The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

AN AUTOMATED MULTI-LAYER INTRUSION DETECTION MECHANISM FOR WIRELESS SENSOR NETWORKS

Dr. GANESH DAVANAM[1], Dr. M.SUNIL KUMAR[2], MS.M.BABITHA[3] and Dr. C.SUSHAMA[4]

[1,2,3,4] Department of Computer Engineering, Sree Vidyanikethan Engineering College (Autonomous),Tirupati, Andhra Pradesh, India.
Email: [1]dgani05@gmail.com, [2]sunilmalchi1@gmail.com, [3]machababitha@gmail.com, [4]Sushama.c@vidyanikethan.edu

ABSTRACT:

A Mobile Adhoc Network (MANET) is composed of nodes which are spatially distributed over a geographical region. The nodes are autonomous in nature and the network is an infrastructure less network. Each node in the network is free to move in any direction and the links between the nodes will be changed frequently. Each node in the network forwards data packets from other nodes and behaves like a router which receives packets from source nodes and forwards it towards destination nodes. In MANET the security plays a major role and this area has grasped many researchers to propose solutions to various issues and challenges in MANET especially in the area of intrusion detection. This paper focuses on establishing real time intrusion detection in MANET using deep neural networks. The deep neural network is able to classify the network traffic as either normal or abnormal. The neural network based intrusion detection is not limited to a particular type of attack. The model eliminates the need for human effort to write signature of various attacks. The model is trained with historic data to classify the type of abnormality in the traffic such as Gray hole, black hole, forging, packet dropping, and flooding attacks. The accuracy of the model in classifying the network traffic is high when compared to other models designed to address the same problem.

KEYWORDS: MANET, intrusion detection, deep neural network, network traffic.

1. INTRODUCTION

A mobile ad hoc network (MANET)[1] composed of nodes which can self-configure themselves and they don't use any infrastructure to connect with other nodes wirelessly[2][3]. MANETs are highly dynamic and their topology is autonomy in nature [4]. Because of their nature MANET demands specific and unique security requirements. MANET is prone to security attacks because of its shared wireless communication medium, multi-hop adhoc data transmission and deployment in unprotected physical location. The network must be protected from not only external attacks but also from attacks from selfish and malicious nodes present in the network. Many mechanisms and approaches have been proposed in various literatures to ensure security against specific attacks in MANET. Many of these approaches ensure security up to only certain extent and Intrusion Detection System is one such efficient solution to safe guard network against multiple security attacks. The intrusion detection mechanism forms as a first step in ensuring the safety and security in the MANET. There are various types of attacks possible in the network which degrades the overall performance of the network. The attacks in the MANET can be categorized as external, internal, wormhole, black hole, flooding, link spoofing, replay, and link with holding attacks.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

In the case of link spoofing attack a malicious node disrupts the routing operation by advertising fake links with the non-neighboring nodes. In link with holding attack the link losses appears to be in more common due to the ignorance of malicious node to advertise the links of specific nodes. The link with holding attack causes serious issues in OLSR routing protocol. In MANET the links between the nodes are not stable in nature as the nodes move dynamically within a geographical area. The topology of the network is not constant over various periods of network simulation. In a replay attack [11] the malicious node records and sends the control messages of a valid node to other nodes. The nodes receive stale routes from the malicious node and update the same in their respective routing table. A specific legitimate node is impersonated by a malicious node to disturb the routing operation in MANET.

The attacks in the MANETs are primarily categorized based on their origin and based on attack nature. Based on origin the attacks are further divided in to two categories namely Internal and External attacks. The attacks are categorized as active or passive attacks based on their nature. The IDS can be categorized in to two classes; Signature based and Anomaly based [2, 3]. Anomaly based IDS is capable of discriminating the normal traffic and abnormal traffic in the network. I can also able to discriminate between the normal and new attack type but it suffers from high false alarming rate and false positive alarms. Signature based attacks are efficient in detecting the multiple attacks whose attack pattern or signature is known already. It cannot able to detect the new attack which it has not seen earlier. The IDS enables the sending nodes in the network to select a safe and secure routing path to the destination. The anomaly based detection is implemented in [4] with proactive routing protocols. The IDS can be implemented in case of reactive routing protocols also [5, 6]. The IDS mechanism can be implemented at each node (node based) or central node in the network (network-based). As the MANET nodes are operating with less energy sources implementing the IDS in each of the node will not be feasible. Hence a network based IDS which analyses the traffic flow in the network to identify the known attacks is more efficient when compared to the other approach.

This paper attempts to design and model network based deep neural classifier that can efficiently detect the abnormal traffic patterns and classify the attack category respectively. The paper is organized as follows. This paper presents a detailed review of various efficient IDS mechanism proposed for MANET in section 2. Section 3 describes the architecture of deep neural network and the Section 4 briefs about the process of collecting network traffic data and the network simulation environment. The section 5 briefs about the experimental results and the quality metrics used for the comparison of the employed classification models. Finally the Section 5 concludes the paper.

2. RELATED WORK

A simple mechanism to implement intrusion detection is to train a classifier using historic network traffic data to classify the normal and abnormal traffic data in the network. The objective of the classification process is to minimize the overall classification error. In the classification of network traffic the cost of undetected attack is high when compared to the cost of giving a false alarm. Intrusion detection is a hot area of research in the field of MANET and

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

many researchers have developed various approaches like rule based and anomaly detection systems. In this paper an intrusion detection system is developed using classification algorithms. A detailed review of various other approaches and algorithms for intrusion detection is conducted. In [5] the first IDS approach for MANET was proposed and the proposed method adopted a distributed and co-operative approach. This became a guide for designing anomaly based IDS. The routing information available on the MAC layer is used for detecting the intruders based on anomaly approach. In [6] the authors have extended the previous work by introducing a cluster based IDS which focused on implementing the proposed IDS approach in a resource constraint environment. From the routing tables statistical features were extracted and using classification decision trees the network traffic was classified as either normal or abnormal. This approach is capable of identifying the source of the attack provided the intrusion originated at a one hop distance. In [7] the authors have proposed two distributed ID approaches. The ID follows a hierarchical and distributed approach respectively. They used Support Vector Machine (SVM) for the classification of intrusion and main focus is on analyzing the intrusion detection in network layer. In the various experiments conducted they found that hierarchically distributed method yielded better results when compared to a fully distributed anomaly detection method. For the classification of abnormal traffic patterns a set of parameters are derived from the network layer.

In another work proposed in [8] a completely distributed anomaly detection approach was proposed and the behavior of the mobile nodes is modeled using the information available in the MAC layer. Cross-feature analysis [9] was applied on the set of extracted feature vectors from the training data. In [10] a co-operative and distributed approach was used for intrusion detection utilizing the information available from the MAC, network and application layers. For classification a Bayesian classifier was used.

From the work mentioned in [14] utilizes a three layered architecture of Recurrent Neural Network (RNN) with 41 features extracted from the network traffic data. The trained RNN is capable of detecting 4 categories of attacks. The performance of the model in discriminating the normal traffic from abnormal traffic was not discussed. The deep learning techniques will help to overcome various challenges in designing a real time network based IDS [15, 16].

We've produced a new WSN dataset, termed WSN-DS, by Almomani and colleagues [17]. WSN included both standard network traffic and a variety of denial-of-service (DoS) assaults (including flooding, grayhole, blackhole, and scheduling attacks). The LEACH methodology was used in its development. In WSNs, this is one of the most prevalent hierarchical routing protocols. NS2 simulator to gather data. Artificial intelligence was implanted using a (WEKA) data-mining toolset. A neural network (ANN) is used to identify and classify the four different attacks. Classification was accomplished through the use of cross-validation with 10 folds and holdout splitting. According to the research, the algorithm ANN trained by WSN-DS obtained a high classification of DoS attacks, with the exception of the grayhole attack, whose detection rate is extremely low in comparison to the other methods used in the study.

In order to detect Denial-of-Service (DoS) attacks in cluster-based WSNs, Dong et al. [18] suggested an intrusion detection model based on information gain ratio and Bagging algorithm.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

When it came time to trim the fat, the authors turned to the information gain ratio. As a result of the Bagging algorithm's development, used to build an ensemble technique for training a group of C4.5 decision trees changing things for the better. NSL-KDD and WSN-DS were used to implement the proposed model. To test the model's performance, split the datasets. This technique offers improved better results than other techniques.

There are a number of machine learning approaches that can be used to detect DoS attacks in WSNs, according to Abdullah et al. [19]. SVM, Naves Bayesian, Random Forest and Decision Tree classifiers were implemented using the WEKA data processing platform. WSN-DS is used as a dataset for the mining tool. This study found that the SVM classifier was the most accurate. Detection accuracy rate compared to the other intrusion detection systems techniques.

3. PROPOSED MULTI LAYER DETECTION MODEL

A framework for vulnerability scanning in WSN, shielded with a defense-in-depth method, is proposed in this work, resulting in increased system security overall. Both the Edge-based Method and the Cloud-based Method use machine learning methods to make it easier to spot attacks on the network that haven't been seen before (see Fig. 1 for an overview). This is a follow-up to our recent study [20]. This section provides an in-depth look at each of the methods that were used:

A. First Detection Layer: Based on naive Bayes theory with our binary classifier [21], [22], we chose to keep things simple and not overwhelm the first detecting layer with false positives and false negatives. Because of its ease and computational efficiency, we chose the Naive Bayes algorithm as the classifier's foundation. This makes it a potential choice for generating real-time decisions about examined packets. Relying on the well-known Bayesian theorem, the Naive Bayes classifier is well-suited to large datasets [23][27][28]. However, even in the most complex real-world situations, this classifier works very well and may outperform more advanced classification approaches. The Naive Bayes model is more computationally efficient than other Classifiers because it enables each feature to contribute equally and freely to the final judgement.

B. Second Detection Layer: Using a Random Forest Because we're aiming for simplicity and speed in the decision-making process at the first layer, as we described in the previous part, the monitored traffic will be classified as either normal or malicious at that layer, with no more specifics about attack type. There are, however, advantages to using a cloud-based second layer of detection for suspicious traffic. This means that more algorithms and more rigorous examination may be carried out. A multi-class classifiers has been utilized to determine the sort of the assault launched, therefore offering suggestions for determining the best defense method. Every tree in the Random Forest classifier offers information on the class of each sample. The class with more votes at the conclusion of the categorization is chosen as the most likely class. To create a wide variety of decision trees, Breiman's concept of bagged with randomly picked features is used as the basis for this classifier's aggregation technique [24]. Decision Random forest classifier uses supervised learning techniques to generate trees, which are then utilized to solve classification and regression problems. Training multiple samples,

ISSN 1533-9211

DOI 10.5281/zenodo.7022800

each with a set of attributes, yields unique rules that may be clearly understood because they are represented as a forest graph.

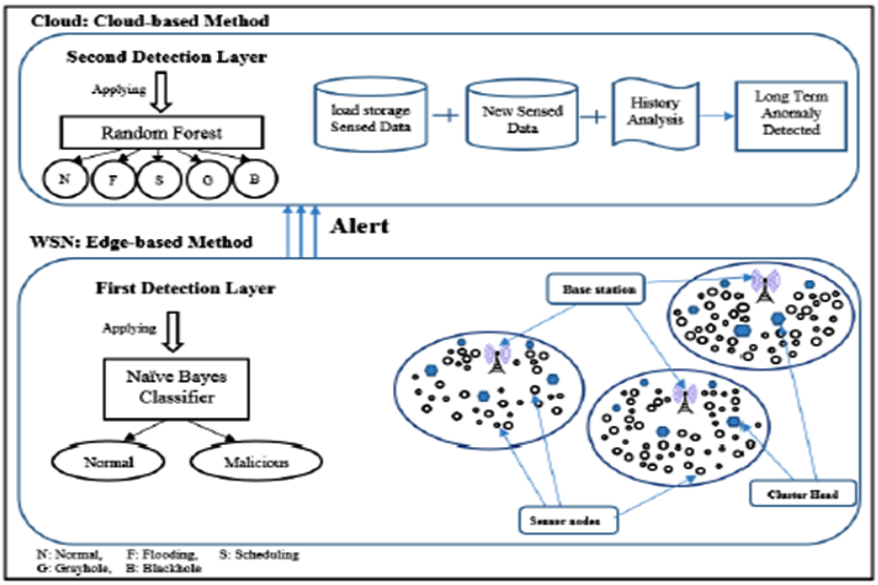

Figure 1: Real time Intrusion detection process

4. DATASET

For training and evaluating the DNN model a MANET has been simulated and a series of experiments were conducted. It is assumed that the network doesn't have any infrastructure and Adhoc On-demand Distance Vector (AODV) routing protocol is used [14]. The network is simulated using NS2 network simulator. The network consists of 200 nodes placed randomly within an area of 1000x1000sq.mt. Each node is equipped with an antenna having 250m propagation and 2 Mbps of channel capacity. The nodes present in the network follows a random way point model. Before changing the position every node remains static for finite period of time and is referred as pause time. Each node moves from one position to another in a speed which ranges between 0 to maximum speed. The maximum speed of a node in the network is configured as 20 m/s. The total simulation period is fixed as 1200s. During the simulation period source nodes generates Constant Bit Rate (CBR) data traffic with a bandwidth of 2 Mbps.

The size of the generated data packets is 512 bytes. Different scenarios have been simulated by varying the number of malicious node present in the network. The number of malicious nodes is varied between 5 and 20 and under each environment the performance of the trained deep neural model is analyzed. Also the performance of the model is analyzed by varying the sampling interval. If the value of sampling interval is high then the detection of intrusion will be slow.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

In the simulations different types of attacks including flooding, black hole, packet dropping, and link spoofing attacks have been simulated to generate abnormal data traffic in the network. The features extracted from the normal data traffic are labeled as Normal and the abnormal data traffic are labeled with the respective type of attack. Once the simulations are completed the feature vectors used for training the neural model are extracted. The features must be selected in such a way that they can better represent the overall information available in the network and sufficiently they must be able to discriminate between normal and abnormal traffic.

The following features are selected from the network layer the total number of data packets sent from each node, number of data packets received by each node, number of route request broadcasted in the network, number of route error packets, number of changes in the route entries, and the number of packets dropped in the network. A training data set was generated for each of the sampling time interval. Each training data set consists of the above mentioned features for various pause time and number of malicious node in the network. Similarly a test data set for evaluating the performance of the model is also generated.

5. EXPERIMENTS & RESULTS:

During the experiments the ability of the Deep learning model in binary classification (normal vs anomaly traffic) and multi-class classification (classifying attack type) is analyzed. The generalization ability of the model depends on the values of the hyper-parameters especially on the value of learning rate. During the training phase if the value of learning rate is kept too low then the model behaves perfectly for training data and when tested on unseen new data its performance will be poor. The generalization ability of the model will become low and it cannot discriminate the new intrusion patterns in the test set.

For assessing the performance of the classifier a series experiments are conducted under various conditions. During each of the experiment the model hyper parameters are varied and the deep neural network is trained based on a k-fold cross validation. Few hyper parameters considered in our experiments includes learning rate, number of hidden layers and the number of neural in each layer, gradient momentum, rate of weight decay, dropout probability. The tuning of hyper-parameters is tough problem in deep learning which involves choosing a set of optimal hyper-parameters for the back propagation learning algorithm.

The learning rate is adjusted during training phase in accordance with the loss function to find an optimal value. The learning rate is varied from higher to lower values and initially the value is kept high and every time using a scheduler defined in Equation below.

$$\eta_t = \eta_{min} + (\eta_{max} - \eta_{min})(\max(0, 1 - x)) \rightarrow 1$$

$$\text{where } x = \left[\frac{\text{iterations}}{\text{stepsize}} - 2\left(\frac{1+\text{iterations}}{2*\text{stepsize}}\right) + 1\right] \rightarrow 2$$

η_{min} and η_{max} are the lower and upper bounds of the learning rate, iterations is the number of completed mini-batches. The Fig. 3 presents a plot of variation in the learning rate against loss

ISSN 1533-9211

DOI 10.5281/zenodo.7022800

function value. When the value of learning rate is too low the model is not converging and when it is high the model starts diverging.

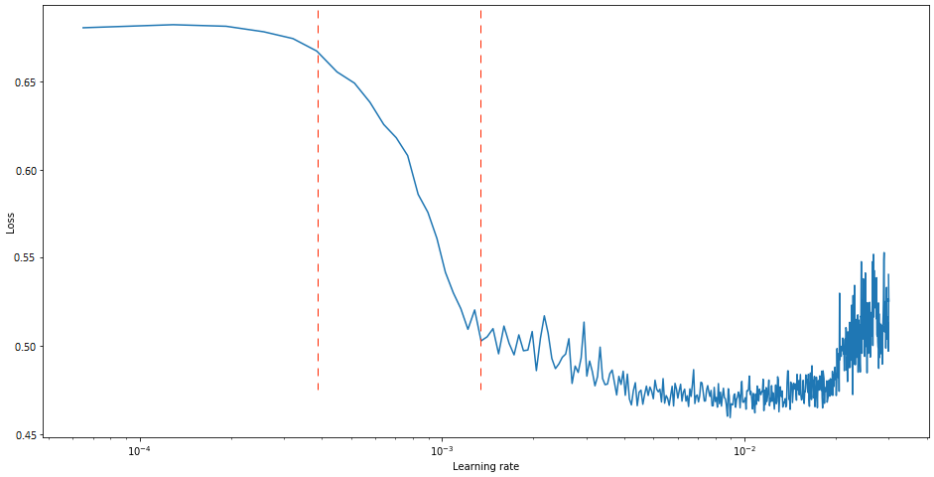

Figure. 2: Loss vs learning rate

When hyper parameters are tuned to an optimal value then the neural network will yield higher accuracy and lower error. The simple technique used for optimization of hyper parameter uses a grid search method, which is complex and exhaustive. The search process is guided through a cross validation score or based on the performance on the validation data [13]. For elimination of over fitting issue dropout regularization was adopted which helps to increase the generalization ability of the network. The activation functions introduce the non-linearity to the model and hence a non-linear decision boundary is produced. The hidden layer output are sent to the Rectified Linear Units (ReLU) and the output layer is given to a softmax activation. ReLU is a simple activation function which is represented as $f(x) = \max(x, 0)$and Softmax activation estimates the class probability and it is expressed mathematically as

$$\sigma(z)_j = \frac{e^{z_j}}{\sum_{k=1}^{K} e^{z_k}} \rightarrow (3)$$

The hyper parameters of the model are fine-tuned using cross validation algorithm wherein the training dataset is split in to non-overlapping k-folds (each subset is mutually exclusive and their union gives the complete training data set. For selecting the hyper parameters k models are built and trained with k-1 subsets of training samples where the k^{th} model is evaluated using the $d_k$subset. The average error of the model is estimated for different values of the hyper parameters and the set of hyper parameters which yields less average error is chosen as optimal values.

In binary classification for discriminating the normal and abnormal data traffic the binary cross entropy loss function is used it can be calculated as:

$$L(y, p) = -(y.\log(p) + (1 - y).\log(1 - p)) \rightarrow (4)$$

ISSN 1533-9211

DOI 10.5281/zenodo.7022800

For classifying the traffic patterns among different category of attacks the loss function was modified in such a way a separate loss for each class label per observation was calculated and summed together.

$$L(y, p) = -\sum_{c=1}^{M} y_{o,c} \log(p_{o,c}) \rightarrow (5)$$

Where M denoted the number of attacks The Random Forest classifier and Naïve Bayes classifiers were also trained with the same training data and compared with the results of the Deep Neural Network. For analyzing the performance of the classifiers Detection Rate (DR) and False Alarm (FA) are used.

$$DR = \frac{TP}{TP+FN}, FA = \frac{FN}{TN+FP} \rightarrow (6)$$

where TP, TN, FP, and FN are TRUE and FALSE positive and negatives of the classifier result respectively. The objective of the classification task is to reduce the false alarm and

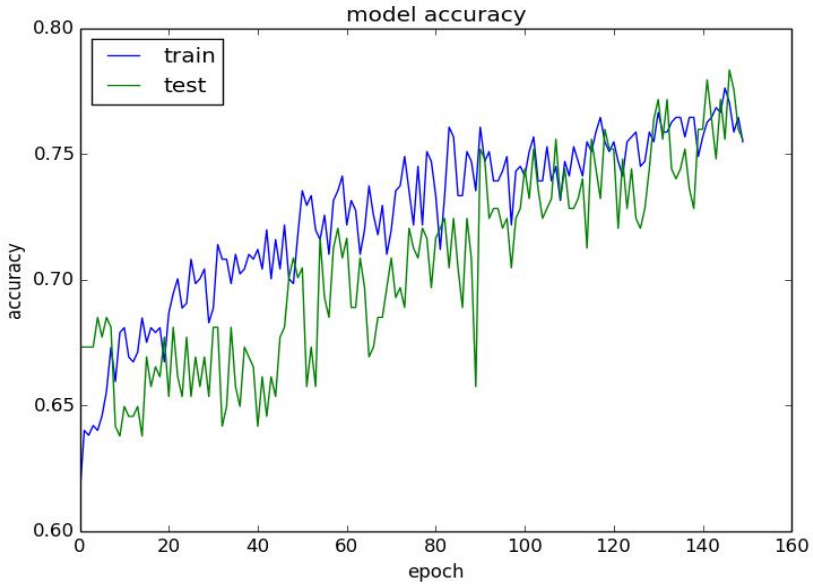

Figure 3: plot of Deep Neural Network accuracy on training and test data set

ISSN 1533-9211

DOI 10.5281/zenodo.7022800

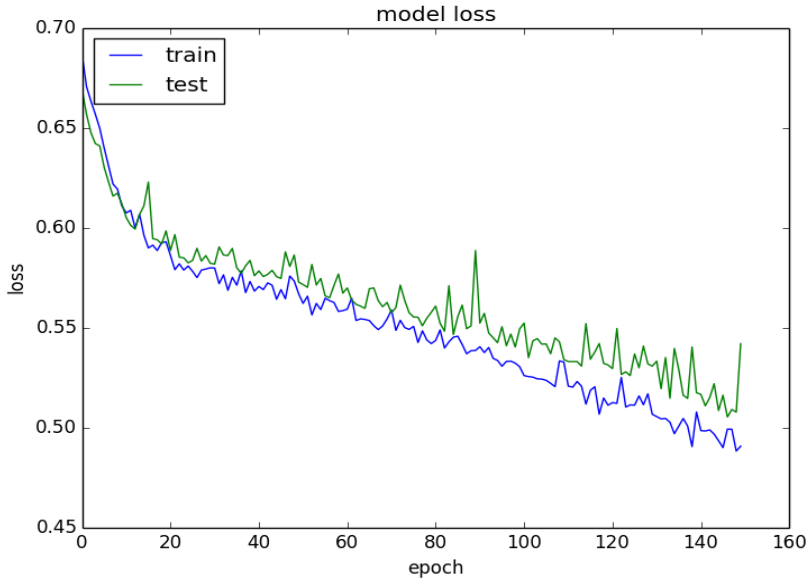

Figure 4: plot of Deep Neural Network losson training and test data set

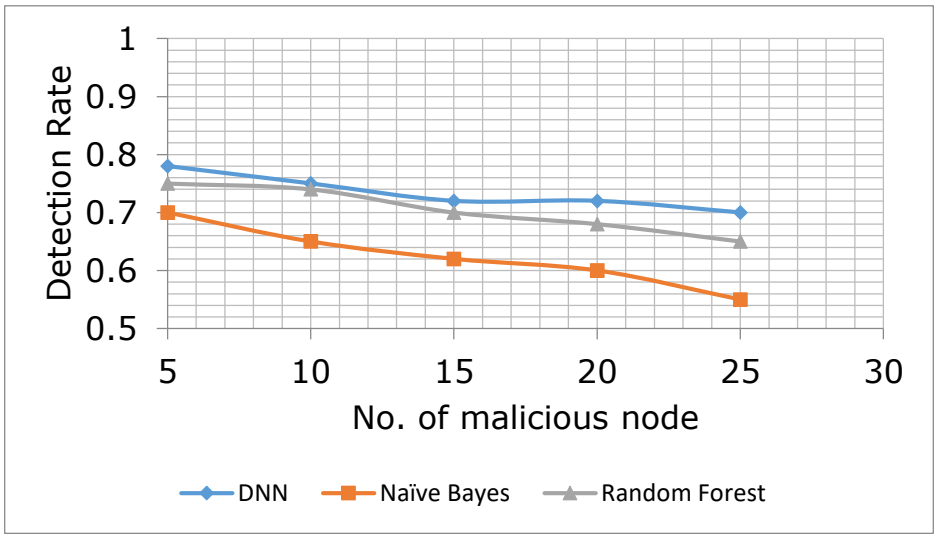

Figure 5: Comparison of classifiers based on Detection Rate

The figure above presents the behavior of classifiers when the number of malicious node in the network is steadily increased. It was observed that the detection rate linearly decreases as the number of malicious node is increased. This is due the fact that the ratio of normal to the abnormal traffic in the network is low when the number of malicious node presents in the network is less. When the malicious node is increased the volume of abnormal traffic in the network is also increases and thereby the variation in between the observed traffic patterns is

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

less. Thus the detection rate of the classifiers steadily decreases. From the Fig 5 it is clear that the deep neural network achieves high detection rate and the Naives Bayes classifier gives the lowest detection rate.

Second Layer Results and discussions:

Attack Type	Previous Results					Proposed Results					% of change
	TPR	FPR	FNR	TNR	P	TPR	FPR	FNR	TNR	P	P
Normal	0.984	0.012	0.016	0.988	0.985	0.995	0.011	0.005	0.988	1.0	+0.3
Flooding	0.958	0.003	0.420	0.997	0.923	0.965	0	0.035	1.0	0.995	0
Scheduling	0.941	0.020	0.059	0.980	0.985	0.953	0.004	0.047	0.996	0.986	0
Gray hole	0.689	0.005	0.311	0.950	0.923	0.758	0.001	0.242	0.999	0.999	+7.2%
Black hole	0.910	0.025	0.090	0.975	0.658	0.952	0.001	0.048	0.999	0.99	+39%

RF classifier is used to do a multi-class classification to identify the specific malicious communication on the second detection layer.in order to select the most effective line of defense; it could be observed that a reasonably high level of complexity was required Table II shows the results of the experiment. Therefore, a high level of detection enables more precise analysis countermeasures that the system will take on its own. For the most part, an IDS's primary goal is to achieve a high degree of accuracy. The number of cases anticipated by this measure [32] you're right, but it's a little too obtrusive. On the basis of this, when comparison of RF classifier performance in comparisons between this research and a previous work that employed the same dataset, such as[24] shows that a greater degree of precision has been achieved.in which the accuracy of assaults detection was improved83 percent, 94 percent, 99.5 percent, 95.6 percent, and 99 percent in Blackhole, Flooding, and Black HoleBeyond the usual threats, there are Grayhole attacks and scheduling accordingly, in the situation (without assaults). In this comparison, we can see that between the work done by [24] and the current project as shown in the diagrams in Figures 6 & 7, where we offer a model that improvement in TPR, TNR, FPR, and other performance metrics Comparison of FNR and Precision with earlier work.

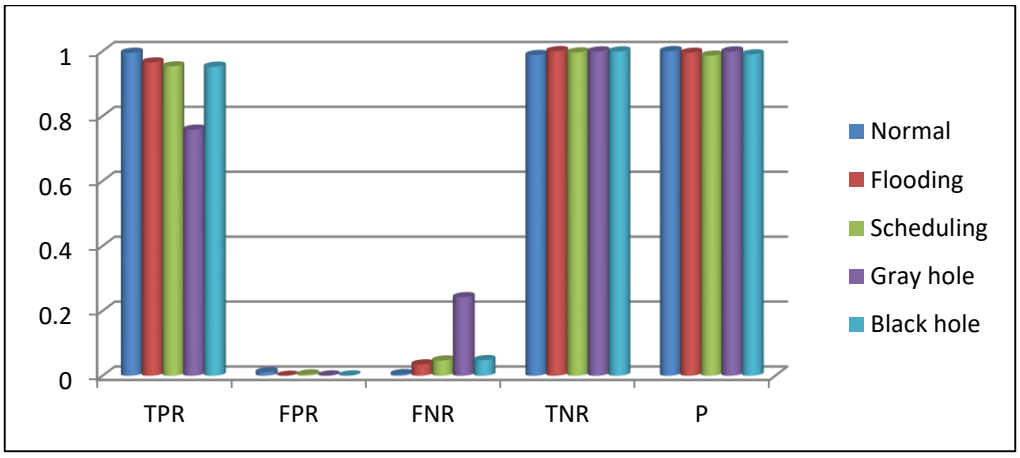

Figure 6: Existing Framework Results

ISSN 1533-9211

DOI 10.5281/zenodo.7022800

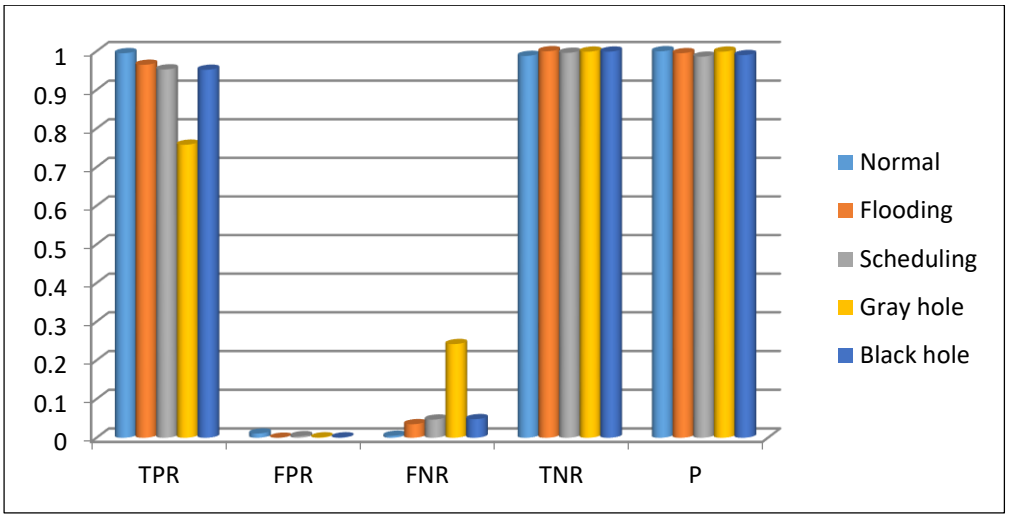

Figure 7: Proposed Multilayer Detection Model Results

6. CONCLUSION

This paper analyzed the suitability of classification algorithms for the intrusion detection in MANETs. Especially the deep neural network was investigated in deep and it is compared with other classifiers such as Naïve Bayes classifier and random forest classifier. The performance of the classifiers was analyzed in terms of detection rate and false alarm. This paper also investigated in detail on the procedure for hyper parameter tuning in Deep Neural Network to yield better accuracy in detecting the abnormalities in the network. The classifiers were trained with the datasets covering different attack types at various levels of network mobility and level of abnormality. On comparing the obtained results it is observed that the Naïve Bayes classifier gives a poor result and the Deep Neural Network yields better results. The generalization ability of the network is high since the over fitting problem is eliminated by using dropout regularization during the training. It can be concluded that the intrusion detection approach using Deep Neural classifiers can be applied in real network scenarios. As a future work the trained classifiers may be tested in real time applications. Packet sniffing tools can be used to capture the network traffic and same set of features are extracted for evaluating the performance of the classifiers. The real time traffic data are manually labeled and compared against the predicted results from the classifier.

REFERENCES

1. "Wireless ATM & Ad Hoc Networks". Kluwer Academic Press. 1997.
2. Morteza M. Zanjireh; Hadi Larijani (May 2015). A Survey on Centralised and Distributed Clustering Routing Algorithms for WSNs (PDF). Conference: IEEE 81st Vehicular Technology Conference: VTC2015-Spring. Glasgow, Scotland. pp. 1–6.
3. Chai KeongToh (2002). "Ad Hoc Mobile Wireless Networks: Protocols and Systems 1st Edition". Prentice Hall PTR.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

4. Zanjireh, M. M.; Shahrabi, A.; Larijani, H. (1 March 2013). "ANCH: A New Clustering Algorithm for Wireless Sensor Networks": 450–455.
5. Y. Zhang, W. Lee, Y. Huang, Intrusion detection techniques for mobile wireless networks, Wireless Networks 9 (5) (2003) 545–556.
6. Ganesh, D., Sunil Kumar, M., & Rama Prasad, V. V. (2017). Mutual Trust Relationship Against Sybil Attack in P2P E-commerce. In Innovations in Computer Science and Engineering (pp. 159-166). Springer, Singapore.
7. H. Deng, Q. Zeng, D.P. Agrawal, SVM-based intrusion detection system for wireless ad hoc networks, in: Proceedings of the 58th IEEE Vehicular Technology Conference (VTC'03), vol. 3, Orlando, FL,USA, 6–9 October 2003, pp. 2147–2151.
8. Davanam, Ganesh, T. Pavan Kumar, and M. Sunil Kumar. "Novel Defense Framework for Cross-layer Attacks in Cognitive Radio Networks." In International Conference on Intelligent and Smart Computing in Data Analytics, pp. 23-33. Springer, Singapore, 2021.
9. Y. Huang, W. Fan, W. Lee, P. Yu, Cross-feature analysis for detecting ad-hoc routing anomalies, in: Proceedings of the 23rd International Conference on Distributed Computing Systems, Rhode Island, USA, 2003, p. 478.
10. S. Bose, S. Bharathimurugan, A. Kannan, Multi-layer intergraded anomaly intrusion detection for mobile ad hoc networks, in: Proceedings of the IEEE International Conference on Signal Processing, Communications and Networking (ICSCN 2007), February 2007, pp. 360–365.
11. Ganesh, Davanam, Thummala Pavan Kumar, and Malchi Sunil Kumar. "OptimisedLevenshtein centroid cross-layer defence for multi-hop cognitive radio networks." IET Communications 15, no. 2 (2021): 245-256.
12. Bengio Y, Simard P, Frasconi P, Learning long-term dependencies with gradient descent is difficult. IEEE Trans. on Neural Networks 1994.
13. Sangamithra, B., P. Neelima, and M. Sunil Kumar. "A memetic algorithm for multi objective vehicle routing problem with time windows." In 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), pp. 1-8. IEEE, 2017.
14. M. Sheikhan, Z. Jadidi, and A. Farrokhi, ''Intrusion detection using reduced-size RNN based on feature grouping,'' Neural Comput. Appl., vol. 21, no. 6, pp. 1185–1190, Sep. 2012.
15. Ganesh D, Kumar TP, Kumar MS. A Dynamic and adaptive learning mechanism to reduce cross layer attacks in cogntive networks. Materials Today: Proceedings. 2020 Dec 31.
16. M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish, and A. E. Hassanien, "Hybrid Intelligent Intrusion Detection Scheme," in Soft computing in industrial applications, pp. 293–303, Springer, 2011.
17. Almomani I, Al-Kasasbeh B and Al-Akhras M 2016 Journal of Sensors 2016.
18. Myint H O and Meesad P 2009 Incremental learning algorithm based on support vector machine with mahalanobis distance (isvmm) for intrusion prevention 2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology vol 2 (IEEE) pp630-633 .
19. Abdullah M A, Alsolami B M, Alyahya H M and Alotibi M H 2018 Journal of fundamental and Applied.
20. D.M.; Ibrahim, and N.M. Alruhaily, "Anomaly detection in Wireles Sensor Networks: A Proposed Framework," International Journal of Interactive Mobile Technologies (iJIM), vol. 14, pp. 150–158, 2020.
21. S.L. Ting, W.H. Ip, Tsang, and H.C. Albert, "Is Naive Bayes a goo classifier for document classification," International Journal of Software Engineering and Its Applications, vol. 5, pp. 37–46, 2011.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7022800

22. E. Frank, Bouckaert, and R. Remco, ”Naive bayes for text classification with unbalanced classes,” In European Conference on Principles of Data Mining and Knowledge Discovery, Springer, pp. 503–510, 2006.
23. A. El Abdouli, L. Hassouni, and H. Anoun, ”Sentiment Analysis of Moroccan Tweets using Naive Bayes Algorithm,” International Journal of Computer Science and Information Security (IJCSIS), vol. 15, 2007.
24. L. Breiman, ”Bagging predictors Machine learning,” Springer, vol. 24, pp. 123–140, 1996.
25. Ghorbani, A.A.; Lu, W. Tavallaee, M. Network intrusion detection and prevention: concepts and techniques. In Springer Science & Business Media, 2009.
26. I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, ”WSN-DS: A dataset for intrusion detection systems in wireless sensor networks,” Journal of Sensors; Hindawi, vol. 2016, pp. 1–16, 2016.
27. SS Chakravarthi, RJ Kannan. "Detection of anomalies in cloud services using network flowdata analysis" , The international Journal of Electrical Engineering & Education, 2020.
28. Samir Ifzarne, Hiba Tabbaa, Imad Hafidi, Nidal Lamghari. "Anomaly Detection using Machine Learning Techniques in Wireless Sensor Networks", Journal of Physics: Conference Series, 2021