrusion detection system (NIDS) generally uses the classification techniques in order to obtain the best possible accuracy and attack detection rate. In this paper, Intrusion Detection System is designed which uses two-stage hybrid classification method. In the first stage it uses Support Vector Machine (SVM) as anomaly detection, and in the second stage it uses Random Forest (RF)/Decision Tree (DT) as misuse. The abnormal activities are detected in the first stage. These abnormal activities are further analyzed and the known attacks are identified in the second stage and are classified as Denial of Service (DoS) attack, Probe attack, Remote to Local (R2L) attack and User to Root (U2R) attack. Simulation results reveal that the proposed hybrid algorithm obtains better accuracy and detection rate than the single classifier namely, SVM, RF and DT algorithm. The experimental results also shows that hybrid algorithm can detect anomaly activity in a reliable way. Proposed technique uses the standard NSL KDD dataset to evaluate/calculate the performance of the proposed approach. Here the results show that the proposed Hybrid SVM-RF/DT IDS technique performs better in terms of detection rate, accuracy and recall than the existing SVM, RF and DT approaches.

Index terms: Intrusion Detection System, Network attacks, Support Vector Machine, Wireless Sensor Network.

I. INTRODUCTION

Wireless Sensor Network is a collection of spatially deployed wireless sensors of small size by which various changes of environmental conditions such as forest fire, air pollutant concentration, and object moving can be monitored in a collaborative manner without relying on any underlying infrastructure support [1]. The security issue arises as the sensors are deployed openly in an unprotected environment and due to the dynamic behavior of the topology in WSNs. In general, network security solutions can be grouped into two main categories: prevention-based techniques and detection-based techniques. Detection based techniques aim at identifying the intrusions that affect the network infrastructure after a failure of the prevention-based techniques. An intrusion detection system is a detection-based technique which monitors either networks or other systems for malicious or anomalous behaviors. Complementing preventative technologies such as firewalls, strong authentication, and user privilege [2], IDSs have become an essential part of enterprise IT security management [3]. They are typically classified as either misuse-based or anomaly-based systems [4].

The misuse detection detects the attack type by comparing events with the previous attack's behavior and the current ones, whereas anomaly detection builds a model of normal behavior, and compares the model with detected events [9], catching those that deviates from the defined normal behavior. Data Mining (DM) techniques are increasingly being used to identify these attacks, anomalies or intrusions in a protected network environment [5]. Classification can be used as the main approach to map a data item into one of several predetermined classes. In this work, the various classification approaches such as Support Vector machine, Random Forest, Decision Tree and the hybrid approaches are focused on intrusion detection systems for wireless sensor networks.

The remaining sections of the manuscript is organized as follows. In section II a detailed literature survey is been carried out on the various intrusion detection system using machine learning algorithm. Section III discusses about the classification approaches and section IV discusses about the various modules used in proposed approach and section V experiments the proposed framework by evaluating the performance on various performance metrics and finally section VI delivers the concluding remarks.

II. RELATED WORK

In network security, Intrusion detection is considered as the foremost research problem which was anticipated by Anderson in 1980 [6]. A novel approach was proposed by Divyatmika et al. [22] to design a network-based intrusion detection system using machine learning approach. A two-tier architecture was designed to detect intrusions on network level. When the analysis depended on the network behavior, the data packets of TCP/IP was considered as input data. The data was preprocessed by parameter filtering and an autonomous model was designed on training set using hierarchical agglomerative clustering algorithm. Further, data got filtered as regular traffic pattern or intrusions using KNN classification. This lowered cost-overheads. The true positive rate of the architecture was 0.99 and false positive rate was 0.01. Thus, the architecture provided a better

Revised Version Manuscript Received on August 19, 2019.

S.Prithi*, Assistant Professor, Department of CSE, Rajalakshmi Engineering College, Chennai, Tamil Nadu., India.(Email: prithi.s@rajalaskhmi.edu.in)

Dr.S.Sumathi, Professor, Department of EEE, PSG College of Technology, Coimbatore, Tamilnadu, India.

security with low false positive rate and high true positive rate. Finally, they analyzed the normal network patterns and learnt progressively to isolate normal data and threats.

An experimental framework was developed by Laskov et al. [23] to perform a comparative analysis on classification and clustering techniques for detecting dubitable actions. Two schemes were used to analyze the data from these two techniques. Training and testing data were taken from the same unknown distribution. The schemes were based on the new or unseen data or patterns which helped them to understand the way IDS can induce its knowledge to new malicious patterns. This is a very essential part for an IDS system.

Hemalatha et al. [26] integrated the data mining concept with IDS to identify the relevant data efficiently and with a lesser execution time. The foremost issues such as classification of data, human interaction level, absence of labeled data, and the effectiveness of Distributed Denial of Service Attack was unraveled using the proposed algorithm. The algorithm was trained and tested using KDD Cup dataset and the results showed a reduced false alarm rate and better accuracy.

Norouzian et al. [28] proposed an efficient classification technique built on a Multilayer Perceptron Neural Network in order to detect and classify data into six classes. The MLP design was implemented with two hidden layers of neurons and an accuracy rate of 90.78% was achieved. Khalilian, et al. [11] conducted a survey of IDS short comings, challenges, and solutions. Denatious, et al. [12] presented a survey identifying DM techniques applied in IDSs to classify the known and unknown attack patterns. Similarly, Injadat et al. [13], discussed DM techniques in the social media context. A systematic literature review was conducted to identify distributed denial of service (DDoS) attacks threatening the existence of cloud-assisted WANs [14]. Sulaimam et al. [15] compared the advantages and disadvantages of the implemented DM techniques in IDSs. The use of similarity and distance measures within the network intrusion anomaly detection research was presented by Weller-Fahy et al. [16]. A comprehensive survey has been done on neural networks [25], fuzzy logic [19], support vector machines (SVM) [20] for designing an efficient and effective IDS. Classifiers are developed using these techniques to classify the incoming network traffics into normal or an attack class. This paper focuses on the Support Vector Machine (SVM), Decision Tree (DT) and Random Forest (RF) among various machine learning algorithms to improve the performance of detected rate and overall accuracy of IDS.

III. CLASSIFICATION APPROACHES

Intrusion detection system can be considered as a classification problem where each record can be classified as an intrusion or a normal data. In the recent decade data mining algorithms are used widely to detect and classify the intrusions. The data mining algorithms are focused to resolve the difficulty of analyzing huge volumes of data and to optimize the detection rules. Some of the classification techniques used for classifying attacks are Bayesian Classification, Neural Network, Decision Trees, Support Vector Machines, K-Nearest Neighbor and rule induction methods. By using a single classifier, the rate of detection will not be good. So, by applying hybridization on two or more classifiers intrusion detection datasets lead to a better performance than any single classifier.

A. Decision Trees (DT)

A DT is a tree-like graph or model, or rather an inverted tree because it has its root at the top and it grows downwards. The tree like structure makes DT meaningful and it can be interpreted easily when compared with other approaches. The goal is to create a classification model that predicts the value of a target attribute based on several input attributes. DT has three basic elements namely a decision node which specifies a test attribute, an edge that represents one of the possible attribute values and a leaf, also called an answer node, which contains the class to which the object belongs.

The possibility of over fitting the training data was reduced by Quinlan [7] C4.5 model. He used decision trees in his model and it yielded a good performance and offered some benefits such as fast and reliable when compared with other existing techniques. The C4.5 algorithm developed by Quinlan [7], generated decision trees using an information theoretic methodology. The performance of various machine learning techniques was surveyed and examined by Sabhnani and Serpen [24]. The objective is to construct decision tree with minimum number of nodes that gives least number of misclassifications on training data. The C4.5 algorithm used divide and conquer strategy. 20% of the records present in the KDD training dataset are set as initial window. After each iteration, from the initial window 20% of records were added and the tree was retrained. In all tests, at least two branches contained a minimum of two records. The best decision tree classifier model achieved the cost per example almost equal to 0.2396.

B. Support Vector Machine

Support vector Machine is a promising supervised learning mode put forward by Vapnik [27]. They are increasingly used as a learning algorithm to classify misuse detection. The input vector is mapped into a feature space with higher dimensional and an optimal hyper-plane is obtained in the higher dimensional feature space. Srinivas Mukkamala et al. [25] proposed SVMs which are mainly used in intrusion detection because of its speed and scalability and training and testing was performed on the DARPA 1998 dataset. The computational time of training set was 17.77 seconds and a accuracy rate of 99.50% was achieved by testing set with a computational time of 1.63 seconds.

C. Random Forest

Random forests are an ensemble learning method employing a multitude of decision trees during training period. Each tree is depended on the values of an independently sampled random vector. Same distribution is considered for all trees in the forest. Once the trees are generated, the most popular class is voted. The generalization error of a forest of tree classifiers are determined by the durability of individual trees in the forest and the correlation between them. The performance of a random forest is comparable with gradient boosting technique, but it is simpler to train and tune, thus making random forest very popular. Farnaaz and Jabbar [17] developed an intrusion detection system based on random forest method. The the effectiveness of the model was tested on an NSL–KDD dataset, and a detection rate of 99.67% was achieved. The drawback of RF algorithm is the slowness of the algorithm to construct many trees and is not suitable for predicting the data in real time. An intrusion detection model based on RF and weighted k-means was proposed by Reda et al. [10] and validation was done over the KDDCup'99 dataset. They were able to achieve accuracy of 98.3%.

In this section the different classification approaches used for detecting intrusion was studied. The challenge of intrusion detection system is to achieve high detection rate and to reduce false alarm rate. By using a single classifier, it is not adequate to accomplish this. Therefore, the classifiers are combined to give a better performance detection than any single classifier. So, in the proposed approach hybrid IDS approach is implemented to obtain high accuracy and high detection rate.

IV. PROPOSED METHODOLOGY& RESULTS

In the proposed method, a hybrid intrusion detection model is designed which combines the misuse and anomaly detection in order to classify the attack classes in intrusion detection dataset namely NSL KDD dataset. A hybrid intrusion detection model namely SVM-RF and SVM-DT are proposed to identify the intrusions with a high accuracy and detection rate. A single classifier doesn't lead to a better performance in terms of accuracy and detection rate so hybrid classifier is proposed. In the first stage, SVM classifier is used as anomaly detection where it classifies the dataset into normal and attack classes. In the second stage the RF/DT classifier is used as misuse detection which classifies the attacks into four classes, namely, DoS, U2R, R2L and probe classes. The proposed framework is depicted in Fig.1 which comprises of three modules that is dataset preprocessing module, classification module, and performance evaluation module.

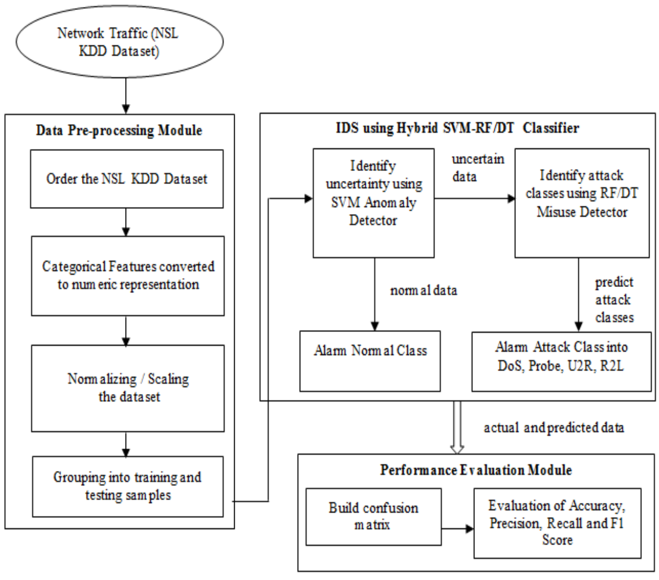
Network Traffic (NSL KDD Dataset)
Data Pre-processing Module
Order the NSL KDD Dataset
Categorical Features converted to numeric representation
Normalizing / Scaling the dataset
Grouping into training and testing samples
IDS using Hybrid SVM-RF/DT Classifier
Identify uncertainty using SVM Anomaly Detector
uncertain data
Identify attack classes using RF/DT Misuse Detector
normal data
predict attack classes
Alarm Normal Class
Alarm Attack Class into DoS, Probe, U2R, R2L
actual and predicted data
Performance Evaluation Module
Build confusion matrix
Evaluation of Accuracy, Precision, Recall and F1 Score

Fig.1 Proposed Framework

V. RESULTS AND DISCUSSIONS

The proposed Hybrid SVM-RF IDS and Hybrid SVM-DT IDS was implemented and evaluated. The experiment was performed on the standard NSL KDD intrusion dataset [18] using R Tool. The proposed approach is validated on the standard NSL-KDD dataset. The dataset is segregated into three datasets, namely dataset1 and dataset 2 with 65,535 samples and 32,767 samples respectively. The accuracy, detection rate, recall and F1-Score are compared and analyzed for NSL-KDD dataset with the existing approaches such as SVM, RF and DT. These datasets are processed and applied on the proposed Hybrid SVM-RF and SVM-DT IDS and the stage wise results are discussed in this section. The overall performance of the proposed Hybrid SVM-RF and Hybrid SVM-DT approaches are also discussed in this section.

A. Evaluation of Results

The proposed hybrid IDS is tested on NSL–KDD dataset, which is divided into three sets. Each set is split into 80% training samples and 20% testing samples and the proposed system is trained on 80% training samples and tested on 20% testing samples

Table 1 shows the number of training and testing samples used for the two types of set. The performance evaluation such as overall accuracy, precision and recall are evaluated and analysis is done on existing approaches such as SVM (linear) [21], SVM (RBF) [21], RF [21] and DT [8] and compared with the proposed approaches Hybrid SVM-RF and Hybrid SVM-DT IDS.

Table 1. 80% Training and 20%Testing Samples for NSL-KDD dataset

Dataset	Total Samples	Training Samples	Testing Samples
Set 1	65535	52428	13107
Set 2	32767	26213	6554

Analysis of Set 1 NSL-KDD Dataset (80% Training and 20% Testing)

The Hybrid SVM-RF IDS and Hybrid SVM-DT IDS are trained on 80% training samples and tested on 20% testing samples of set 1 and the performance metrics such as accuracy, precision and recall are evaluated and analyzed and shown in Fig.2. When compared to existing approaches, the accuracy of the proposed Hybrid SVM-RF performs 0.2% better than the proposed Hybrid SVM-DT, 5.35% increase in performance than DT [8], a rise of 2.17% accuracy than RF [21], 1.55% better than SVM (RBF) [21] and an increase of 0.98% than SVM (Linear) [21]. When compared to existing approaches, the precision/detection rate of the proposed Hybrid SVM-RF shows a slight margin of 0.21% increase than the proposed Hybrid SVM-DT, 0.4% better than DT [8], a rise of 1.82 % accuracy than RF [21], 2% better than SVM (RBF) [21] and an increase of 2.34% than SVM (Linear) [21]. The recall rate of the proposed Hybrid SVM-RF performs 0.2% better than Hybrid SVM-DT, increase of 3.44

% accuracy than RF [21], 2.43% rise than SVM (RBF) [21] and 2.07% better than SVM (Linear) [21] and 1.03% increase than DT [8].

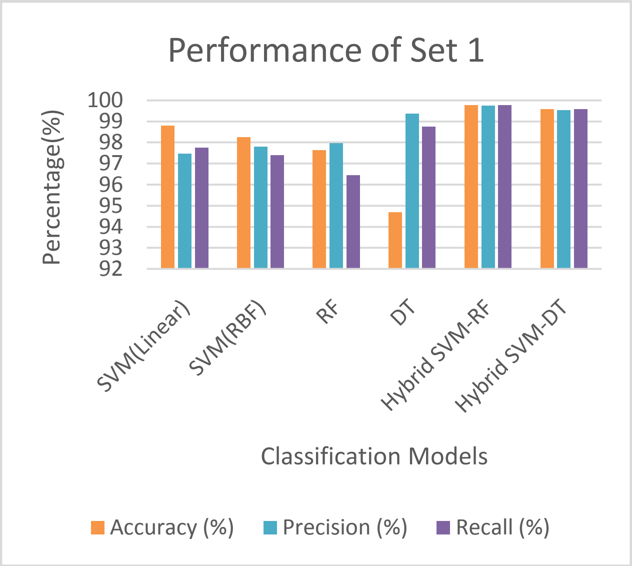

Fig.2. Performance of Set 1 (80% Training and 20% Testing)

Table 2 and Table 3 tabulates the classification report of Hybrid SVM-DT and Hybrid SVM-RF classifiers. It can be observed that the precision, recall and F1-score for U2R attacks seems to be only 50%, 22.22% and 30.76% respectively in case of hybrid SVM-DT and shows a better precision rate of 60%, recall as 37.5% and F1-score of 46.16% for Hybrid SVM-RF. It can be observed that the classification of U2R attack is comparatively low than the other attacks. Both Hybrid SVM-DT and Hybrid SVM-RF performs a poor detection rate, recall rate and F1-Score in detecting U2R attacks this is because the learning algorithm is triggered to be biased on subject to the most frequent records, thus prevent it from recognizing rare attack records.

Table 2. Classification Report of Hybrid SVM-DT of Set 1 (80% Training and 20% Testing)

	Precision (%)	Recall (%)	F1-Score (%)
Normal	99.59	99.71	99.65
DoS	99.77	99.92	99.84
R2L	93.69	88.89	91.23
Probe	99.34	98.78	99.06
U2R	50.00	22.22	30.76
micro avg	99.57	99.57	99.57
macro avg	88.48	81.90	85.06
weighted avg	99.56	99.59	99.57

Table 3. Classification Report of Hybrid SVM-RF of Set 1 (80% Training and 20% Testing)

	Precision (%)	Recall (%)	F1-Score (%)
Normal	99.68	99.91	99.79
DoS	99.96	99.98	99.97
R2L	99.06	91.38	95.07
Probe	99.75	99.33	99.54
U2R	60.00	37.5	46.16
micro avg	99.77	99.77	99.77
macro avg	79.81	85.62	82.61
weighted avg	99.75	99.79	99.77

Analysis of Set 2 NSL-KDD Dataset (80% Training and 20% Testing)

The accuracy of SVM (Linear), SVM (RBF), RF, DT, Hybrid SVM-DT and Hybrid SVM-RF on 20% testing samples and 80% training samples for Set 2 is shown in Fig.3. When compared to existing approaches, the accuracy of the proposed Hybrid SVM-RF performs 0.23% better than Hybrid SVM-DT, 2.42% better accuracy than RF [21], 1.18% better than SVM (RBF) [21], 1.33% better than SVM (Linear) [21] and 5.79% increase than DT [8]. When compared to existing approaches, the precision/detection rate of the proposed Hybrid SVM-RF performs a margin of 0.24% better than Hybrid SVM-DT, 1.78 % better detection rate than RF [21], 0.98% better than SVM (RBF) [21], 0.79% better than SVM (Linear) [21] and 0.95% increase than DT [8]. The precision rate of the proposed Hybrid SVM-RF performs 1.25% better than Hybrid SVM-DT, an increase of 2.25% recall rate than RF [21], 1.13% better than SVM (RBF) [21], 1.02% better than SVM (Linear) [21] and 2.11% increase than DT [8].

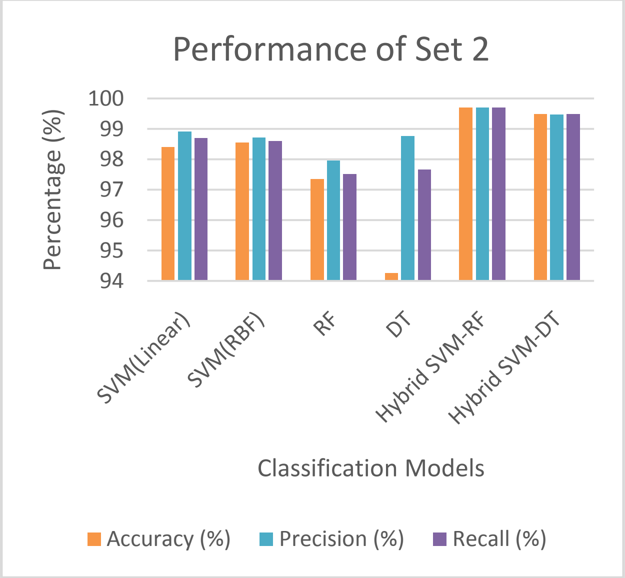

Fig.3. Performance of Set 2 (80% Training and 20% Testing)

Table 4 and Table 5 tabulates the classification report of Hybrid SVM-DT and Hybrid SVM-RF IDS. The report illustrates the precision, recall and F1-score for each type of class attack for Set 2 NSL-KDD data samples as well as the micro average, macro average and weighted average score for these three metrics. It can be observed that for the proposed Hybrid SVM-DT the precision, recall and F1-score for U2R attack seems to be only 50%, 20% and 28.57% respectively and for R2L attack class it produces 92.45% precision, 92,.45% recall and F1-score. In case of Hybrid SVM-RF the recall rate and F1-score for R2L attack is 91.07% and 94.45% but the precision rate, recall rate and F1-score for U2R attack seems to be 66.67%, 50% and 57.14% respectively.

Table 4. Classification Report of Hybrid SVM-DT of Set 2 (80% Training and 20% Testing)

	Precision (%)	Recall (%)	F1-Score (%)
Normal	99.71	99.48	99.59
DoS	99.70	99.87	99.78
R2L	92.45	92.45	92.45
Probe	97.96	99.14	98.55
U2R	50.00	20.00	28.57
micro avg	99.63	99.63	99.63
macro avg	87.96	82.19	84.98
weighted avg	99.46	99.51	99.48

Table 5. Classification Report of Hybrid SVM-RF of Set 2 (80% Training and 20% Testing)

	Precision (%)	Recall (%)	F1-Score (%)
Normal	99.57	99.91	99.74
DoS	100.00	99.87	99.93
R2L	98.08	91.07	94.45
Probe	99.67	99.02	99.34
U2R	66.67	50.00	57.14
micro avg	99.71	99.71	99.71
macro avg	92.80	87.97	90.32
weighted avg	99.70	99.72	99.71

VI. CONCLUSION

Several techniques such as anomaly-based IDS, misuse-based IDS, signature-based IDS have been used to design intrusion detection systems, but machine learning techniques such as Decision Trees, Random Forest, k-Nearest Neighbor (KNN, Support Vector Machine are common in recent literature. In this paper, a new intelligent network intrusion detection system using two-stage (Anomaly-Misuse) hybrid classification technique namely SVM-RF and SVM-DT have been proposed and tested. The different machine learning techniques, namely, SVM (linear), SVM (RBF), RF, DT and Hybrid approaches SVM-RF and SVM-DT are investigated and compared on NSL-KDD dataset. The results indicate that the ability of the proposed Hybrid SVM–RF IDS produces more accurate results as well as better detection rate than Hybrid SVM-DT IDS. In the future in order to improve the efficiency and computational time, neural network approaches such as Artificial Neural Network, Convolutional Neural Network can be used. Secondly, more appropriate set of attributes/features can be chosen for classifying network intrusions so that the accuracy of classification can be improved as well as optimization algorithms such as PSO, ACO, Cuckoo Search can be used to find an optimal set of attributes/features and finally the focus is to investigate the problem of security level in wireless sensor networks and to embed the proposed Hybrid SVM-RF IDS and Hybrid SVM-DT IDS in the intrusion detection model of the WSN.

REFERENCES

1. I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communication Magazine, vol. 40, 2002, pp. 102–114.
2. P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, “Practical real-time intrusion detection using machine learning approaches,” Computer Communications, vol. 34, no. 18, 2011, pp. 2227 – 2235.
3. S. Axelsson, “The base-rate fallacy and the difficulty of intrusion detection,” ACM Trans. Inf. Syst. Secur., vol.3, no.3, 2000, pp.186–205.
4. A.G. deSá,A. C. Pereira, and G. L. Pappa, “A customized classification algorithm for credit card fraud detection,” Engineering Applications of Artificial Intelligence, vol. 72, 2018, pp. 21 – 29.
5. W. Lee, S. J. Stolfo, and K. W. Mok, “A data mining framework for building intrusion detection models,” in Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No.99CB36344), pp. 120–132.
6. P. Anderson, "Computer security threat monitoring and surveillance," Technical Report, James P. Anderson Co., Fort Washington, PA, 1980.
7. Quinlan, “C4.5: Programs for Machine Learning,” 1993, Morgan Kaufmann Publishers, San Mateo, CA.
8. Vaishali Kosamkar, S Chaudhari Sangita, "Improved Intrusion Detection System using C4.5 Decision Tree and Support Vector Machine", International Journal of Computer Science and Information Technologies, vol. 5, no. 2, 2014, pp. 1463-1467.
9. K.Q. Yan, S. C. Wang., S.S. Wang and C.W. Liu, “Hybrid Intrusion Detection System for Enhancing the Security of a Cluster based Wireless Sensor Network,” in Proceedings of the Computer Science and Information Technology (ICCSIT), July 2010, vol.1, pp.114-118.
10. R. M. Elbasiony, E.A. Sallam, T.E. Eltobely, M. M. Fahmy, “A hybrid network intrusion detection framework based on random forests and weighted k-means,” in Shams Engineering Journal, Volume 4, Issue 4,2013,Pages 753-762, ISSN 2090-4479, https://doi.org/10.1016/j.asej.2013.01.003
11. M. Khalilian, N. Mustapha, M. N. Sulaiman, and A. Mamat, “Intrusion detection system with data mining approach: A review,” Global Journal of Computer Science and Technology, 2011.
12. D. K. Denatious and A. John, “Survey on data mining techniques to enhance intrusion detection,” in 2012 International Conference on Computer Communication and Informatics, Jan 2012, pp. 1–5.
13. M. Injadat, F. Salo, and A. B. Nassif, “Data mining techniques in social media: A survey,” Neurocomputing, vol. 214, 2016, pp. 654 – 670.
14. R. Latif, H. Abbas, and S. Assar, “Distributed denial of attack in cloud- assisted wireless body area networks: A systematic literature review,” Journal of Medical Systems, vol.38, no.11, 2014, pp.128.
15. A. S. Subaira and P. Anitha, “Efficient classification mechanism for network intrusion detection system based on data mining techniques: A survey,” in 2014 IEEE 8th International Conference on Intelligent Systems and Control (ISCO), Jan 2014, pp. 274–280.

16. D. J. Weller-Fahy, B. J. Borghetti, and A. A. Sodemann, “A survey of distance and similarity measures used within network intrusion anomaly detection,” IEEE Communications Surveys Tutorials, vol. 17, no. 1, 2015, pp. 70–91.
17. N. Farnaaz, M.A. Jabbar, “Random Forest Modelling for Network Intrusion Detection System,” Procedia Computer Science, Volume 89, 2016, Pages 213-217.
18. http://nsl.cs.unb.ca/NSL-KDD/
19. S. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review", Applied Soft Computing, vol.10, 2010, pp. 1-35.
20. S. Mukkamala, G. Janoski and A. Sung, "Intrusion detection: support vector machines and neural networks", in proceedings of the IEEE International Joint Conference on Neural Networks (ANNIE), St. Louis, MO, 2002, pp. 1702-1707
21. Ahmad, I., Basheri, M., Iqbal, M.J., Rahim, A.: “Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection,” IEEE Access 6, 2018, 33789–33795.
22. Divyatmika, Manasa Sreekesh, “A Two-tier Network based Intrusion Detection System Architecture using Machine Learning Approach,” International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016 in proceeding of IEEExplore.
23. Wenke Lee and Salvatore J. Stolfo “Data mining approaches for intrusion detection,” in Proceedings of the 7th USENIX Security Symposium - Volume 7, SSYM’98, pages 6–6, Berkeley, CA, USA, 1998.
24. Sabhnani M, Serpen G, “Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context,” in Proc. of the Intl. Conference on Machine Learning, Models, Technologies and Applications, vol. 1, 2003, pp. 209–215.
25. Srinivas Mockamole, Guadalupe Janoski, Andrew Sung, “Intrusion Detection: Support Vector Machines and Neural Networks,” in Proceedings of the IEEE International Joint Conference on Neural Networks, 2002, pp. 1702-1707.
26. G.V. Nadiammai, M. Hemalatha, “Effective approach toward Intrusion Detection System using data mining technique,” Egyptian Informatics Journal 2015, in proceeding Elsevier Pp 37–50.
27. Cortes, Vapnik, “Support-vector networks, Machine Learning,” vol.20, 1995, pp.273–297.
28. M. R. Norouzian and S. Merati, “Classifying attacks in a network intrusion detection system based on artificial neural networks,” in Advanced Communication Technology (ICACT), 2011 13th International Conference on, pp. 868–873.

AUTHORS PROFILE

Dr.S.Sumathi did her B.E ECEand Masters in Applied Electronics at GCT, Coimbatore. She has done her Ph.D. in the area of Data Mining. She is currently working as Professor in the Department of EEE, PSG College of Technology, Coimbatore. She has about 30 years of experience in teaching and research. Her research interest includes Neural Networks, Fuzzy Systems and Data Mining. She received Gold medal from the Institution of Engineers Journal, Computer Engineering Division, Subject Award for the research paper in 2002-2003 and also the Best Project Award for her UG technical report in 1999.

Ms.S.Prithi did her B.Tech degree in Information Technology at CSI College of Engineering, The Nilgiris and Masters in Computer Science and Engineering at Dr.M.G.R University, Chennai. She is pursuing her Ph.D. in the area of Automata Theory, Wireless Sensor Networks and Computational Intelligence. She is currently working as an Assistant Professor in Rajalakshmi Engineering College,Chennai. Her research interest includes Automata Theory, Network Security and Computational Intelligence.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication