A Simple and Effective Intrusion Detection System for Manets

M V D S Krishna Murty, Lakshmi Rajamani

***Abstract**: This work proposes a simple and effective Intrusion Detection System (IDS) to classify different attacks in MANETs. IDS extracts four features for every traffic pattern and applies Support Vector Machine algorithm over them for the classification. Before applying the feature extraction, the input traffic pattern is subjected to pre-processing as it is composed of non-uniform features. IDS classifies the input traffic pattern into three classes; they are normal, blackhole and wormhole. Finally, this work analyses the feasibility of machine learning algorithms for the detection of security attacks in MANETs. For experimental validation, we have referred a self-created dataset which was acquired from the observations of blackhole and wormhole attacked node's traffic patterns. Moreover, we have also validated the proposed method through NSL-KDD dataset.*

***Keywords**: Intrusion Detection System, Preprocessing, Feature Extraction, Support Vector Machine, Self-Created Dataset.*

I. INTRODUCTION

Mobile Ad hoc networks (MANETs) are one of the wireless networks formed with the mobile devices as nodes. Due to the nature of decentralized communication, MANETs have gained huge interest in different applications including emergency rescue operations, military operations, collaborative distributed computing, disaster management and some personal network applications [1] etc. Due to the unique characteristics of mobile nodes, there are several challenges in MANETs which need to be solved. Among the several challenges, the mobility is the major challenge and it consequences to several sub-challenges. Almost all the problems in MANETs are linked with mobility of nodes. Among several sub-challenges, secure data exchange between mobile nodes is the major challenge. Due to the open network topology, distributed nature, and the absence of centralized administration in MANETs, the mobile nodes are susceptible for various attacks [2].

Manuscript received on 31 January 2023 | Revised Manuscript received on 06 February 2023 | Manuscript Accepted on 15 February 2023 | Manuscript published on 28 February 2023.

*Correspondence Author
M V D S Krishna Murty*, Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad (Telangana), India. E-mail: mkrishnamurty@gmail.com, ORCID ID: https://orcid.org/0000-0002-4705-3818
Dr. Lakshmi Rajamani, Professor and Head (Retd), Department of Computer Science and Engineering, Osmania University, Hyderabad (Telangana), India. E-mail: drlakshmiraja@gmail.com

The impact of these attacks ranges from naïve passive eavesdropping to serious battery draining attacks [3]. Majorly the attackers focus on the resources of mobile nodes like battery power, bandwidth, and data. Among the several security attacks in MANETs, blackhole attack [4] and wormhole attack [5] are the two major attacks which cause serious damages to the network. These two attacks are dynamic in nature and varies based on several network parameters. Hence, the identification of mobile nodes those were attacked with blackhole and wormhole attacks is much difficult. Recently, the involvement of artificial intelligence has been increased in different applications. Compared to the static algorithms which cannot provide any prior information about the attacks to mobile nodes, the machine learning algorithms which train the nodes can help in proper and accurate detection of attacks. A mobile node trained with the attack's characteristics can easily identify the attacked or compromised neighbour node. Hence our research has got motivated with these issues and focused over the development of effective Intrusion Detection System to solve these problems up to certain extent. This paper explains a simple and effective Intrusion Detection System for the classification of mobile nodes into three classes; they are normal, blackhole and wormhole. The overall system composed of three phases; they are pre-processing, features extraction and classification. At the initial phase, the input data is normalized and transformed into a unique format because the raw data collected from MANETs is non-uniform in nature. For feature extraction, we have employed four statistical features namely mean, variance, maximum and minimum. After feature extraction, we have applied principal component analysis for dimensionality reduction and finally Support Vector Machine (SVM) algorithm is used for classification.

The remaining paper is organized as follows; Section II explores the literature survey on IDS methods. Section III explores the details of proposed approach. Section IV explores the details of experimental analysis and the final Section concludes the paper.

II. LITERATURE SURVEY

IDS mainly works based on the principle of machine learning and information processing. In IDS, the mobile node initially learns about the characteristics of different attacks through machine learning algorithms and it becomes ready to identify the attack if occurs. IDS works on the features of network traffic (data packet and control packets).

Retrieval Number: 100.1/ijies.B10770210223
DOI: 10.35940/ijies.B1077.0210223
Journal Website: www.ijies.org

*Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.*

For an incoming traffic pattern, the node analyses its features and matches those features with the features by which it was trained. If the features of incoming packet are matched with attack features, then the incoming traffic is declared as an attacked packet or packet coming from attacked node.

The earlier IDS works [6-9] are employed on fixed network traffic which was acquired in specific situations. In that, researchers kept a monitoring unit in networked system and analyzed the flow of traffic. Based on the analysis, they formulated standard datasets and kept for public use. KDD-CUP 99 is such kind of dataset which was generally used by the researchers. In this section, we explore the details about several earlier IDS mechanisms.

Ji et al. [10] proposed the IDS model in three steps; feature selection, visual analysis and classification. Under feature selection, this method employed a signal processing technique, i.e., Multi-level Discrete wavelet transform (MDWT). Next, for visual analysis, iPCA is employed and finally for classification, the SVM algorithm is employed. NSL-KDD dataset is used to validate the developed IDS model. However, the data connections related to data traffic won’t have any significance of high and low frequencies. Ambusaidi et al. [11] have developed filter based feature selection mechanism called as Flexible Mutual Information based Feature Selection (FMIFS) to select optimal features for data traffic connections.

FMIFS employs mutual information(MI) to determine the mutual dependency between features and based on the obtained MI values, the duplicate features are eliminated. The duplicate features are the features those have less contribution towards the class as well as neighbor features. Least Square SVM (LS-SVM) is employed for classification and the simulations are conducted on the three datasets such as KDD cup99, NS-KDD and Kyoto2006+. Fei Zhao et al. [12] proposed a new feature selection algorithm called as Redundant Penalty between Features based on Mutual Information (RPFMI) to select optimal features.

The RPFMI considers three factors during the feature selection; they are redundancy between features, the effect between selected features, classes and their relationship with candidate features. Two datasets such as KDD Cup99 and Kyoto 2006+ are employed for experimental validation. The performance is measured through accuracy measure. Jingping Song et al. [13, 14] proposed a Modified Mutual Information based feature Selection (MMIFS) method for intrusion detection. After the selection of features through MMIFS, they employed C4.5 classifier for classification purpose.

For simulation purpose, they used KDD Cup99 dataset and performance is measured through accuracy measure. G. Farahani [15] proposed a new method called as Cross-Correlation based feature selection (CCFS) and employed four classifiers for classification purpose. The four classifiers are namely K-nearest neighbor (KNN), Decision Tree (DT), Naïve Bayes (NB) and SVM. The main purpose of CCFS is dimensionality reduction and thereby reduction of computational burden. For simulation purpose, they have considered four datasets such as KDD Cup99, NSL-KDD, AWID and CIC-IDS2017 and the performance is measured through accuracy, recall and precision.

Chun Meng et al. [16] proposed an improved version of K-means algorithm for intrusion detection in computer networks. Initially, the PCA algorithm is applied to reduce the dimensionality of dataset and then the outlier detection is used for the elimination of outliers that have great impact on the final clustering results. The initial clustering center is chosen with the help of distance such that it can get an optimal local solution and then the K is used to get final cluster centers.

Simulation is done with the help of KDD Cup99 and the performance is measured through detection rate, and false positive rate. Wang et al. [17] proposed an ensemble method for the anomaly based intrusion detection. This method combined two ML algorithms namely Artificial Neural Networks (ANN) and Fuzzy Clustering (FC). FC is adopted for the creation of different training sets and ANN is adopted for the training of created models. Finally they applied fuzzy aggregation module to find the average results of all models. Experiments are conducted through the KDD Cup 99 dataset and performance is measured through detection stability and precision.

Hoz et al. [18] proposed an anomaly based model by hybridizing three algorithms namely Probabilistic Self Organizing Maps (PSOMs), Fisher Discriminant Ratio (FDR) and Principal Component Analysis (PCA). In their method, the FDR and PCA are aimed at the discovery of feature selection by suppressing noises. PSOMs are aimed at the modelling the feature space and to ensure a perfect discrimination between normal and malicious connections. The detection capabilities are altered without repetitive training but by altering the probable activation units.

III. PROPOSED APPROACH

The overall working mechanism of proposed IDS is shown in Figure.1. Accordingly, the proposed mechanism initially preprocesses the input data and then extracts features. Finally, the obtained features are fed to machine learning algorithm for classification. As an additional methodology, the obtained features are processed through principal component analysis (PCA) for dimensionality reduction.

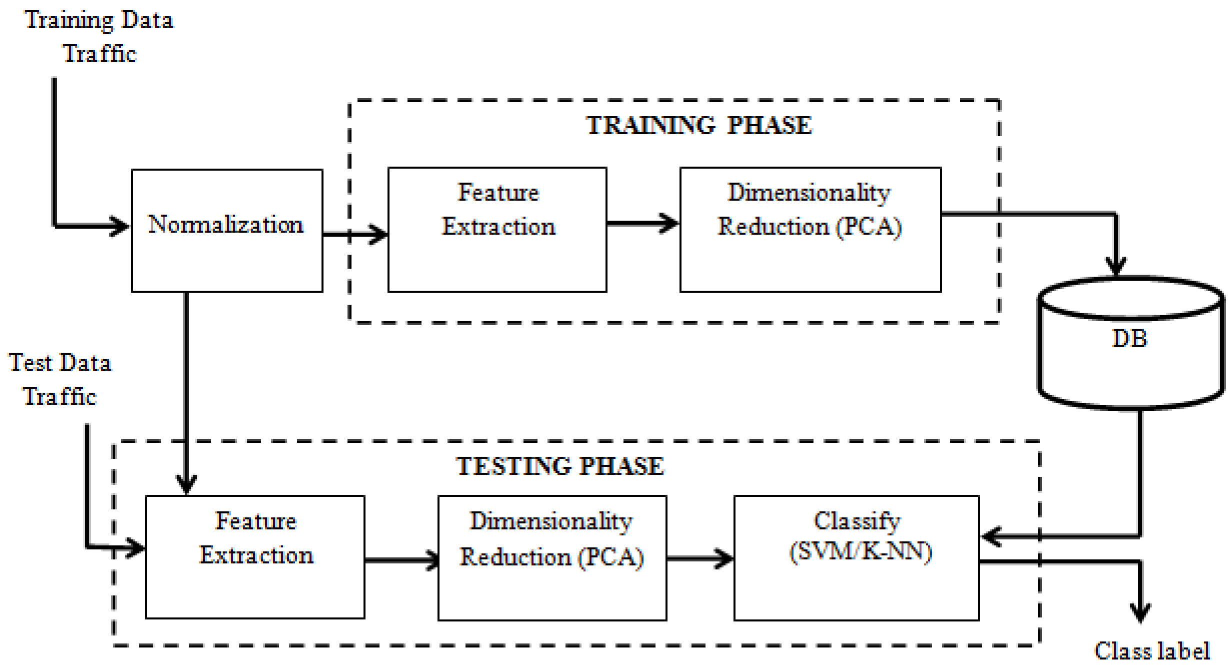

Figure.1 Overall Block Diagram of IDS Mechanism

3.1 Normalization

The features of packet in raw form can be inconsistent, incomplete, redundant and noisy. In the obtained blackhole and wormhole packet features, every packet is represented with a set of features and they are not in the same format. Some features are symbolic in nature, some features sand numerical and some features are in binary format. To process this dataset, all the features are needed to be in an uniform format. Hence to sort out all these problems, data normalization is needed and it varies from dataset to dataset. For demonstration purpose, here we employed a step-by-step normalization process as shown below-

Step 1: Consider the dataset X with size $M \times N$, where M is total number of packets and N is total number of features used to represent each packet.

Step 2: Fetch the features those need to be normalized

$$F_i = X(i); \quad (1)$$

Where F_i denotes the i^{th} feature which needs to be normalized. In case of our new dataset, we found that each packet is represented with 52 features of which 31 are symbolic, 8 are numeric and the remaining are binary. Here, only symbolic features are processed for normalization. Thus, the value of *i* in Eq. (5.1) varies from 1 to 31.

Step 3: Find out the total number of occurrences of each feature by comparing it with its name specified already. The comparison followed by count is done as follows:

$$M_i = \sum_{i=1}^{L} strcmp(F_i, Feature\_X) \quad (2)$$

Where $Feature\_X$ represents the individual feature name and the F_i represent the i^{th} feature in every row.

Step 4: Measure the probability of each feature given as

$$PF_i = \frac{M_i}{Length(X)} \quad (3)$$

Where M_i is the total number of occurrences of feature *i* and $Length(X)$ denotes the total size of respective row.

Step 5: Replace the probability values of i^{th} feature in their respective position in the row X.

For other datasets, if we observe the incomplete connections, then the connection is completed by adding zeros in sufficient number. Similarly for the datasets which have connections with abnormal values like NaN and Infinity, they are replaced with 0's.

3.2 Feature Extraction

For feature extraction, we measure totally four types of features; they are mean, standard deviation, maximum and minimum. Each packet is represented with these four features. At training phase, every packet is initially processed for block division and then each block is processed to compute four features. Then the obtained features are processed through PCA to get only principal components. For a given row X of size, 1×52, it is divided into several overlapping blocks of size $1 \times w$. The mathematical calculations of the four features are described as follows:

A. Mean: The mean is measured as a ratio of summation of features in the block to the total number of features in that block.

$$\mu = \frac{1}{w}\sum_{i=1}^{w} p_i \quad (4)$$

Where p_i is the feature at i^{th} position in the block of size $1 \times w$.

B. Maximum: For a given Block Bx of size $1 \times w$, the maximum feature is calculated as

$$Mx = Max(B) \quad (5)$$

C. Minimum: For a given Block Bx of size $1 \times w$, the minimum feature is calculated as

Retrieval Number: 100.1/ijies.B10770210223
DOI: 10.35940/ijies.B1077.0210223
Journal Website: www.ijies.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

$$Mn = Min(B) \tag{6}$$

D. Standard deviation: Standard deviation explores the statistical distribution relative to the mean. Standard deviation can also be called as square root of variance. For a given Block Bx of size $1 \times w$, the standard deviation is

calculated as

$$\sigma = \sqrt{\frac{1}{wxw}\sum_{i=1}^{wxw}(p_i - \mu)^2} \tag{7}$$

Hence, each packet is represented with B number of mean values, standard deviation values, maximum values and minimum values. For example, if the B value is 20, then each packet is represented with 20 mean values, 20 standard deviation values, 20 maximum values and 20 minimum values. Thus, the total number of features used to represent one packet is 80. For instance, if 300 packets are used for every class to train the system. In such case, each class is represented with totally 80*300 = 24,000 features which are huge in number. Hence, we have applied PCA to reduce the dimension with less information loss. Similarly, the PCA is applied over the test packet also.

3.3 Classification

For classification purpose, we have employed the most popular SVM algorithm. Basically, the SVM increases the samples size such that it can separate them effectively. Hence, instead of general trend towards the dimensionality reduction, SVM follows an opposite process and increases the size of features. The main idea is to determine a hyperplane to put the samples from class inside it. SVM employs kernel functions that postulate the linear and non-linear features and hence it is able to construct a separating plane that is implicitly defined by the kernel function. Here, we have employed LIBSVM for classification purpose at first stage.

IV. EXPERIMENTAL ANALYSIS

To show the effectiveness of proposed IDS model, we have conducted a vast set of experiments over different datasets and the performance is analyzed at every dataset. Initially, we explain the details of datasets. Next we explore the details of observed results and performance metrics. Finally we alleviate the effectiveness of proposed model by comparing the results obtained through existing methods.

4.1 Datasets and Settings

For simulation, we have considered two datasets; they are NSL-KDD and self-created dataset. Initially the details of self-created dataset are explained and then the details of NSL-KDD.

A. Self-created dataset

This is the real time dataset which we have acquired during our research on the blackhole and wormhole attacks in MANETs. The main theme behind this dataset is the observation of packet characteristics in the network in the presence of blackhole and wormhole attacks. As we used AODV for routing, the packet features are derived based on the characteristics of AODV protocol. In our research, we found that each packet is represented with 52 features. For dataset creation, we varied different network parameters and analyzed the packets coming from blackhole and wormhole attacked nodes. Based on the analysis, we have accumulated different features those have strong relation with blackhole and wormhole attack. Alongside, we have also acquired the features with normal characteristics, i.e., no attack. On an average, we have acquired totally 12,354 normal packet traffic patterns, 6128 blackhole associated packet traffic patterns and 6355 wormhole associated packet traffic patterns. In each class, we have employed 70% for training and 30% for testing. The details of simulation data of self-created dataset is shown in Table.1.

Table. 1 Self-created dataset statistics

Class/Set		Total Traffic Patterns	Training (70%)	Testing (30%)
Normal		12,354	8648	3706
Attacks (12,483)	Blackhole	6128	4290	1838
	Wormhole	6355	4449	1906

B. NSL-KDD

The NSL-KDD is a revised version of KDD cup 99 dataset that has been proposed by Tavallaee et al. This dataset is reconstructed by addressing several problems of KDD cup99 like huge number of redundant records. To group the connections into five groups, the initial dataset was subjected to different classifiers and everyone is labeled with the number of successful estimations. This dataset consists of five types of classes. They are Normal, DoS, U2R, R2L and Probe. Among these classes, the first one is non-attack and the remaining four are attacks. Each connection of NSL-KDD dataset consists of 41 features. Further, the dataset consists of three different sets, they are KDDTrain$^+$, KDDTest$^+$ and KDDTest^{-21}. The initial set, i.e., the KDDTrain+ consists of 125973 connections among them 67343 are normal traffic connections and 58630 are attack traffic connections. In the second set, i.e., KDDTest$^+$, the total number of traffic connections are 22544 among them 9711 are normal traffic connections and 12833 are attack traffic connections. Finally in the KDDtest^{-21} set, the total number of connections present are 11850 out of which 2152 are normal traffic connections and 9698 are attack traffic connections. We have conduct ed a cross validation over the KDDTrain$^+$ set and also considered a validation test using KDDTest+ and KDDTrain-21 sets. The details of number of connections present in these sets are demonstrated in Table.2

Table. 2 NSL-KDD Dataset Statistics

Class/Set		KDD Train$^+$	KDD Test$^+$	KDD Test^{-21}
Normal		67343	9711	2152
Attacks	DoS	45927	7458	4342
	U2R	52	200	200
	R2L	995	2754	2754
	Probe	11656	2421	2402
	Total	58630	12833	9698
Total		125973	22544	11850

Table. 3 Confusion Matrix of Self-Created Dataset

Actual/ Predicted	Normal	Blackhole	Wormhole	Total
Normal	**3335**	200	171	3706
Blackhole	300	**1360**	178	1838
Wormhole	372	200	**1334**	1906
Total	4007	1760	**1683**	7450

Table. 4 Performance Metrics of Proposed Method for Self-Created Dataset

Class/Metric	DR (%)	PPV (%)	FNR (%)	FPR (%)	FAR (%)	F-Score (%)
Normal	89.9952	83.23	10.01	16.77	13.39	86.4852
Blackhole	73.9965	77.2741	26.012	22.7345	24.37	75.6042
Wormhole	69.9522	79.2652	30.0142	20.7415	25.371	74.3429

4.2 Results

Initially, we have explained the results of self-created dataset and then the details of NSL-KDD. For both datasets, we have trained the system with the number of specified patterns in the above tables. Once the training is completed, we started testing through the testing connections. After the completion of testing, a confusion matrix is formulated based on detected results. From that confusion matrix, we have measured the performance through several performance metrics.

Table.3 shows the confusion matrix of the results obtained after the simulation of proposed model over self-created dataset. For the simulation purpose, we have considered only 70% of training data and 30% testing data. Actually, the original self-created dataset has 17,387 traffic connections in training set and 7000 traffic connections in testing set. Here, we aimed to conduct a five-fold cross validation mechanism and hence we have considered only 70% of data for training and 30% for testing phases. At every validation, we have removed some traffic connections from the past trained and test sets and add new connections those were not used in earlier validations. In this way, we have conducted totally five-fold cross validations and the best results are shown in Table.3. Based on these values, the performance is measured through several performance metrics and they are shown in Table.4. From these values, we can observe that the maximum DR and PPV are observed for normal patterns. Since the normal traffic patterns are much deviated from attacked traffic patterns, the system can classify them effectively. In the remaining two classes, the larger false positives are observed with normal traffic as they have much deviation with individuals. The blackhole packet characteristics are much different with the characteristics of wormhole packet; they experienced more false positives with normal category. For instance, we can see the FP of normal is 300 while FP of wormhole is only 178 under blackhole category. Similarly, the FP of normal is 372 while the FP of blackhole is only 200 under wormhole. Based on these observations, we can say that the packet characteristics vary significantly when the attack on the nodes changes. In such scenario, the common malicious node identification mechanism is not suitable. Every attack needs specific detection mechanism and then only the MANET can be protected from serious network attacks.

Further, the individual analysis is carried out by varying the kernels in SVM algorithm. In this case study, we have changed the traffic patterns used for training and testing along with kernels. For each fold, we have employed three kernels such as Linear, Polynomial and RBF and performance is measured through F-score. The results are shown in the following figures.

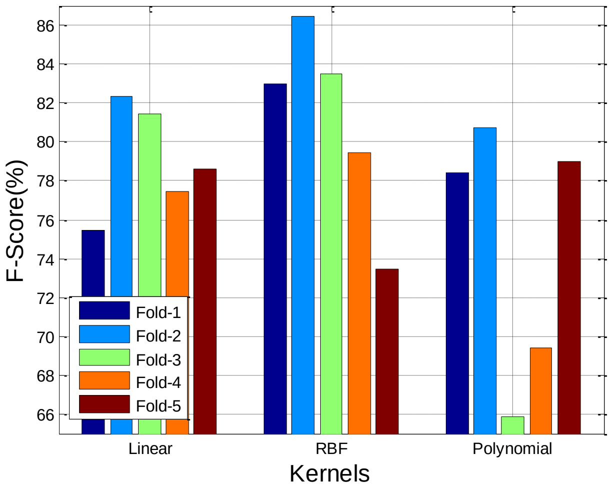

Figure. 2 F-Score of Normal Class Under Different Kernels

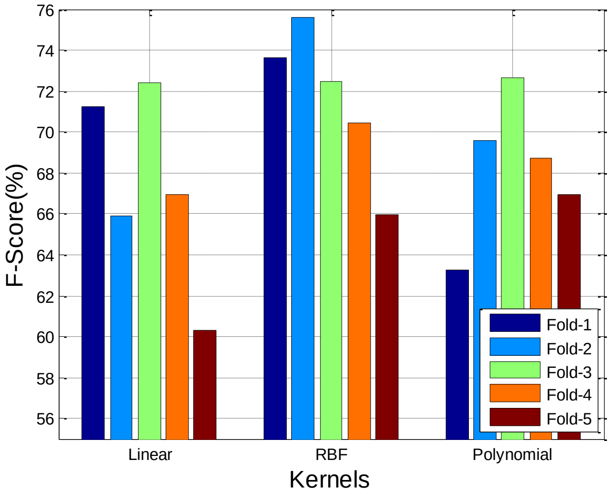

Figure. 3 F-score of Blackhole Atack under different kernels

Figure.2, Figure.3 and Figure.4 shows the F-core analysis for three different categories such as normal, blackhole and wormhole attacks. The analysis is carried out under different kernels and in different folds. From the results, the maximum F-score is observed at RBF kerenl and it is approximatley 86.4842%, 75.6030% and 74.3433% for normal, blackhole and wormhole atatcks respectively. Further, the average F-score of normal class is observed as 79.0620%, 81.1560% and 74.6820% for Linear, RBF and Polynomial kernels respectively. Next, the the average F-score of blackhole attack class is observed as 67.3640%, 71.6300% and 68.2280% for Linear, RBF and Polynomial kernsl respectively. Finally, the average F-score of wormhole attack class is observed as 66.9460%, 70.4300% and 66.6280% for Linear, RBF and Polynomial kernals respectively.

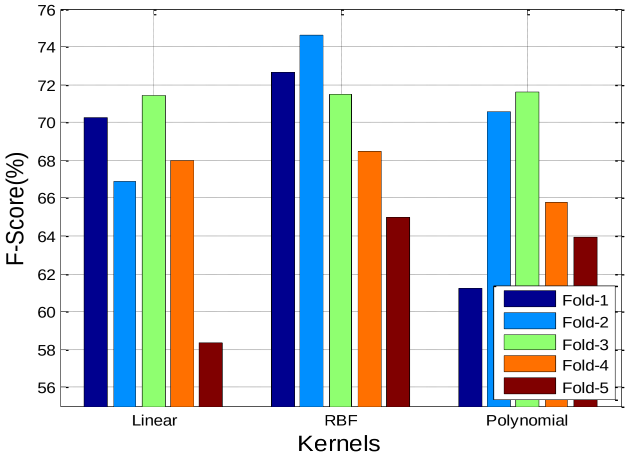

Figure. 4 F-score of Wormhole Under Different Kernels

Table.5 shows the confusion matrix of the results obtained after the simulation of NSL-KDD dataset. To construct this matrix, we have simulated the traffic connections of 75% of KDD Train+ and KDD Test+. This dataset is also subjected to five-fold cross validation by exchanging the traffic connections of each and every class. At every validation, 25% of connections are replaced with new traffic connections in both training and testing sets. The selection of traffic connections is done randomly and there is no specific criterion for this process. Based on the values shown in Table.5, the performance metrics are calculated and demonstrated in Table.6.

Table. 5 Confusion matrix of results from the simulation of KDD Test$^+$ of NSL-KDD dataset

	Normal	DoS	U2R	R2L	probe	Total
Normal	**5826**	925	100	100	332	7283
Dos	705	**4205**	164	136	383	5593
U2R	19	10	**103**	11	7	150
R2L	241	160	200	**1342**	122	2065
Probe	165	105	115	87	**1343**	1815
Total	6956	5405	682	1676	2187	**16906**

Table. 6 Performance Metrics of Proposed Method for KDD Test$^+$ of NSL-KDD Dataset

Class/Metric	DR (%)	PPV (%)	FNR (%)	FPR (%)	FAR (%)	F-Score (%)
Normal	79.9900	83.7600	20.0100	16.2400	18.1300	81.8300
DoS	75.1800	77.8000	24.8200	22.2000	23.5100	76.4700
U2R	68.6700	15.1000	31.3300	84.9000	58.1200	24.7600
R2L	64.9900	80.0007	35.0100	19.9300	27.4747	71.7500
Probe	73.9900	61.4100	26.0100	38.5900	32.3000	67.1200

Based on the performance metrics, we can observe that the maximum recall and precision are observed at the classification of normal class. Further, among the attack classes, the major attacks such as DoS and Probe have gained almost equal performance while the minor attacks have gained slightly lower performance. From Table.5.7, the average DR is observed as 72.5640% while the average PPV, FPR, FNR, FAR and F-score are observed as 63.6141%, 27.4360%, 36.3720%, 31.9069% and 64.3860% respectively. Compared to different earlier methods those worked on NSL-KDD datasets, the proposed method had not shown encouraging performance because it has considered only the basic features which are not able to explore the in-depth discriminative characteristics of attacks. However, to provide a support for self-created dataset, we have conducted this simulation.

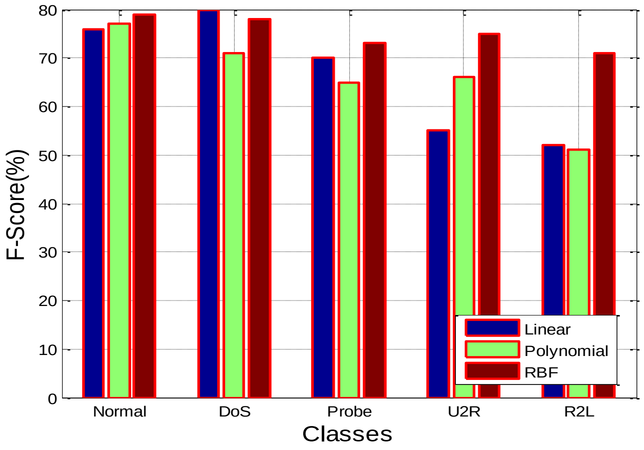

Figure. 5 Average F-score of Uder Different SVM Kernels

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Figure.5 shows the comparison between different kernels through mean F-scores. To do this simulation, the SVM is employed with three set of kernels; they are Linear, RBF and Polynomial. From the results, we can see that the maximum F-score is obtained at Linear kernel for the classification of DoS attack. The average F-score for Linear kernel is observed as 66.6320% while for Polynomial and RBF kernels, it is observed as 67.1240% and 75.2014% respectively.

V. CONCLUSION

This work mainly aimed at the analysis of machine learning algorithm in the detection of several security attacks in MANETs. As there is no work employed for the detection of malicious nodes in MANETs through machine learning algorithms, we were interested to do a simple analysis and carried out over the packet features acquired from real time data. The major novelty is the self-created dataset which was acquired from data packets passing through MANETs. The accomplishment of information process and machine learning algorithms over the self-created dataset revealed the possibilities to deploy machine learning strategies in MANETs for malicious nodes identification. Based on the simulation studies, we conclude that the IDS is effective for purely static data (created in the past by observing several network traffic) which may or may not work effectively on MANETs. As the mobile nodes are dynamic and the attacks are purely random in nature, a system trained with a constant set of features can’t show encouraging detection results

ACKNOWLEDGEMENT

Authors acknowledge the immense help received from the scholars whose articles are cited and included in references of this paper. The authors are obliged to authors/editors/publishers of all those articles, journals, and books from where the literature of this paper has been reviewed.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	Conceptualization, software, methodology, validation, formal analysis, investigation, M V D S Krishna Murty; writing-original draft preparation, M V D S Krishna Murty; writing-review and editing, M V D S Krishna Murty, Lakshmi Rajamani

REFERENCES

1. G. A. Walikar, R. C. Biradar, A survey on hybrid routing mechanisms in mobile ad hoc networks, *Journal of Network and Computer Applications*, 77 (2017) 48-63. [CrossRef]
2. G. Dhananjayan and J. Subbiah, “T2AR: trust-aware ad-hoc routing protocol for MANET”, *SpringerPlus (2016) 5:995*. [CrossRef]
3. Serhani, N. Naja, and A. Jamali. QLAR: A Q-learning based adaptive routing for MANETS. *In Computer Systems and Applications*, pages 1–7, 2017. [CrossRef]
4. Raja Mahmood RA, Khan AI, “A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks, *International Symposium on High Capacity Optical Networks and Enabling Technologies*, Dubai, United Arab Emirates, November 2007. [CrossRef]
5. Yih-Chun Hu, A. Perrig, D.B. Johnson, “Wormhole attacks in wireless networks”, ***IEEE** Journal on Selected Areas in Communications*, Vol. 24, Issue. 2, Feb. 2006, pp.370-380. [CrossRef]
6. H. J. Liao, C. H. Richard Lin, Y.C. Lin, K. Y. Tung, “Intrusion detection system: a comprehensive review”, *J. Netw. Comput. Appl*. 36 (2013) 16–24. [CrossRef]
7. A. Murali, M. Rao, “A survey on intrusion detection approaches”, *in: Proc. 1st Int. Conf. Inf. Commun. Technol. ICICT*, 2005, pp. 233–240.
8. C. Kolias, G. Kambourakis, M. Maragoudakis, “Swarm intelligence in intrusion detection: a survey”, *Comput. Secur*. 30 (2011) 625–642. [CrossRef]
9. Ahmed, M. , Mahmood, A. N. , & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60* , 19–31 [CrossRef]
10. S.-Y. Ji, B. K. Jeong, S. Choi, D.H. Jeong, “A multi-level intrusion detection method for abnormal network behaviors”, *J. Netw.Comput. Appl*. 62 (2016) 9–17. [CrossRef]
11. M.A. Ambusaidi, X. He, P. Nanda, Z. Tan, “Building an intrusion detection system using a filter-based feature selection algorithm”, *IEEE Trans. Comput*. 65 (2016) 2986–2998. [CrossRef]
12. Fei Zhao, Jiyong Zhao, Xinxin Niu, Shoushan Luo and Yang Xin, “A Filter Feature Selection Algorithm Based on Mutual Information for Intrusion Detection”, Appl. Sci. 2018, 8, 1535; doi:10.3390/app8091535. [CrossRef]
13. Jingping Song, Zhiliang Zhu , Peter Scully, Chris Price, “Modified Mutual Information-based Feature Selection for Intrusion Detection Systems in Decision Tree Learning”, Journal of Computers, Vol. 9, No. 7, July 2014, pp.1542-1546. [CrossRef]
14. Jingping Song, Zhiliang Zhu, and Chris Price, "Feature Grouping for Intrusion Detection Based on Mutual Information," Journal of Communications, vol. 9, no. 12, pp. 987-993, 2014.
15. G. Farahani, “Feature Selection Based on Cross-Correlation for the Intrusion Detection System”, *Hindawi Security and Communication Networks*, Volume 2020, Article ID 8875404, 17 pages. [CrossRef]
16. Chun Meng, Yuanyuan Lv, Long You and Yuchen Yue, “Intrusion Detection Method Based on Improved K-Means Algorithm”, *IOP Conf. Series: Journal of Physics: Conf. Series* 1302 (2019) 032011. [CrossRef]
17. G. Wang, J. Hao, J. Ma, and L. Huang, “A new approach to intrusion detection using artificial neural networks and fuzzy clustering,” *Expert Systems with Applications*, vol. 37, no. 9, pp. 6225 – 6232, 2010. [CrossRef]
18. E. De la Hoz, E. De La Hoz, A. Ortiz, J. Ortega, and B. Prieto, “PCA filtering and probabilistic SOM for network intrusion detection,” *Neurocomputing*, vol. 164, pp. 71–81, 2015. [CrossRef]

AUTHORS PROFILE

M V D S Krishna Murty, completed B.E. in CSE from University of Madaras, Chennai and M. Tech in CS from JNTU, Hyderabad. Currently, he is a research scholar in the department of CSE at JNTUH, Hyderabad. His area of interests are MANETs and Machine Learning. He has 21 years of teaching experience and 5.5 years of industrial experience as a software professional. He has presented technical papers in the area of MANETs and Data Science at international conferences held in India. Also, he has publications in reputed international journals.

Dr. Lakshmi Rajamani, obtained Ph.D (CSE) from Jadavpur University, Kolkata and worked as a Professor and Head in the department of CSE at OUCE, Osmania University, Hyderabad. Her area of interests are Fuzzy Logic and Network Security. She has several papers published in reputed international journals. Also, she has presented technical papers in international conferences held in India and abroad.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.