Int. J. of Network Security, Vol. 6, April 2014

Anomaly Detection System for Routing Attacks in Mobile Ad Hoc Networks

Konagala Pavani[1], Dr.Avula Damodaram[2]
[1] Vaagdevi College of Engineering,CSE, Warangal, India
Email: bandaripavani@gmail.com
[2] Jawaharlal Nehru Technological University,CSE,Hyderabad, India
Email: damodarama@gmail.com

Abstract-- **A mobile ad hoc network (MANET) is a dynamic network without any fixed infrastructure. MANETs are more susceptible to the security attacks because of the properties such as node mobility, lack of centralized management and limited band width. To tackle these security issues secure and robust routing protocols are been proposed. Also many security schemes such as encryption, authentication and firewalls have been proposed. However we cannot completely eliminate such risks, there is a strong need for intrusion detection system. So, in this paper we propose machine learning techniques for detecting normal and attacked behaviour of the system. The presence investigation effectively applied machine learning techniques such as Decision Tree (C-4.5), Multi Layer Perceptron (MLP), K-Nearest Neighbourhood (KNN) and Support Vector Machine (SVM). These methods were tested for black hole and gray hole attacks. We have implemented these attacks using NS2 simulator. The experimental results show that MLP has detected the attacks with more accuracy and less error rate than the other methods. This paper also presents a graphical representation of the results.**

Index Terms**—Intrusion Detection System, Multi Layer Perceptron, K-Nearest Neighbourhood, Support Vector Machine, Black hole attack, gray hole attack.**

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of mobile nodes which communicate via wireless radio links. The nodes in MANET are communicated without any central base station. MANET's network topology is dynamic because at any instance a node may leave the network and may re-join the network. As MANETs provide reliable routing services without any fixed infrastructure, they are being used in various applications such as military & civilian areas, rescue operations, personal area, and campus. However flexibility and adaptability of MANETs made them more susceptible to the attacks. Because of node mobility, it is very difficult to maintain security in MANETs than wired networks. Therefore, we need a strong security system. MANETs doesn't have the facility of installing firewalls at routers and switches as in wired networks. So, to enhance the security level of MANETs Intrusion detection systems (IDS) can be used. IDS is a software system which monitors the intrusions [1] occurring in a computer system or in a network. An Intrusion Detection System is used to analyze malicious behaviours in the network and generates reports. It also tries to prevent intrusions that comprise system security.

Misuse and Anomaly detection are two general approaches to intrusion detection [2]. Misuse detection or Signature based detection generates an alarm when a known attack signature is matched. Anomaly detection identifies activities that deviate from the normal behaviour of the monitored system and thus has the potential to detect an intrusion. In fact, anomaly detection can be regarded as a classification problem which classifies normal or attacked behaviour.

The three existing approaches for intrusion detection [3] [4] in MANETs include Distributed Anomaly Detection, Simple Network Management Protocol (SNMP) based Local Intrusion detection system (LIDS) and Watchdog Approach. This paper defines anomaly detection method for detecting network layer attacks namely Black hole and Gray hole attacks in MANET using LIDS. Ad hoc On Demand Vector (AODV) [5] routing protocol has been adopted to monitor these security vulnerabilities.

The rest of this paper is organized as follows. In next section we review some related work. In section III we described proposed system. Section IV describes the type of attacks. Section V describes NS2 simulation. Section VI & VII explain data extraction and feature selection process. Section VIII describes IDS techniques. Training with TANAGRA is explained in Section IX. The results are shown in section X. Finally, we summarize our work in Section XI.

II. RELATED WORK

In recent years, researchers have proposed different methods to improve security level of MANET. Y. Zhang,et al.[2], proposed an architecture for a distributed and cooperative intrusion detection system based on statistical anomaly detection techniques. Rizivi et al. used watchdog and pathrater approaches to show the effects of routing misbehaviour in DSR protocol [6]. Loo et al [7] used a clustering algorithm for detecting routing attacks in sensor networks. K.S.Sujatha et al [8] proposed Design of Genetic Algorithm based IDS for MANETs. Huang [9] proposed an anomaly detection scheme that gives solution for routing anomalies. Sohail Abbas et al [10] have proposed Light weight Sybil attack detection in MANETs. Rakesh Shrestha et al [11] proposed a novel technique for cross layer intrusion detection system for MANETs. Zahra Moradi et al [12] proposed a neural network technique for detecting Denial of Service attacks. Katharine Chang et al [13] proposed Application layer intrusion detection system for MANETs.

III. PROPOSED SYSTEM

The proposed system is shown in Figure 1 which represents the schematic architecture of intrusion detection in MANETs.

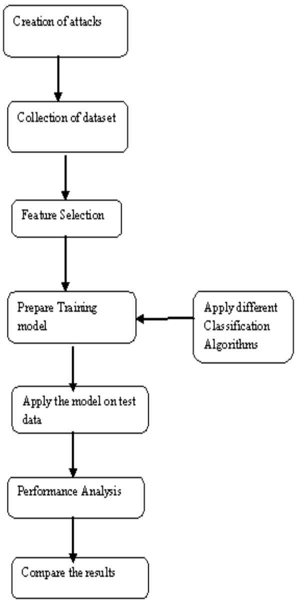

Figure 1.Architecture of Proposed System

.

The aim of the proposed approach is to classify best classification model to tackle black hole & gray hole attacks in MANETs which includes creation of intrusions in the network, collection of audit data, training, performance analysis and comparison of results. This proposed intrusion detection in MANET involves the creation of intrusions in the network i.e. design of black hole and gray hole nodes with various node combinations like 20, 21, 22….etc. and collection of audit data. Then the sample set consisting of instances with attack and normal behaviour was constructed by extracting the features from this audit data. However the training is performed using various classification algorithms which are discussed in next subsequent sections. Then in the next step, training is performed using training data (extracted from sample set) which contain both normal and attacked data. Subsequently testing is carried to test extent of data set (unseen data) matching with the model. Finally the performance of these models is analyzed to asses' best model using different metrics.

Anomaly detection is considered as a classification problem in which normal and attacked (black & gray hole) behaviours are classified. Multilayer Perceptron, Decision Tree, K-Nearest Neighbourhood, Support Vector Machine are the most popular techniques for classification. Proposed approach is to design best classification model to tackle black hole and gray hole attacks in MANETs. The proposed architecture is discussed in detail in forth coming sections.

IV.DEFINITION OF ATTACKS

The proposed method implements following attacks.

A. Black Hole attack

Black hole attack is an active attack type [14] which occurs in network layer. It is also called as packet drop attack as it drops messages. In this type of attack, black hole node waits for neighbouring nodes to send RREQ messages. When the black hole node receives a RREQ message from the neighbouring nodes, without checking its routing table, immediately sends a false RREP message to the requesting node by giving route to destination over itself. The black hole node displays high sequence number to settle in the routing table of the victim node and sends RREP to requesting node, before other nodes send a true one. Therefore requesting node assumes that route discovery process is completed and ignores other RREP messages. Then the source node routes the packets to destination through this compromised node. In the same manner the black hole node attacks all RREQ messages and takes over all routes. Therefore all packets are sent to destination over black hole node. The black hole node without forwarding the packets to the destination discards them. In this way a black hole node can affects the whole network. This type of attack reduces the packet delivery ratio of the network.

B. Gray Hole Attack

Gray hole attack [14] is also an active attack type which leads to dropping of messages. Gray hole node first behaves normally and agrees to forward the message but fails to do so. In this attack type the gray hole node, after receiving RREQ message from source node, uni cast the RREP message back to the source node. So the source node starts communicating through this path. But later the gray hole node drops the packets. This process goes on until gray hole node succeeds its aim (e.g. network resource consumption, battery consumption).

V. NS2 SIMULATION OF ATTACKS

We conducted our experiments using Network Simulator version 2.29. NS-2[15] [16] is a simulation project developed by the University of California Berkley and it is a part of software of VINT [17] project which is supported by DARPA since 1995. It is one of the most widely used network simulators for wired and wireless networks. The simulated network consists of nodes which are placed randomly within 1000m*1000m area. Each node moves around the network according to random way point model. The duration of each experiment was 500s. The MAC layer protocol used in the simulation is IEEE 802.11. The simulation was repeated with different number of nodes (from 20 through 100). During each run the trace files were collected and finally, the trace analysis was done to measure the performance. The simulation parameters selected for implementing the attacks are tabulated in table 1. The network is designed with new routing protocol which contains the attacking nodes.

TABLE 1. SIMULATION PARAMETERS

Parameter	Definition
Protocol	AODV
Mac Layer	IEEE 802.11
Simulation time	500 s
Connection time	450 s
Node Placement	Random
Simulation Area	1000*1000
Size of data packet	512
Traffic Sources	CBR
Number of nodes	20 to100
Version NS2	NS-2.29(under windows, cygwin)
Data rate	10 kbits

VI. DATA EXTRACTION

After designing the network with attacking nodes, audit data is collected. This data is collected by analyzing the log files generated by NS2 simulation. This data consists of network information such as routing updates and attack information which is collected from physical, network and MAC layers.

VII. FEATURE SELECTION

There are different kinds of features which affect the network in presence of attacks. The features we have selected from audit records to design intrusion detection are as follows

Node-node number
RREQ-Number of RREQ sent
RREP- Number of RREP sent
Variance- Variance of the delay
Sent-Number of packets sent
Received-Number of packets received by receiver
Delay-Delay in sending the packet
Drop- Number of packets dropped during transmission
Packet Delivery Ratio-Number of packets delivered in a second.

VIII. INTRUSION DETECTIOON SYSTEM

Intrusion Detection System analyses the audit data and tries to find the intrusions .It works as the defensive mechanism in securing the system. Data mining is a new approach for intrusion detection for MANETs. Classification is one of the data mining algorithms, which have been investigated as a useful technique for IDS. In this paper we have applied MLP, Decision Tree, KNN and SVM. We have used TANAGRA software to model the network. The dataset we have collected from the experiments consist about 200 instances or examples.

A. Multi Layer Perceptron

Artificial Neural Network (ANN) [18] is one of the artificial intelligence methods which are inspired by human nervous system. It consists of a large number of highly interconnected processing elements called as neurons. Neurons work with each other to solve specific problem. ANNs are utilized to detect the node under attacks. It is designed with summing element followed by an activation function. In this, output of each neuron is given as input to the neurons in the next layer. A multi layer perceptron (MLP) is a feed forward ANN model which maps set of input data to a set of output data. It consists of multilayer of nodes, with each layer fully connected to other node.MLP can classify data which is not linearly separable.MLP uses a supervised learning technique called as back propagation algorithm for training the network. Architecture of MLP consists of 3 types of layers. They are an input layer, one or more hidden layers, and an output layer. Each node in one layer connects with certain weight to every node in the next layer. The network is trained by changing connection weights.MLP is trained by applying the audit data as input. Figure 2 represents the flowchart to train MLP..

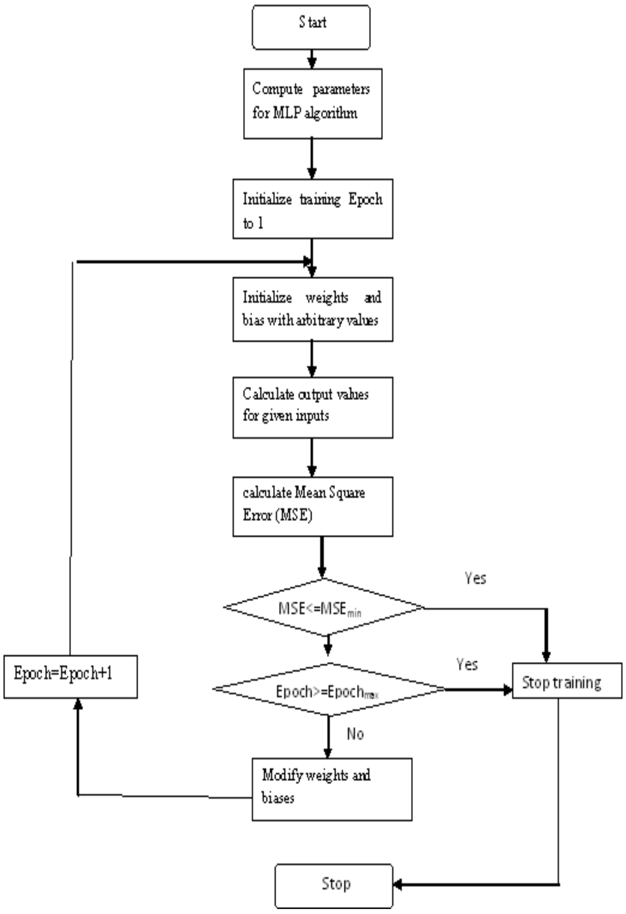
Start
Compute parameters for MLP algorithm
Initialize training Epoch to 1
Initialize weights and bias with arbitrary values
Calculate output values for given inputs
calculate Mean Square Error (MSE)
MSE<=MSE$_{min}$
Yes
Epoch>=Epoch$_{max}$
Yes
Stop training
No
Epoch=Epoch+1
Modify weights and biases
Stop

Figure 2. Flowchart to train Multi Layer Perceptron

The designed network model consists of 9 input neurons, 3 hidden layer neurons and one output layer. The architecture used in our experiments is shown in Figure 3.

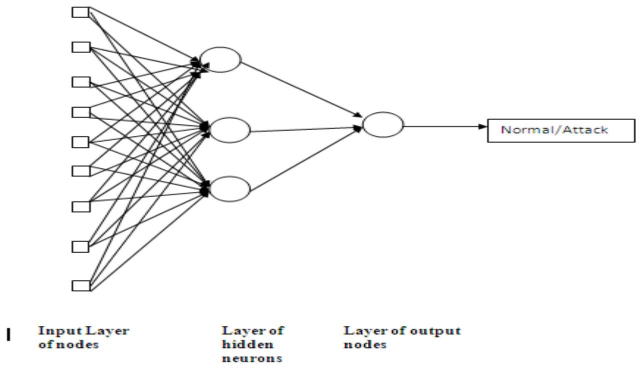

Figure 3.Architecture of MLP

B. Decision Tree

Decision tree is one of the classification algorithms in data mining used for intrusion detection. Decision tree is a simple if then else rules. These rules categorize data according to the attributes. It constructs a model from the pre classified data set. Each record in the dataset represents set of attributes and a class label (attack/normal). Using the values of these attributes decision tree builds a model. This model is used to classify future data for which class label is unknown. A decision tree consists of nodes, leaves and edges. In our experiments we have used C 4.5 which is one of the popular learning algorithms proposed by Quinlan in 1993[19].

C. K-Nearest Neighbourhood

K- Nearest neighbour algorithm [20] [21] is the simplest of all machine learning algorithms. It is used to separate the data points into several classes and predicts the class of new sample point. The sample is classified by a majority vote of its neighbours. If k=1, then the sample is assigned to the class of that single neighbour. The learning process of KNN is simpler than other models. In learning step it simply loads the sample set into the database. To test the new sample(S) it follows the following steps.

- Calculate distances of all training samples to test sample S
- Find the k instances in training sample set which are closest to S
- These k instances then vote to determine the class of S

The distances between training samples and test sample can be calculated by using Hamming distances, Euclidean distance, Manhattan distance, Local distance functions, global distance functions and weights etc. In our experiments we have used Euclidean distance as distance function. After finding distance, neighbours vote in order to predict the class of sample S. This voting can be done by using Majority voting or inverse distance-weighted voting methods. In our experiments we have used majority voting method**.** Figure 4 shows the example for KNN classification. In this example the test sample should be classified either to the class of black triangles or to the class of green squares. If k=3 it is assigned to the class triangles as there are two triangles and one square inside the circle.

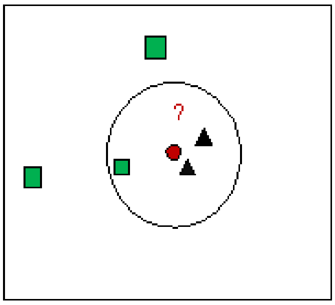

Figure 4. Example for KNN classification

D. *Support Vector Machine*

A Support Vector Machine (C-SVC) is one of the most successful classification algorithms in neural networks. It is a type of feed forward network introduced by Vapnik [22] [23] which is used for pattern classification and non–linear regression. SVM constructs a hyper plane as the decision surface in such a way that the margin of separation between positive and negative examples is maximized. The property of SVM is that it is an approximate implementation to the structure risk minimization (SRM) principle in statistical learning theory. SVMs classify data by determining a set of support vectors, which are members of the set of training inputs that outline a hyper plane in the feature space.

IX. RESULTS AND DISCUSSION

The performance of classification algorithms was evaluated by series of experiments under varying conditions by random selection of 65% data for training and 35% data for testing. The training phase was repeated for 100 epochs and most widely used evaluation parameters for testing of performance of classifier were error rate, accuracy, sensitivity, specificity and ROC Curves.

A. *Error Rate*

The instance's class which is predicted incorrectly is called as an error. The error rate is the proportion of the errors made over the whole set of instances which measures the overall performance of classifier. In our experiments we have calculated training and testing error rates for both types of attacks. The error rates are been shown as graph in Figure 5 & Figure 6. The training and testing error rates for gray hole and black hole attack revealed higher training & testing error rates for gray hole attack when compared with black hole attack. However the lowest training & testing error rates were observed for C 4.5 among all the methods studied for both types of attacks.

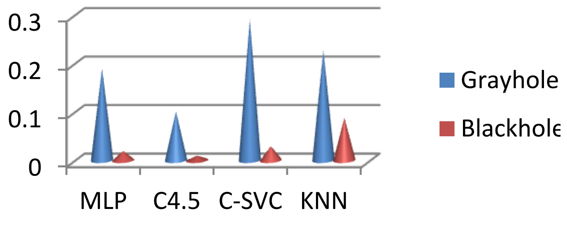

Figure 5.Training Error

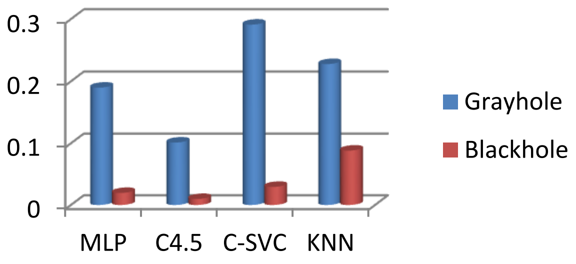

Figure 6.Testing Error

B. *Accuracy*

Accuracy is the proportion of correctly classified instances over the whole set of instances.
Technically Accuracy can be defined as shown in "1".

$$\text{Accuracy}= \frac{\text{No of correctly classified examples}}{\text{Total no of examples}}*100. \qquad (1)$$

Figure 7 & Figure 8 represents the graphical representation of training and testing accuracies for black and gray hole attacks. The classifier C 4.5 has achieved training accuracy of 99% for black hole attack and 90% for gray hole attack indicating highest training accuracy for black hole attack compared to gray hole attack. Similarly MLP and SVM classifiers have achieved training accuracy measures 99% and 97% for black hole attack, 82% and 71% for gray hole attack respectively. Finally KNN classifier has achieved the training accuracy of 87% for black hole attack and 56% for gray hole attack indicating lowest measures among all other methods applied. The classifier C 4.5 has achieved testing accuracy of 99 % for black hole attack61%-99% for both types of attacks, while MLP and SVM classifier have achieved accuracy measures between 70%-99% and 61%-95% respectively. Finally, KNN classifier has achieved the lowest measures for both types of attacks ranging between 56%-87%.

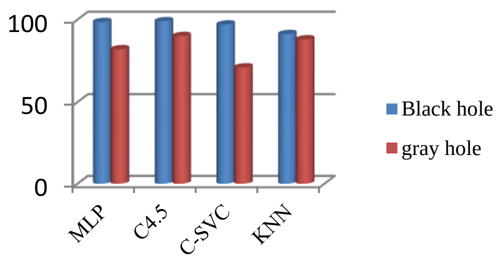

Figure 7.Training Accuracy

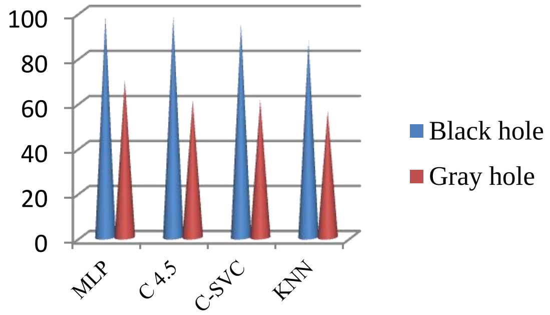

Figure 8.Testing Accuracy

C. *Confusion Matrix*

A binary classification model classifies each instance or examples into one of 2 classes, true (attack) or false (normal).This gives four possible classifications for each instance. They are True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN).The same result is shown as a confusion matrix. Based on this matrix following metrics are also used to evaluate the performance of models.

Sensitivity

Sensitivity is also known as True Positive Rate (TPR) which is defined in “2”. If TPR or sensitivity is more, the model is good at classifying the instances.

$$\text{TPR (Sensitivity)} = \frac{TP}{(TP+FN)} * 100 \qquad (2)$$

Specificity

Specificity is also known as True Negative Rate (TNR) which is defined in “3”.

$$\text{TNR (Specificity)} = \frac{TN}{(TN+FP)} * 100 \qquad (3)$$

False Positive Rate (FPR)

FPR can be calculated as shown in the equation “4”.

$$\text{FPR}=\frac{FP}{(TN+FP)} *100. \qquad (4)$$

The above metrics are calculated and tabulated in the Table 2 & 3.

TABLE II. COMPARISON OF METRICS FOR BLACK HOLE

Black hole/Testing	Sensitivity	Specificity	FPR
MLP	0.92	0.75	0.25
C4.5	1	0.96	0.03
KNN	0.90	0.85	0.14
SVM	1	0.89	0.10

TABLE III. COMPARISON OF METRICS FOR GRAY HOLE ATTACK

Gray hole Testing	Sensitivity	Specificity	FPR
MLP	0.6	0.75	0.25
C4.5	0.33	0.75	0.25
KNN	0.33	0.67	0.32
SVM	0.66	0.57	0.42

If sensitivity is high, the classifier is good at classifying records of positive class i.e. it produces few False Negatives and high false positive rate. If it is 100% the classifier produces zero False Negatives .If specificity is high ,the classifier is good at classifying records of negative class i.e. it produces few False Positives. In our experiments for black hole attack, C4.5 is good at classification as it is producing high sensitivity & specificity than other models. Whereas for gray hole attack SVM is good at classification as this model is producing high sensitivity than other models.

D. Receiver Operating Characteristics (ROC) Curves

ROC graphs are the best tools for assessing performance of classifiers. These are the two dimensional graphs constructed by plotting FPR Vs TPR. The diagonal line from (0, 0) to (1, 1) (Figure 8) shows random classifier performance.

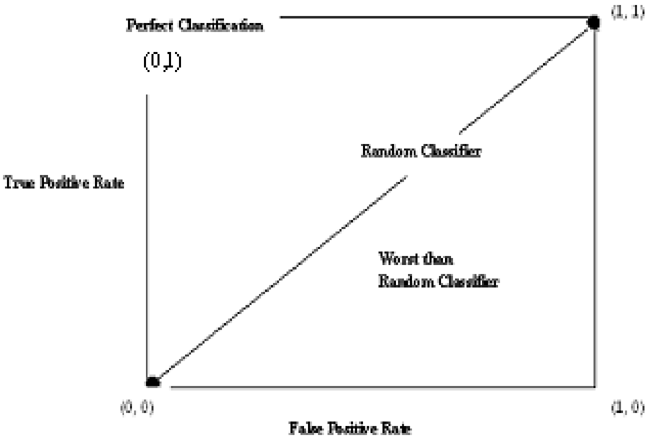

Figure 9.ROC for Random classifier

The classification model mapped onto this diagonal line produces same number of false positives & true positives. ROC graphs are symmetric along random performance line .Classifiers that fall below the region of random performance line gives worst performance than random classifier. The point (0, 1) on the top left corner shows perfect classification i.e. 100% TPR & 0% FPR. The point (0, 0) on bottom of the random classifier line, will not produce any false positives or true positives. However the point (1, 1) on the right top of random classifier line produces large number of true positives and false positives.
Figures 10, 11, 12 & 13 show the ROC graphs for the black hole attack and Figures 14, 15, 16, & 17 show the ROC graphs for gray hole attack. AUC (Area under Curve) is a variable which gives the area below the ROC curve. The best model will have maximum AUC value. According to Table 4 for black hole attack MLP & Decision Tree are giving high AUC values i.e. 99.89% and for gray hole attack SVM is giving high AUC values i.e. 81.84% whereas random classifier will have AUC value as 50%.

TABLE IV. COMPARISON OF AUC VALUES

AUC(in Percentage)	MLP	C4.5	KNN	SVM
Black hole	99.89	99.89	92.21	97.55

Gray hole	74.25	65.17	57.7	81.84

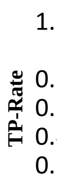

Figure 10. ROC Curve for MLP- Black hole attack

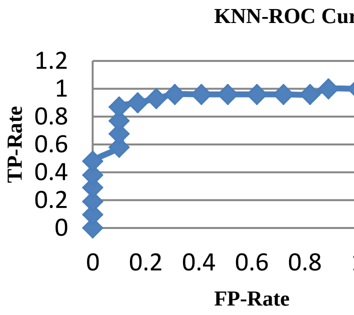

Figure 11. ROC Curve for KNN- Black hole attack

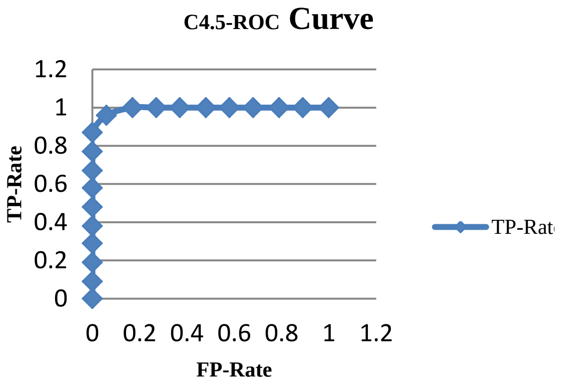

Figure 12. ROC Curve for C4.5- Black hole attack

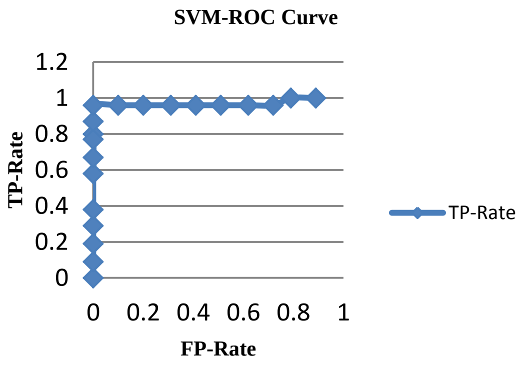

Figure 13. ROC Curve for SVM-Black hole attack

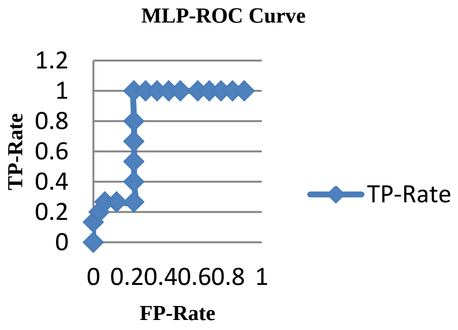

Figure 14. ROC Curve for MLP-Gray hole attack

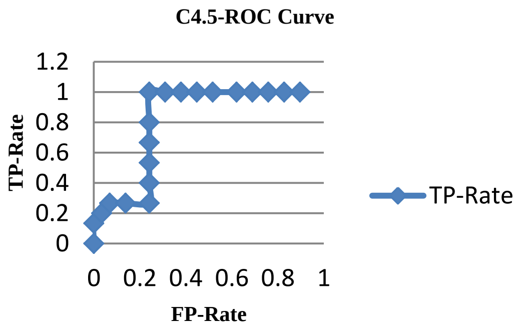

Figure 15. ROC Curve for C4.5-Gray hole attack

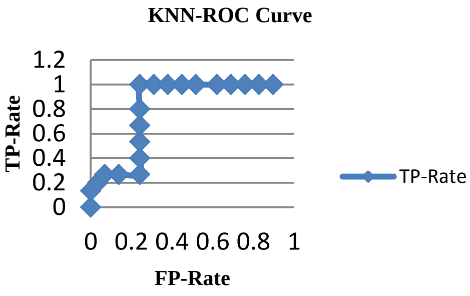

Figure 16. ROC Curve for KNN-Gray hole attack

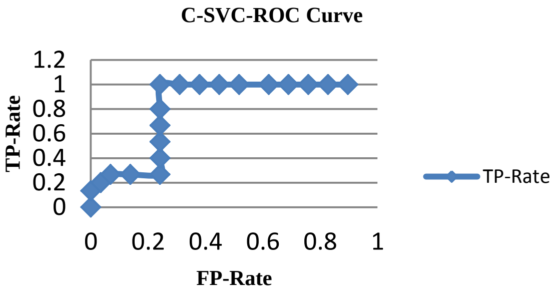

Figure 17. ROC Curve for SVM-Gray hole attack

The ROC curves of Decision Tree & MLP are almost touches the “perfect classification “point on the top left corner i.e. (1, 0) for Black hole attack and SVM & MLP in case of gray hole attack .

When comparing the four classification algorithms (MLP, C4.5, KNN, SVM) for black hole attack, in terms of accuracy, sensitivity & AUC, MLP and C 4.5 both have achieved highest values than other models. Similarly in terms of error rate & FPR, C 4.5 and MLP both have achieved lowest values compared to other models. Similarly, when comparing the four classification algorithms (MLP, C4.5, KNN, SVM) for gray hole attack, in terms of accuracy, sensitivity & specificity, MLP and C 4.5 both have achieved highest values than other models. However MLP & SVM have achieved highest AUC values compared to other models. Similarly in terms of error rate & FPR, C 4.5 & MLP both have achieved lowest values compared to other models. Finally, when comparing the four classification algorithms in terms of different metrics for both types of attacks MLP is giving better results than other models.

XI. Conclusions

In this paper we have analyzed the security threats faced in an ad hoc network. We have defined two types of threats namely Black hole and gray hole Attacks. These attacks were implemented against Ad hoc On Demand Vector reactive routing protocol using Network Simulator-2. Network Simulator is used to create a MANET environment. We then analyzed Trace files and sample set is constructed. Data mining techniques are applied on this sample set to build intrusion detection models in MANETs. This research has conducted a comparison among four data mining classification algorithms namely MLP, C 4.5, KNN & SVM. This study concludes from the results that MLP is a better classifier than other three classification models to detect black hole and gray hole attacks in MANETs. The proposed method is efficiently classifying attack and normal nodes.

References

[1] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour.” A survey of routing attacks in mobile adhoc networks”, *IEEE Wireless Communication*, 14 (5), pp. 85-91, 2007.

[2] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *ACM J. Wireless Networks*, pp. 545-556, 2003.

[3] Tiranuch Anantvalee , Jie Wu “A Survey on Intrusion Detection in Mobile Ad hoc Network “ in 2006 *Springer*.

[4] U. Sharmila Begam1, Dr. G. Murugaboopathi “A Recent secure intrusion detection system for MANETs” in *International Conference on Information Systems and Computing (ICISC-2013).*

[5] C. Perkins and E. Royer. “Ad-hoc on-demand distance vector routing”. In the 2nd *IEEE workshop on Mobile Computing Systems and Applications*, February 1999.

[6] S. S. Rizvi, S. Poudyal, V. Edla, and R. Nepal, " A Novel Approach for Creating Trust to Reduce Malicious Behavior in MANET", *ACM* 978-1-59593-770-4., 2007.

[7] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, “Intrusion Detection for Routing attacks in Sensor Networks,” in *International Journal of Distributed Sensor Networks*, pp. 313-332, october-December 2006.

[8] K.S. Sujatha,Vydekin Dhaman,R.S Bhuvaneswans “Design of Genetic Algorithm based IDS for MANET” in *IEEE conference ICRTIT*-2012.

[9] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in the Proceedings of the 23rd *International Conference on Distributed Computing Systems (ICDCS)* Providence, pp. 478-487, 2003.

[10] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat "Lightweight Sybil Attack Detection in MANETs" *IEEE SYSTEMS JOURNAL*, VOL. 7, NO. 2, JUNE 2013

[11] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han*," A Novel Cross Layer Intrusion Detection System in MANET",in the proceedings of 24th *IEEE International Conference on Advanced Information Networking and Applications*,2010.

[12] Zahra moradi and Mohammad Teshnehlab "Implimantaion of Neural Networks for Intrusion Detection in MANET "in *IEEE conference (ICETECT) 2011*.

[13] Katharine Chang and Kang G. Shin" Application- Layer Intrusion Detection in MANETs" in Proceedings of the *43rd Hawaii International Conference on System Sciences* – 2010.

[14] Konagala Pavani and Dr. Damodaram Avula' "Performance of Mobile Adhoc Networks in Presence of Attacks"in 3rd *international Conference on Information Security and Artificial Intelligence (ISAI 2012)*,Pune

[15] http://www.isi.edu/nsnam/ns/ K. Fall and e Varadhan. The ns Manual (formerly ns Notes and Documentation), 2000.

[16] NS by example http://nile.wpi.edu/NS/overview.html,14 May 2006.

[17] Virtual IntercNetwork Testbed, http://www.isi.edu/nsnam/vint, 14 May 2006.

[18] Alan Bivens, Chandrika Palagiri "Network based intrusion detection using neural networks" in proc intelligent *engineering systems through artificial neural networks* 2002.

[19] Quinlan JR. "C4.5: programs for machine learning," Log Altos,CA: Morgan Kaufmann; 1993.

[20] Oliver Sutton ,"Introduction to k Nearest Neighbour Classi_cation and Condensed Nearest Neighbour Data Reduction", February, 2012

[21] Gongde Guo1, Hui Wang 1, David Bell 2, Yaxin Bi 2, and Kieran Greer "KNN Model-Based Approach in Classification,"

[22] B. E. Boser, I.M. Guyon, and V. N.Vapnik, "A training algorithm for optimal margin classifier," in Proc. 5th ACM Workshop Comput. Learning Theory, Pittsburgh, PA, July 1992, pp. 144–152.

[23] K.Pavani, Dr.Damodaram "Anomaly Detection in Computer Security using Support Vector Machines",IT For Real World Problem"*International conference on IT For Real World Problem,*December 2009.