Intrusion Detection System using One Class SVM with and without Feature Selection in Wormhole Attack Detection

T. J. Nagalakshmi, P. C. Kishore Raja, S. Pravin Kumar, V. Veeramanikandan

Abstract: ***An Ad-hoc network is a kind of wireless construction from one to another computer, without having Wi-Fi access point or Router. However, the Ad hoc approach offers marginal security and decreases the data transfer rate. Consequently, it helps the attacker to connect with the ad-hoc network without any trouble. Therefore, a robust and reliable intrusion detection system (IDS) is a necessity of today's information security domain. These IDS systems play a vital role in monitoring the threats encountered in a network by detecting the change in the normal profile due to attacks. Recently, to detect attacks the IDS are being equipped with machine learning algorithms to attain better accuracy and fast detection speed. Most of the IDS use different network features. However, enormous number of features makes the detection and prevention complicated. The IDS presented in this paper employs random forest and principal component analysis to minimize the number of features for network IDS for wireless ad hoc networks. The one class SVM has been used for detection of worm hole attack with and without feature selection. The performances of these approaches are compared with various existing techniques with false positive rate (FPR), accuracy and detection rate. Here, the accuracy improves and false positive rate reduces when intrusion is detected with feature selection technique. This paper discusses the performance of the one class SVM classifier in the wireless adhoc network IDS with random forest feature selection and principal component analysis feature selection techniques and one class SVM classifier without feature selection technique in the detection of wormhole attack. And the performance of one class SVM IDS is better in the detection of wormhole attack while it is implemented with principal component analysis feature selection technique.***

Keywords: Wireless adhoc network, Intrusion detection system, Feature selection by Random Forest Method and Principal Component Analysis, One class SVM, Performance metrics of IDS.

I. INTRODUCTION

Wireless adhoc networks utilize the similar components as in wired networks, but the medium of transmission of data is air. Consequently, the information could be hacked easily and therefore the security issues become questionable. Over last years, by the enormous development of system-based forces as well as susceptible data on systems, the system safety has become one of the most significant troubles in the cyber world. Allowing to Bao and Mell (2001), violations are definite as "attempts to compromise the confidentiality, integrity, or availability of a computer or network, or to bypass the security mechanisms of a computer or network." Although there is an existence of a extensive series of safety engineerings for example in order encoding, right of entry manage, as well as intrusion avoidance are helped to defend the system based systems, still there are numerous hidden intrusions or attacks are present.(Computer Crime and Security Survey, 2004).

Intrusion Detection System:

An intrusion detection system (IDS) is a system that monitors network traffic for mistrustful activity and disputes alerts when such activity is revealed. The IDS is classified into two categories. They are misuse detection system which operates on the recognized attacker, stored in the database and anomaly IDS which operates on unrecognized attacker present inside or outside of the network. IDS compare the standard behaviour of the network with current behaviour, to identify the anomaly.

This can be done in two phases, training phase and testing phase. In training phase, modeling of a known normal behaviour of the network is performed whereas, in testing phase, the process of comparing the current behaviour with normal behaviour is performed. Many detection schemes based on statistical methods or soft computing techniques are available for detecting anomaly.

Nowadays, because of the tremendous growth of adhoc network, we are in the need of rapid intrusion detection processors. So we are stepping in to deep machine learning model of IDSs for wireless adhoc network. The application of machine learning models in the IDS leads to high accuracy, high detection rate as well as small FPR. One of the best classifier used in the detection of attacks in wireless adhoc network is one class SVM. It has high accuracy, high detection rate and low processing speed. Nowadays, many research works are going in one class SVM.

In wireless adhoc network, many network layer features are available, in general 41 features. When all these features are considered in the detection of attack, the processing time increases at the cost of accuracy and detection rate. Therefore, the features having

Revised Manuscript Received on December 11, 2019.
* Correspondence Author
T. J. Nagalakshmi1, Asst. Prof., Department of ECE, Saveetha School of Engineering, SIMATS, Chennai, India.
Dr. P. C. Kishore Raja,Professor, Department of ECE, SRM University, Delhi - NCR, Sonepat, India.
S. Pravin Kumar, UG student, Department of ECE, Saveetha School of Engineering, SIMATS, Chennai, India
V. Veeramanikandan, UG student, Department of ECE, Saveetha School of Engineering, SIMATS, Chennai, India

high impact on attacks are considered for the detection of intrusion. This makes the IDS simple and fast.

II. LITERATURE SURVEY IN ONE CLASS SVM AS IDS

Fatemeh and Sajjad (2013), designed a kernel based one class SVM. It is used in IDS which is very fast and precise. It achieves better equilibrium between detection rate as well as FPR [1-3]. This IDS was tested with the simulated data generated by NS2 simulator used with AODV protocol. Here the detection rate as well as FPR improves [4-6]. This IDS was also tested with flooding, neighborhood, black hole, wormhole and rushing attacks [7]. The average detection rate is 95.61% and false alarm rate is 2.14%.

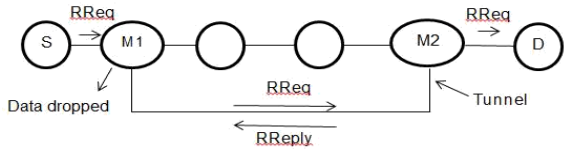
Ming et. al (2015), explained the advantages of an IDS technique which uses one class SVM over two class SVM [8-9]. The one class SVM uses normal attack free dataset as training dataset. After training phase the IDS can able to detect the attack [10-12]. For KDD CUP'99 dataset, the precision is 0.9903, Recall is 0.9161 and F-value is 0.9518 when tested with DoS attacks [13-15].

Guillermo et. al (2013), proposed the one class time adaptive support vector machine to notice the anomalousness's. These IDS having high discovery rate as well as low FPR [16-18].

III. IMPACT OF WORMHOLE ATTACK IN WIRELESS AD HOC NETWORKS

The wormhole attack (WA) is a mostly cruel MANET path attack because it is simple [19] to initiate, capable to initiated in few manners, tough to notice, as well as can induce substantial transaction disturbance (Hu and Johnson, 2003, Ozdemir et. al, 2011, Song an Li, 2005, Yih Chun et.al, 2006, Newlin et al, 2016). A WA can simply be propelled with the enemy lacking having alertness of the system otherwise flexible any real nodes otherwise cryptographic methods [20]. The channel is also a high occurrence connection. It produces the delusion that the two stop points of the way are extremely shut to every other [21-22]. Fig. 1 shows the WA architecture. It may be initiated in the following four ways.

a) Hidden Mode Wormhole Attack
b) Participation Wormhole
c) In-band wormhole link
d) Out of band link.



S – Source, D – Destination, M1, M2 – Malicious nodes, RReq – Receiver Request, RReply – Receiver Reply

Fig. 1. Wormhole attack

The main idea of the present study is to detect worm hole attack. Here the attacker, receives all packets from the senders present in the network. So, there is a notable change in the percentage of the route changed (PRC), percentage of hop count changed (PHC), maximum - changes in sequence number (Max_Seq), maximum changes in hop count (Max_Hop), average difference in sequence number (Diff_Seq), and average difference in hop count (Diff_HC). The delay (Percentage of delay change (PDC)) computed from the previous history of the network is also affected. The attacker node will have high receiver power (Percentage of receive power changed).

Therefore, for the present study, the above said twelve network layer features are considered for the design of intrusion detection system. They are listed in Table 1.

Table- I: Network Layer Features

SYMBOL	NETWORK FEATURES	NAME
F1	Percentage of Route changed	PRC
F2	Percentage of Hop Count changed	PHC
F3	Maximum Changes in Sequence Number	Max_Seq
F4	Maximum Changes in Hop Count	Max_Hop
F5	Average Difference in Sequence Number	Diff_Seq
F6	Average Difference in Hop Count	Diff_HC
F7	Percentage of Delay changed	PDC
F8	Percentage of Receive Power changed	PRPC
F9	Percentage of Drop Ratio changed	PDRC
F10	Percentage of Neighbour count changed	PNCC
F11	Percentage of average difference in neighbour count with all neighbours changed	PDNCC
F12	Percentage of Packet Sent Count changed	PPSC

A. Importance of Feature Selection

Place As the number of features increase, the training speed decreases, model interpretability reduces and thereby it diminishes the overall performance of the intrusion detection system. It is possible to select some features from the data that are most important for the problem. Thus, feature selection is the procedure of choosing a division of applicable characteristics.

Thus the feature selection is also known as variable chosen or else attributes selection and it is different from dimensionality reduction. In feature selection method, it includes and excludes the attributes present in the data without varying them (Al-Jarrah et.al, 2014, Hossein and Hamid, 2016.Mohammad and Masih, 2013, Muthurajkumar, et al, 2013, Naveen, 2013)

Machine learning models are very effective in selecting the features of network layers from the wireless adhoc networks. The models used in the present study are discussed in detail.

B. Importance Random Forest Feature Selection Technique

Random forest method was initially created by Tin Kam Ho. Later the extension was developed by Leo Breiman and Adele Cutler. It builds a collection of decision trees with precise variance. This method easily implements machine learning algorithm even without hyper-parameter tuning. It is furthermore commonly utilized methods, since its as well as reality which capable utilized for both categorization as well as deterioration jobs. Arbitrary forest algorithm can be used for both supervised and unsupervised learning models. Here, greater amount of trees in forest makes the effects more accurate.

For feature selection, the data are pre-processed using standard-scaler function. Then the data fitting was done using “gini” technique. Afterwards, the dataset was splitted into training data set and test data set. 60% of the dataset was used as test set and remaining 40% of the data were used as training set. With the “accuracy score” module, the weightage or score of each feature is calculated. The features with top score are taken for attack detection. Predictions are made on the test data and the same were compared with the known test set targets. The score of the feature represent its impact on the network performance.

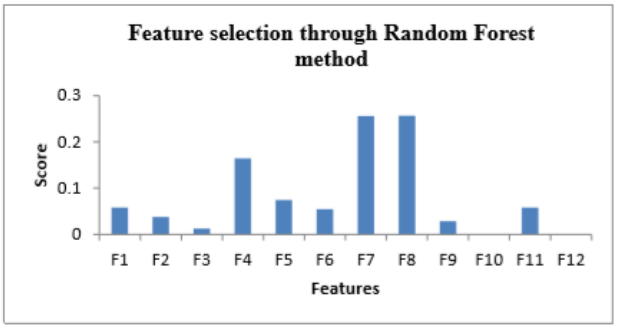


Fig. 2. Feature selection through Random Forest method

Figure 2 exemplifies the scores obtained by different network layer features. The following features with high score were selected for the design of Intrusion detection system.

1) Percentage of Route count changed.
2) Percentage of hop count changed.
3) Percentage of receiver node power changed.
4) Drop ratio.

Subsequently, with the help these four selected features, the wormhole attack is detected using One class SVM.

C. Principal Component Analysis (PCA) Feature Selection Technique

The PCA technique is used to minimize the dimension or number of features of a information set, which consist of several variables that are interrelated to each other. This is done by transforming the variables (scaled data set) to a new set of variables, called principal components. The first PCA the greatest version exist in the real elements. These are eigen vectors of a variance medium as well as thus they are immaterial. When we move from first Principal Component to last Principal Component, the variation present in the Principal Components decreases.

D. Procedure to Implement PCA in IDS

Step 1: Normalization of data: Here, the data set mean is zero.

Step 2: Construction of co-variance matrix:

Var_ [x1] = Cov_ [x1, x1]

Var_ [x2] = Cov_ [x2, x2]

$$\begin{pmatrix} \text{Var\_[x1]} & \text{Cov\_ [x1, x2].} \\ & \end{pmatrix}$$

Covariance matrix =Cov _[x2, x1] Var _[x2]

Step 3: Calculation of Eigen values as well as Eigen vectors of the covariance matrix: The Eigenvalue ג, of a representing Eigen vector v discover by clearing (גI-A) v =0. Here, ג is the Eigen value of matrix A. I is the distinctiveness matrix.

Step 4: Selection of eigen vectors: For n variable data set, n number of eigen vectors andeigen values we will have. To minimize the count of characteristics, we must select the variables from the order of highest eigen values.

Feature vector = {eig1, eig2, eig3,…..}

Step 5: Principal component matrix

New data = Feature vectorT × Scaled dataT

Now the new data set for the analysation is the product of the transposed feature vector and transposed scaled vector.

New data = Matrix with principal components

Feature vector = Matrix with eigen values

Scaled data = Scaled version of original dataset.

The Figure 3 shows the variance of all network layer features in terms of transformed components. Based on the score, the following 4 features are shortlisted.

1. Average difference in sequence number
2. Maximum changes in hop count.
3. Average difference in hop count.
4. Drop ratio

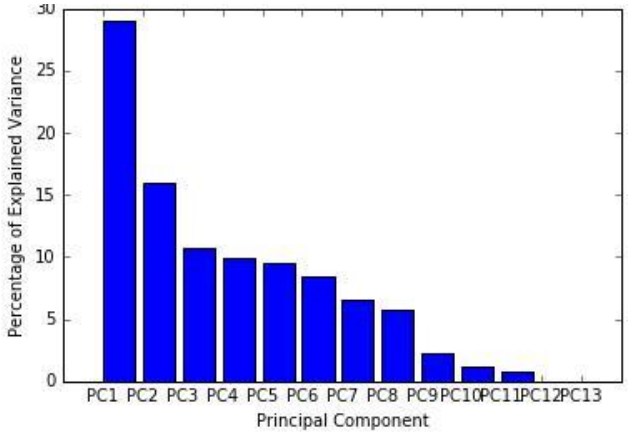


Fig. 3. Wormhole Feature selection by PCA method

E. The Design of IDS

In the IDS, the total data are classified into normal and attacked data. The data are labelled as "normal" and "abnormal" based on its behaviour. It compares the performance of one division SVM IDS with as well as without feature selection. Following procedure is adopted to classify the data. The methodology used in the detection of intrusion here is plotted in the Fig.4

- Import data from CSV file.
- Network layer feature data are normalized.
- Train the one class SVM model with partial data set.
- Test the models with full data set.
  - Normal and abnormal nodes are classified.

F. One Class SVM without Feature Selection in Intrusion Detection

From the simulated Adhoc network, the 12 network layer feature data are collected. Fromm this forty percent of the collected dataset is used as a training dataset and remaining sixty percent is used as a testing dataset. After repeated iterations, RBF Kernel was selected. nu value, gamma value and outlier fraction were respectively 0.95, 0.5 and 0.01. Classification of normal and abnormal nodes based on the behaviour. The performance metrics of the IDS system is computed and compared with the existing systems [23-24].
In this IDS, the following twelve network layer features are used for the detection of anomalies.

a) Percentage of Route changed
b) Percentage of Hop Count changed
c) Maximum Changes in Sequence Number
d) Maximum Changes in Hop Count
e) Average Difference in Sequence Number
f) Average Difference in Hop Count
g) Percentage of Delay changed
h) Percentage of Receive Power changed
i) Percentage of Drop Ratio changed
j) Percentage of Neighbour count changed
k) Percentage of average difference in neighbour count with all neighbors changed
l) Percentage of Packet Sent Count changed

G. One Class SVM with Feature Selection in IDS

From the simulated Adhoc network, the 12 network layer feature data are collected. By using Principle component analysis and Random forest method four features were identified as mentioned in previous section. Forty percent of the collected dataset is used as a training dataset and remaining sixty percent is used as a testing dataset. After repeated iterations, RBF Kernel was selected. nu value, gamma value and outlier fraction were respectively 0.95, 0.5 and 0.01. Normal and abnormal nodes are classified based on the behaviour. The performance metrics of the IDS system is computed and compared with the existing systems.

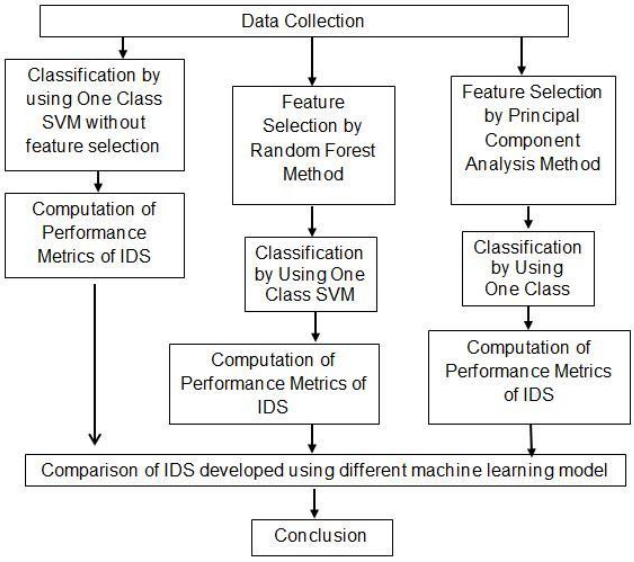


Fig. 4. Methodology used for IDS

IV. SIMULATION ENVIRONMENT

In present work simulation version of Network simulator NS2 version is used. It is most widely used tool for wireless networks. Here the simulation area is 1000 × 1000 meter. There are 100 nodes deployed in random position. All the node are AODV enabled sending the route request for destination node In this scenario node 10 is used source of the worm hole and node 45 is used as worm hole sink to apply tunnel between them.

Table- II: Simulation Parameters

Area of Simulation	(1000 x 1000) m
Node coverage	250 m
Number of Nodes	100
Total Simulation Time	200s
Packet Size	512byts

Initial Energy	100J
Type of MAC	802.11
Attacker	2 to 10
Antenna model	Omni directional
Number of Traffic	1-5
Application	CBR

The NS-2 parameters are listed in Table 1. Constant bit Rate (CBR) application traffic is used. The coverage areas of nodes are configured 250m. Each packet starts from an in discriminate source to indiscriminate destination with a randomly chosen speed. A pause time of 200 seconds was chosen. From this simulated environment the 12 network layer features are collected. And these network layer features are used in the IDS to detect the attacks.

A. Performance Metrics of the IDS

The NS-2 Generally, the performance metrics of IDS in wireless ad hoc network is computed using the following.

a) Detection rate gives the rate of correctly identified intrusion in the wireless adhocnetwork, from the total intrusions are taking place in the network.

$$\text{Detection Rate} = \frac{Correctly\ detected\ intrusions}{Total\ intrusions\ in\ the\ network}$$

b) False positive rate gives the rate of normal activities detected as abnormal activities in the wireless adhoc network. For high detection rate, false alarm rate should be low.

$$\text{False positive rate} = \frac{Normal\ marked\ as\ intrusions}{Total\ normal\ activities} = \frac{FP}{TN+FP}$$

c) Exactness denotes the quantity of accurately separated examples into malevolent as well as benignant.

$$\text{Accuracy} = \frac{(TP+TN)}{(TP+TN+FP+FN)}$$

d) Correctness denotes the charge for the accurately recognized malevolent traffic allowing for all examples anticipated as malevolent.

$$\text{Precision} = \text{Pr} = \frac{TP}{TP+FP}$$

e) Specificity (TNR), denotes the quantity of accurately categorized real benignant traffic in the wireless adhoc network.

$$\text{Specificity (True Negative Rate)} = \text{Sp} = \text{TNR} = \frac{TN}{TN+FP}$$

f) $$\textbf{Sensitivity}\ (\text{True Positive Rate}) = \text{TPR} = \frac{TP}{TP+FN} * 100$$

If TPR is more model is good at classifying the instances.

g) . $$\textbf{F-Value}, \text{F-Score, or F-Measure} = \text{FV} = \frac{2+Pr+DR}{Pr+DR}.$$

It is the combination of Correctness as well as detection rate with a consonant mean.

h) Matthews Correlation Coefficient (MCC)–is an equilibrated compute that denotes the correct categorization despite of the division sizes. It is definite by

$$\text{MCC} = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$$

Where, False Positive (FP) is the amount of regular node treated as attacker node, False Negative (FN) is the amount of attacker node treated as regular node, True Negative (TN) is the number of normal node treated as normal node as well as True Positive (TP) is the number of attacker node treated as attacker node. The performance of the IDS is also analysed by Receiver operating characteristics curve (ROC) as well as Area under curve (AUC).

The ROC curve is a method to signify the act of a classifier. It is initiated from signal recognition theory as well as is utilized in several areas, counting on the estimation of intrusion detection systems. Fundamentally, it is the diagram between TPR and FPR functions. For instance, Fawcett (2006) used ROC curves (Fig. 5) to predict the performance of an intrusion detection system built using machine learning models. The region beneath ROC Curve (AUC), is a number between 0 and 1, which thereby represents the performance of the IDS. When the AUC value is close to zero, the IDS falls under the category of poor classifier. Whereas if the value is close to one then it will be the best classifier. Also, if the AUC value is about 0.5, then it will be a random classifier.

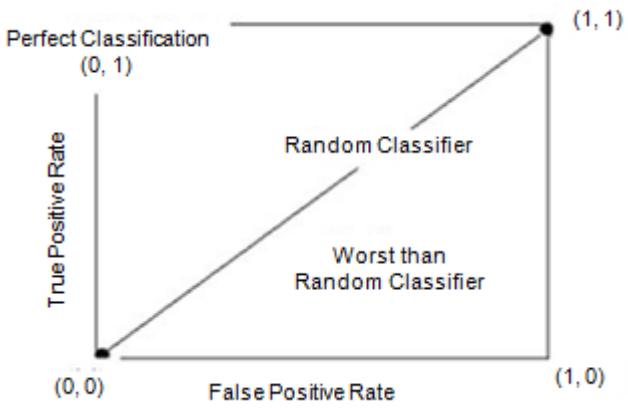


Fig. 5. ROC for Random classifier

B. Performance Metrics of IDS Using One Class SVM without Feature Selection

The performance metrics of one class SVM (without feature selection) classifier used to build the IDS for the wireless adhoc network, is presented in Table 3.

Table- III: Performance metrics of One class SVM without feature selection IDS

Ids Parameter	One Class Svm (Without Feature Selection)
Detection Rate	100%

Accuracy	96.67%

False Positive Rate	3.5%
Precision	62.5%
Specificity (Tnr)	96.47%
Sensitivity (Tpr)	100%
F-Value	0.7692
Mcc	0.7764

For the one class SVM intrusion detection systems with twelve network layer features, the detection rate and accuracy were respectively 100% and 96.67%. The false positive rate is as low as 3.5%. Lower value indicates that the performance of the IDS good. But the precision of the IDS is 62.5% since it considers normal node as attacker node. The specificity and sensitivity were found to be 96.47% and 100%. respectively. The F-value or F-factor is 0.7692 and Mathews coefficient factor is 0.7764. The Fig. 6 gives the plot for the performance metrics of one class SVM classifier. These all values infer that, the IDS built using one class SVM without feature selection can detect almost all attackers present in the network. The receiver operating characteristics curve of the intrusion detection system built using one class SVM classifier without feature selection, is illustrated in Fig. 7. The values are very close to the ordinate (0,1), which thereby means that the classifier falls under the good category. The Fig. 8 sketches the area under the curve (AUC). For an ideal IDS, the AUC should be equal to one. The AUC of the IDS designed is 0.9831125. With all these values it can be concluded that the IDS designed, is highly efficient.

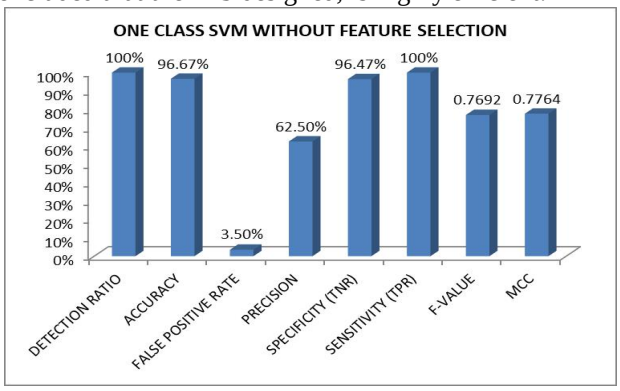


Fig. 6. Anomaly detection in One class SVM without feature selection

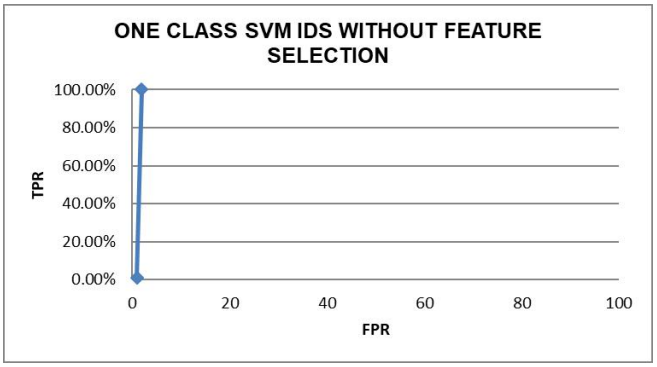


Fig. 7. ROC of one class SVM in attack detection

C. Performance Metrics of IDS Using One Class SVM with Feature Selection

For the Twelve network layer features were reduced to four using the machine learning models, random forest method and principal component analysis techniques.

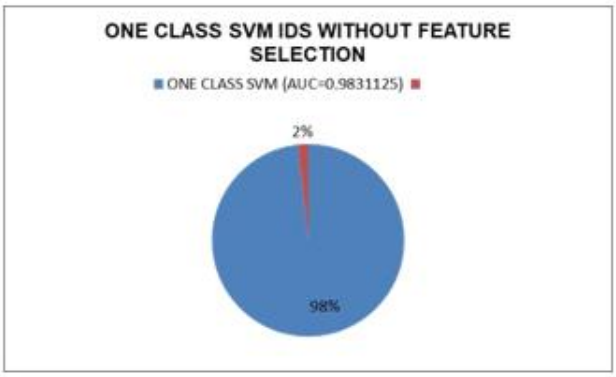


Fig. 8. AUC of one class SVM IDS without feature selection

D. Performance Metrics of IDS using One Class SVM with Random Forest Feature Selection Technique

The performance metrics of the IDS built using one class SVM with Random forest feature selection technique is given in Table 4. As it could seen, the accuracy of the system improved to 97.7%, FPR reduced to 2.35%, Precision increased to 71.42% and F-value improved to 0.8333, which is better than the metrics given by one class SVM IDS without feature selection.

Table- IV: Performance metrics of the RF + One class SVM IDS

IDS PARAMETER	RF + ONE CLASS SVM IDS
DETECTION RATE	100%
ACCURACY	97.7%
FALSE POSITIVE RATE	2.35%
PRECISION	71.42%

SPECIFICITY (TNR)	97.64%
SENSITIVITY (TPR)	100%
F-VALUE	83.33%
MCC	83.51%

Figure 9 shows the graphical representation of the performance metrics of the IDS. Figure 10 illustrates the ROC plot of RF (rain forest) + One class SVM based IDS. This is plotted between TPR and FPR.

Here, the curve falls under the good classifier region. Figure 11 depicts the area under curve of RF + One class SVM IDS. The value AUC is 0.99988, very close to 1, which thereby means that the intrusion detection system is nearly a perfect classifier. From the ROC and AUC of the IDS this is infer that this new present work RF + One class SVM IDS is a good classifier. Here, this system makes IDS very simple with four network layer features. Therefore, the complexity of the system is reduced and thereby it achieves 100% detection ratio, Specificity 97.64% and MCC value 83.51%.

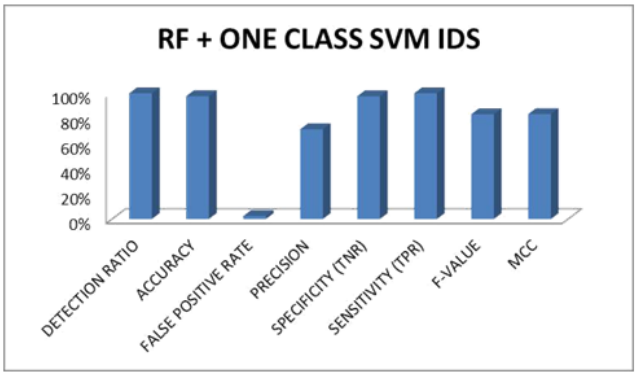


Fig. 9. IDS metrics of RF+One Class SVM

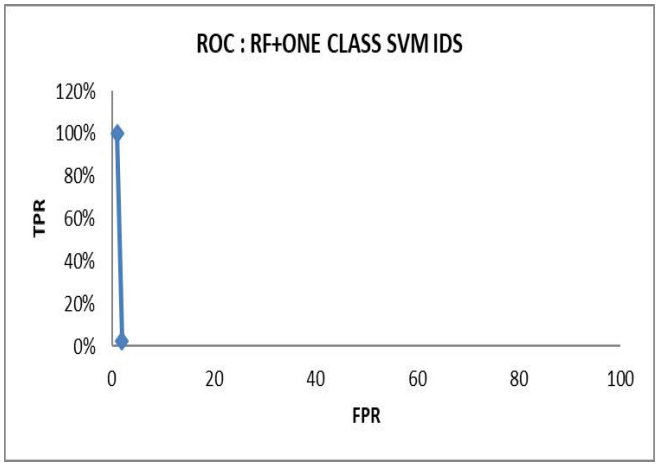


Fig. 10. ROC of RF+ONE CLASS SVM IDS

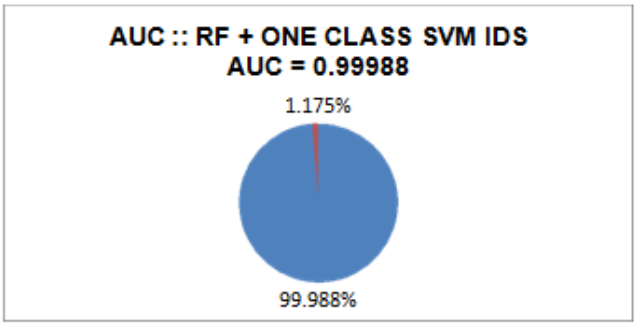


Fig. 11. AUC of RF + One class SVM IDS

E. Performance Metrics of IDS using One Class SVM with Principal Component Analysis Feature Selection Technique

Using the Principal component analysis method, four network layer features are selected from the 12 network layer features. These 4 features are used to detect the intrusion in the adhoc network. Here, the accuracy improved to 98.8%, FPR reduced to 1.17% and precision improved to 83.3% when compared to the one class SVM without feature selection IDS. The performance metrics of the new IDS is given in Table 5. The graphical representation of the performance metrics is represented in Fig. 12. Figure 13 illustrates the ROC of the new present system. Here the coordinates are near to (1,1). Therefore, it falls under the category of good classifier. Figure 14 represents the AUC of this system, where the value is 0.99411, very close to 1. Thus, this is a good classifier.

Table- V: Performance metrics of the PCA + One class SVM IDS

IDS PARAMETER	PCA + ONE CLASS SVM
DETECTION RATE	100%
ACCURACY	98.8%
FALSE POSITIVE RATE	1.17%
PRECISION	83.3 %
SPECIFICITY (TNR)	98.8 %
SENSITIVITY (TPR)	100%
F-VALUE	90.89%
MCC	90.74%

Here, the detection ratio is 100%, the specificity improved to 98.8%, the sensitivity is 100% and MCC value is 90.74%. From the above metrics it can be inferred that, one class SVM classifier with PCA feature selection is a good IDS.

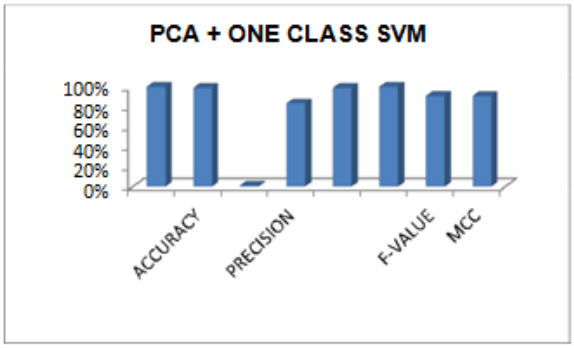


Fig. 12. Performance metrics of PCA + One Class SVM IDS

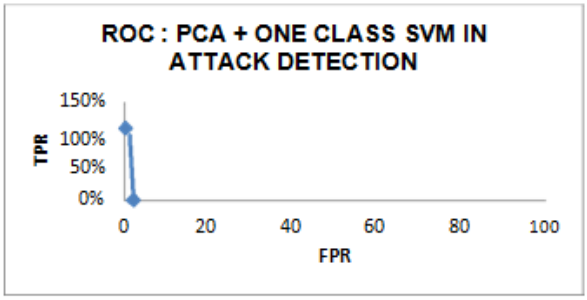


Fig. 13. ROC of a PCA+One Class SVM in attack detection

F. Comparison of IDS using One Class SVM with and without Feature Selection

The Table 6 gives the details of the comparison of performance metrics of the IDS using one class SVM with and without feature selection. The Fig 15 shows the graphical representation of the above performance metrics. It is inferred that; the performance efficiency improves with feature selection. With feature selection, the exactness of the false detection improves, the false positive rate reduces randomly, precision increases and the specificity increase.

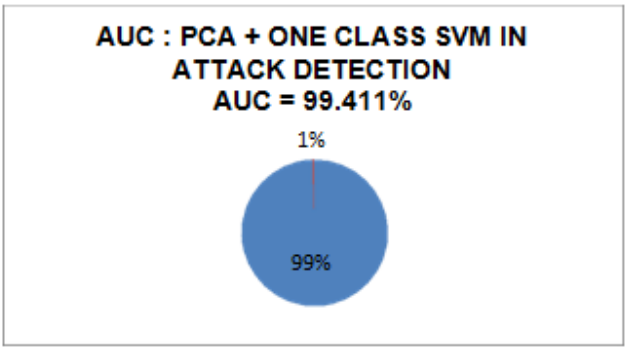


Fig. 14. AUC of PCA + One class SVM IDS in attack detection

Through this analysis it is demonstrated that, the IDS designed using the features selected through PCA method is having very low FPR, high precision rate, high specificity, high F-value and high MCC factor, when compared with the IDS designed using the features selected using random forest method.

Table- VI: Comparison of One Class SVM with and without feature selection

IDS PARAMETER	ONE CLASS SVM (Without feature selection)	ONE CLASS SVM (With feature selection)	
		RF + ONE CLASS SVM IDS	PCA + ONE CLASS SVM IDS
DETECTION RATE	100%	100%	100%
ACCURACY	96.67%	97.7%	98.8%
FALSE POSITIVE RATE	3.5%	2.35%	1.17%
PRECISION	62.5%	71.42%	83.3 %
SPECIFICITY (TNR)	96.47%	97.64%	98.8 %
SENSITIVITY (TPR)	100%	100%	100%
F-VALUE	0.7692	0.8333	0.9089
MCC	0.7764	0.8351	0.9074

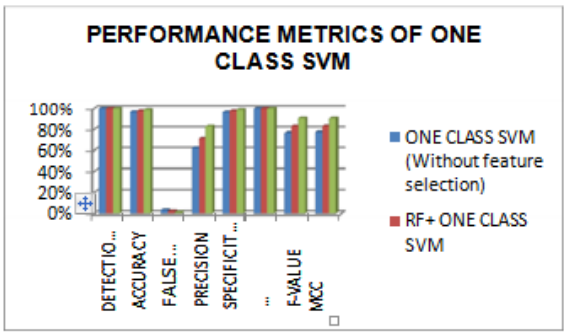


Fig. 15. AUC Comparison of performance metrics of One class SVM with and without feature selection

G. Existing IDS using one class SVM

A similar IDS was designed by Ming zhang et.al (2015) to detect DoS attack and Probe attack, using One Class SVM. They compared the performance metrics with C-SVM and PNN IDS techniques. The detection rate was 100% for One class SVM in the detection of DoS attack and Probe attack. In C-SVM, the detection rate was 99.58% and 86.98% in the detection of DoS attack and Probe attack respectively. By using PNN IDS, the detection rate was 99.79% and 98.73% in in the detection of DoS attack and Probe attack respectively.

Whereas, Leandros et.al (2014) used one class SVM intrusion detection technique with RBF kernel, nu value as 0.07 and gamma value as 0.01. They reported an accuracy of 98.87%. Patric Nader et. al (2015) proposed a Mahalanobis distance based one class SVM IDS in SCADA. For the intrusions of NMRI, CMRI and DoS, they reported an accuracy of 99.28%, 99.83% and 95.56% respectively. The FPR for the intrusions were as low as 1%. Fatemeh barani et.al (2013), proposed an IDS using One class SVM in the detection of flooding attack, blackhole attack, wormhole attack, rushing attacks. They reported an average detection ratio of 95.61% and average FPR 2.14%. In the detection of black hole attack the detection rate as well as FPR was 95.34% and 1.88% respectively. In the detection of worm hole attack the detection rate as well as FPR was 95.15% and 2.43 % respectively.

V. RESULT AND DISCUSSION

As per our surveyed techniques we can detect the intruder. In this paper we can get an proper security and beacon to the system thus we can get an phenomenal accuracy. The intruders can be detected by the comparative study we can get a mean value for the above study. So, in actual time we can get internal intruders and malfunctions coming in large scale can be diminished. This can be used by several MNC's which they can prevent enormous protective information.

VI. CONCLUSION

A similar An IDS was built using one class SVM having 12 network layer features. The accuracy and detection rate of these IDS was 96.67% and 100% respectively. Whereas, the FPR was 3.5%. Although the accuracy and detection ratio were good, FPR could be improved.

Two Intrusion detection system were designed using one class SVM with network layer feature selection (RF and PCA), to improve the performance. Twelve network layer features were minimized to four using random forest (RF) and principal component analysis (PCA) methods. The accuracy and detection rate of the IDS built using one class SVM and four network layer features (selected using random forest method) were 97.7% and 100% respectively. Whereas, the FPR was 2.35%. Similarly, the accuracy and detection rate of the IDS built using one class SVM and four network layer features (selected using principal component analysis method) were 98.8% and 100% respectively. Whereas, the FPR was 1.17%. It was clearly observed from the performance metrics that one class SVM with principal component analysis method for feature selection was the best performer compared to the other two IDS designed using one class SVM.

REFERENCES

1. CSI/FBI Computer Crime and Security Survey, (2004), Computer Security Inst., San Francisco, CA. [Online]. Available: http://www.issa-sac.org/docs/FBI2004.pdf.
2. Al-Jarrah, A. Siddiqui, M. Elsalamouny, P.D. Yoo, S. Muhaidat, K. Kim, " Machine-Learning-Based Feature Selection Techniques for Large-Scale Network Intrusion Detection, Computer society", *International Conference on Distributed Computing Systems Workshops*, *IEEE Xplore*: 01, INSPEC Accession Number: 14563151, Pg :177-180 (2014).
3. Paulo angelo alves resende and and ré costa drummond, ,"A Survey of Random Forest Based Methods for Intrusion Detection Systems, ACM Computing Surveys", Vol. 51, No. 3, Article 48 (2018).
4. Bao Cui-Mei, "Intrusion Detection Based on One-class SVM andSNMP MIB data", *IEEE Xplore*, *International Conference on Information Assurance and Security*, Pg: 245-249 (2009).
5. Fatemeh Barani, Sajjad Gerami, , ManetSVM: "Dynamic Anomaly Detection using Oneclass Support Vector Machine in MANETs", *IEEE*, INSPEC Accession Number: 14162120 (2013).
6. Ming Zhang, Boyi Xu, Jie Gong, , "An Anomaly Detection Model based on One-class SVM to Detect Network Intrusions", *IEEE International Conference on Mobile Ad-hoc and Sensor Networks*, INSPEC Accession Number: 15822091(2015).
7. Hu, Y. C., Perrig, A., & Johnson, D. B., Packet leashes:" A defense against wormhole attacks in wireless networks", In IEEE computer and communications, Vol. 3, pg: 1976– 1986 (2003).
8. Hossein Gharaee, Hamid Hosseinvand, , "A New Feature Selection IDS based on Genetic Algorithm and SVM", In *IEEE International Symposium on Telecommunications*, Pg: 139-144. (2016).
9. Leandros A. Maglaras, Jianmin Jiang," A real time OCSVM Intrusion Detection module with low overhead for SCADA systems", *International Journal of Advanced Research in Artificial Intelligence* , Vol 3, N0 10, Pg: 45-53. (2014).
10. Fatemeh Barani, Sajjad Gerami, ManetSVM: "Dynamic Anomaly Detection using Oneclass Support Vector Machine in MANETs", IEEE, INSPEC Accession Number: 14162120. (2013).
11. Madria, S. & Yin, J, SeRWA:" A secure routing protocol against wormhole attacks in sensor networks, Ad Hoc Networks", 7(6), Pg: 1051–1063. (2009).
12. Ming Zhang, Boyi Xu, Jie Gong, "An Anomaly Detection Model based on One-class SVM to Detect Network Intrusions", *IEEE International Conference on Mobile Ad-hoc and Sensor Networks*, INSPEC Accession Number: 15822091(2015).
13. Patric Nader, Paul Honeine and Pierre Beauseroy, " Online One-class Classification for Intrusion Detection Based on the Mahalanobis Distance, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning", Pg: 22-24. (2015).
14. Mohammad K. Houri Zarch, Masih Abedini, " An unsupervised anomaly detection engine with an efficient feature set for AODV", *International ISC Conference on Information Security and Cryptology*, DOI:10.1109/ISCISC.2013.6767334 (2013).
15. Muthurajkumar, SannasiGanapathy, KanagasabaiKulothungan, MuthusamyVijayalakshmi, " Intelligent feature selection and classification techniques for intrusion detection in networks": *a survey*, *EURASIP Journal on WirelessCommunications and Networking* – Springer, Pg: 1-16. (2013).
16. Song, N., Qian, L., & Li, X., , "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach". *In IEEE international parallel and distributed processing symposium*, Pg: 8-18. (2005).
17. Nauman Shahid • Ijaz Haider Naqvi • Saad Bin Qaisar ," One-class support vector machines: analysis of outlier detection for wireless sensor networks in harsh environments, Artificial Intelligence Review", DOI:10.1007/s10462-013-9395-x (2013).
18. NewlinRajkumar .M ,. Shiny M. U, Amsa Rani R," Detection of wormhole attack using cooperative bait detection scheme", WSN, Vol. 49 Issue 2, Pg: 78-86. (2016).
19. Neveen I. Ghali, ,"Feature Selection for Effective Anomaly-Based Intrusion Detection", *International Journal of Computer Science and Network Security*, VOL.9 No.3. (2009)
20. Özdemir, M. Meghdadi, and Ý. Güler, , "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", *Journal IETE technical review*, Vol. 28, Issue 2, Pg: 89-102. (2011).
21. Patric Nader, Paul Honeine and Pierre Beauseroy, , "Online One-class Classification for Intrusion Detection Based on the Mahalanobis Distance", European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, Pg: 22-24. (2015).
22. Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Wormhole Attacks in Wireless Networks", *IEEE Journal on selected areas in communications*, Vol. 24, No. 2, Pg: 370-380.
23. S. Mohankumar, "Analysis of different wavelets for brain image classification using support vector machine", *International Journal of Advances in Signal and Image Sciences*, Vol. 2, No. 1, pp. 1-4.
24. S. Murugan, and C. Srinivasan, "Underwater Object Recognition Using KNN Classifier", *International Journal of MC Square Scientific Research*, Vol. 9, No. 3, 2017, pp. 48-52.

AUTHORS PROFILE

Ms.T.J.Nagalakshmi, working as a Asst. Professor in Department of Electronics and Communication Engineering at Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu State, India. She has 11 years of teaching experiences in Engineering Colleges. She has published 30 papers in International journals and has presented in 5 International Conferences at various Engineering Colleges. Her areas of specialization are VLSI, Artificial Intelligence, Networks and Compilers.

Dr. P C Kishore Raja working as a Professor in Department of ECE in SRM University, Delhi - NCR, Sonepat, India. He has published many indexed papers and completed many sponsored projects from reputed institutions. His area of specialization is Wireless Communication, Cognitive radio network.

.PravinKumar, is a UG student doing Electronics and communication Engineering programme in Saveetha School of Engineering, SIMATS, Chennai, India. He has very good knowledge in Python and he developed many mathematical models.

Veeramanikandan, is a UG student doing Electronics and communication Engineering programme in Saveetha School of Engineering, SIMATS, Chennai, India. His area of interest is wireless communication.