International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

Intrusion Detection System for Vehicular Ad-hoc Network using Deep Learning

Rasika S. Vitalkar[1], Samrat S. Thorat[2], Dinesh V. Rojatkar[3]

[1]M.Tech Student, Department of Electronics Engineering, Government College of Engineering, Amravati, Maharashtra, India
[2]Assistant Professor, Department of Electronics Engineering, Government College of Engineering, Amravati, Maharashtra, India
[3]Associate Professor, Department of Electronics Engineering, Government College of Engineering, Amravati, Maharashtra, INDIA

Abstract - *Vehicular Ad-hoc Networks (VANETs) are gaining much interest and research efforts over recent years, VANETs play a vital role in the success of self-driving and semi self-driving vehicles, where they improve safety and comfort. However, security threats that are either seen in the ad-hoc networks or unique to VANET present considerable challenges. The main objective of VANET is to improve the safety, comfort, driving efficiency. There is rapid development in smart vehicles for transmitting the information, all these vehicles are now uses the internet services for communication. Such vehicles depend heavily on external communication with the surrounding environment via data control and Cooperative Awareness Messages (CAMs) exchanges. VANETs are potentially exposed to a number of attacks. This work presents an Intrusion Detection System (IDS) for VANET that relies on anomaly detection to protect the external communication system from attacks. These attacks aim to disrupt the transmission between vehicles and roadside units. In this paper we proposed intrusion detection system for VANET which used Deep Belief Network (DBN) algorithm of deep learning. Deep Belief Network is an effective method of solving the problems from neural network with deep layer, such as low velocity and the overfitting phenomenon in learning. The intrusion detection system for VANET is used to detect the attack and prevent the network.*

Key Words: *Deep Belief Network, Deep learning, Intrusion Detection, Vehicular Ad-hoc network (VANET),CICIDS2017 dataset*

1. INTRODUCTION

A Vehicular ad hoc network called VANET is a mobile network allowing to vehicles to communicate with each other in the absence of fixed infrastructure, with the aim of improving road safety through the exchange of alerts between vehicles. VANET is an emerging type of Mobile Ad-hoc Networks (MANETs). VANET consists of On-Board Units (OBUs) and Road Side Units (RSUs). VANETs play a vital role in the growth and the use of self-driving and semi self-driving vehicles. Internal and external communication systems are considered important components in autonomous and semi-autonomous cars. Safety is one of the most crucial objectives of VANET. As safety will reduce accidents, save lives and reduce traffics. Among side safety, other services such as Internet access, weather forecast, and geolocation information can enrich travel experience by providing travel comfort, convenience and infotainment. Vehicle Ad Hoc Network (VANET) is one of the developing technologies that can dramatically change ways of communication and industry. It suggestively rallies the quality of human beings and will become a reality soon. Many vehicle makers began incorporating wireless access in the vehicular environment (WAVE) in their vehicles and WAVE is a technology designed on the IEEE 802.11p protocol that provides the broadcast standard for the Dedicated short-range communications technology (DSRC). VANET enables wireless communication between vehicles through the DSRC including vehicle-to-vehicle communication (V2V) as well as vehicle infrastructure communication (V2I) VANETs represent the communication between vehicles (V2I) and their Road Side Units (RSUs) or intra vehicular communication (V2V) in radio coverage area. These are two types of vehicle communication vehicle to vehicle communication(V2V) in which a pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure and second is communication between the road side units (RSU), a fixed infrastructure, and vehicle called vehicle to infrastructure communication. VANET Structure is shown in fig.1.

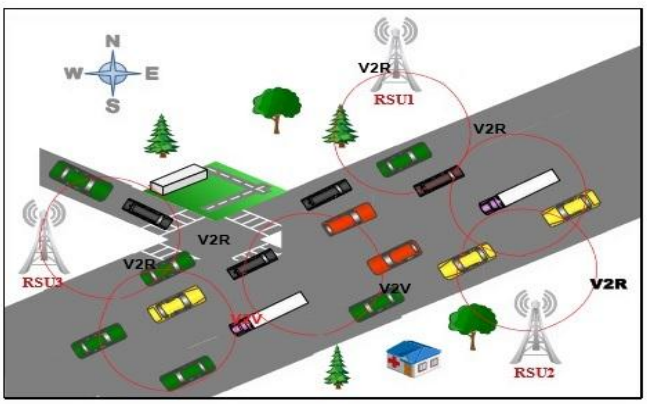

Figure 1 : VANET Structure

To improve the safety of driving the vehicles which also increase the need of security in VANET. To address the security issues in VANET Intrusion Detection Systems (IDS) is deployed inside each vehicle to detect internal and external security threats and network attacks. An intrusion detection system (IDS) is a mechanism to identify abnormal or suspicious activities on the target network. There are two main types of cyber analytics in support of Intrusion Detection Systems are misuse-based, and anomaly-based. Misuse-based technologies can only detect known types of intrusions with a large requirement of storage and anomaly-based intrusions are emerging every second. Intelligent intrusion detection methods include data mining, decision tree, support vector machine, genetic algorithm, artificial neural network and so on.

2. RELATED WORK

In recent years, automatic vehicles are widely used. All the vehicles are connected with each other through internet to transfer the information. When attacker tries to hack the information between two vehicles and may the message reach to destination after specific delay then there is possibility of accident to avoid these situations many algorithms has developed which given as: Machine learning algorithm used in Classification approach for intrusion detection in vehicle system [1] in these paper KNN (K Nearest Neighbor) and SVM (Support Vector Machine) machine learning algorithms has used to detect the different types of attacks in vehicular ad-hoc network. Both KNN and SVM used for classification and regression of data. In these paper DoS and fuzzy Attacks can identify. A multilayer Perceptron-Based Distributed Intrusion Detection System for Internet of Vehicles [2], it proposed a multilayer perceptron (MLP) neural network to detect intruders or attackers on an IoV (Internet of Vehicles) network. Results are in the form of prediction, classification reports, and confusion matrix. In these paper they can identify DoS, U2R, R2L, Probe Attacks in vehicular ad-hoc network. Intrusion Detection System for Detecting Rogue Nodes in Vehicular Ad-hoc Network [3] has proposed to detect the false information reporting is done by the rogue nodes in the network using anomaly based detection approach. To evaluate the system, Road Side Unit (RSU) has implemented within the communication ranges so that the entire test geographic region has covered. With every node, which is calculating the global parameter flow will get meta-information from RSUs in whose communication range remains the node. Hence, the anonymity of the location of the vehicle can be assured. Rogue nodes are introduced in the system and IDS is used to detect these rogue nodes. Intrusion detection using deep belief network and probabilistic neural network [4] in this paper intrusion detection system is developed only for network they use deep belief network for classification of attacks. These paper detect the attacks from network which connected to the internet. A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network [5] in this paper artificial intelligence is used and for classification of denial of service attack and distributed denial of service attack Random Forest (RF) algorithm is used. DoS, DDoS attack can detect using these algorithms. DeepVCM: A Deep Learning Based Intrusion Detection Method in VANET [6]. They implement intrusion detection system for vehicular communication model using deep learning algorithms. For feature extraction CNN (Convolutional Neural Network) algorithm is used and for classification LSTM (Long Short Term Memory) algorithm is used. In these paper they can identify the Dos, DDos, Black Hole, Wormhole and Sybil Attack. Vehicle ad-hoc network are decentralized. The VANET fully controls each node. Hence, the system is prone to attacks like misuse of the vehicular ad-hoc communication and disruption of system functionally, changing the traffic light red or green or give wrong signals to free the fastest lane on a highway, etc. Maglaras [7] combined the dynamic agents and static detection to design intrusion detection system in VANET. Deep Belief Network is a deep learning algorithm [7]. Neural networks have played an important role in many fields such as object classification and data fitting due to its powerful self-learning and adaption. Neural network has developed into a great subject since its creation and there emerging a lot of kinds of neural networks. Deep belief network uses Restricted Boltzmann Machine (RBM). RBM has a two-layer stochastic network it uses two layers namely hidden layer and visible layer. Restricted Boltzmann Machine, unsupervised learning, has the advantage of fitting the feature of the samples. So when we have an output of the hidden layer in a RBM, we can use it as the visible layer's input of another RBM. This process can be regard as further feature extraction from the extracted feature of our samples. With this kind of thought, Hinton raised Deep Belief Network. Deep Learning algorithm has attracted extensive attention worldwide. It has been used a lot in data fitting, recognition, classification and such fields. Deep learning has played an important role in Internet search engine. This is because its unsupervised learning algorithm fits Big Data of Internet quite well.

3. DEEP BELIEF NETWORK ALGORITHM

Deep belief networks are a class of deep neural networks algorithms that are modeled after the human brain, giving them a greater ability to recognize patterns and process complex information. Deep Belief Networks are a graphical representation which are essentially generative in nature i.e. it produces all possible values which can be generated for the case at hand. It is an amalgamation of probability and statistics with machine learning and neural networks. Deep Belief Networks consist of multiple layers with values, wherein there is a relation between the layers but not the values. The main aim is to help the system classify the data into different categories. Deep belief networks are algorithms that use probabilities and unsupervised learning

to produce outputs. They are composed of binary latent variables, and they contain both undirected layers and directed layers. Each layer in deep belief networks learns the entire input. In convolutional neural networks, the first layers only filter inputs for basic features, such as edges, and the later layers recombine all the simple patterns found by the previous layers. Deep belief networks, on the other hand, work globally and regulate each layer in order. Deep Belief Networks consist of multiple layers with values, wherein there is a relation between the layers but not the values. The main aim is to help the system classify the data into different categories as shown in figure3.

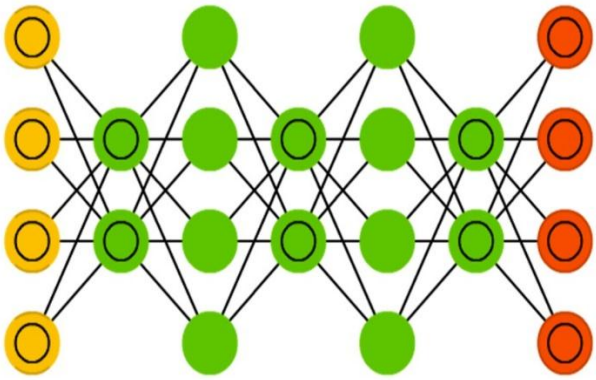

Figure2 : Deep Belief Network Architecture

Deep belief networks helped in solving problems related to inference and learning problems and to create unbiased values to be stored in leaf nodes. Deep Belief Networks are composed of unsupervised networks like RBMs. In this the invisible layer of each sub-network is the visible layer of the next. The hidden or invisible layers are not connected to each other and are conditionally independent. The probability of a joint configuration network over both visible and hidden layers depends on the joint configuration network's energy compared with the energy of all other joint configuration networks. The first step is to train a layer of properties which can obtain the input signals from the pixels directly. The next step is to treat the values of this layer as pixels and learn the features of the previously obtained features in a second hidden layer. Every time another layer of properties or features is added to the belief network, there will be an improvement in the lower bound on the log probability of the training data set.

Image Recognition, Video Recognition and Motion Capture data are the application of Deep Belief Network. Motion capture data involves tracking the movement of objects or people and also uses deep belief networks. Motion capture is tricky because a machine can quickly lose track of, for example, a vehicle and if another vehicle that looks similar enters the frame or if something obstructs their view temporarily. Motion capture thus relies not only on what an object or vehicle look like but also on velocity and distance. Motion capture is widely used in video game development and in filmmaking.

4. Dataset: CICIDS2017

In both type of vehicle communication i.e. vehicle to vehicle communication and in vehicle to infrastructure communication they use Wi-Fi network for transmitting data from source to destination, and in Wi-Fi network used some protocols that are HTTP, HTTPS, FTP, SSH, and email protocols. And this dataset build using all these protocols so we can use this dataset for VANET network. In real world it is not possible to collect the real world packet from vehicle because driverless automatic vehicles are not available. So we used CICIDS2017 dataset which is related to real world data.

CICIDS2017 dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack. Generating realistic background traffic was their top priority in building this dataset. They have used our proposed B-Profile system (Sharafaldin, et al. 2016) to profile the abstract behaviour of human interactions and generates naturalistic benign background traffic. For this dataset, they built the abstract behaviour of 25 users based on the HTTP, HTTPS, FTP, SSH, and email protocols.

The data capturing period started at 9 a.m., Monday, July 3, 2017 and ended at 5 p.m. on Friday July 7, 2017, for a total of 5 days. Monday is the normal day and only includes the benign traffic. The implemented attacks include Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS. They have been executed both morning and afternoon on Tuesday, Wednesday, Thursday and Friday.

In this dataset evaluation framework (Gharib et al., 2016), we have identified eleven criteria that are necessary for building a reliable benchmark dataset. None of the previous IDS datasets could cover all of the 11 criteria.

5. PROPOSED WORK

This proposed work used Deep Learning algorithm namely Deep Belief Network (DBN) for Intrusion Detection in Vehicular Ad-hoc Network (VANET). CICIDS2017 this dataset is used to trained the system which is related to VANET scenario. At the output there are two types binary classification and multiclass classification, binary classification gives output whether there is attack or not and in multiclass classification they gives the attack name if intrusion is detected in network.

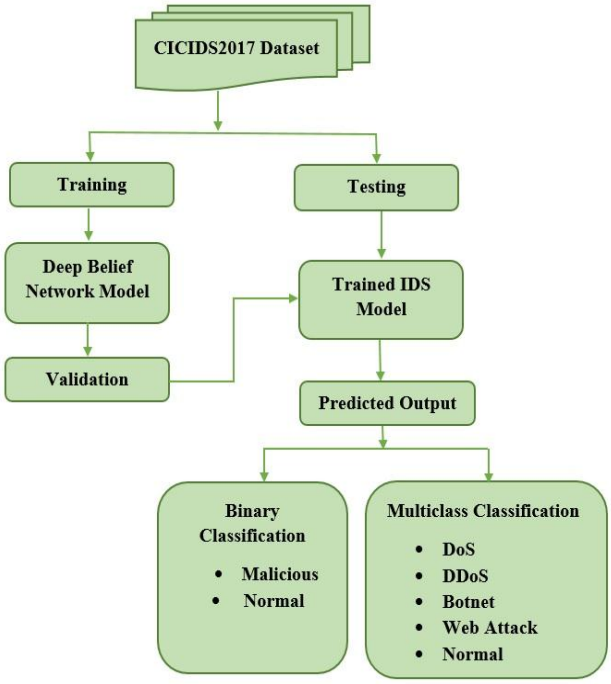

Figure 3. Block diagram of proposed work

The block diagram in "figure 3". gives a view of the proposed work:

5.1 Training/Testing Dataset

For trained the system CICIDS2017 dataset is used. These dataset is in raw format. From these dataset 60% data used for trained the data and 30% data used for testing. The ratio used for training and testing is depend on researcher and application.

5.2 Pre-processing

Pre-processing is required to convert the raw data into readable format, basically the dataset is in raw format so this step is required. Remove unnecessary data from dataset is done in this process also arrange the complete data in our format. Labelling for various attacks rearranging the attacks and feature, these steps are coming under pre-processing. These step is completely depending on the dataset and our requirement of dataset for our project. In these repeated data and unnecessary data removed from dataset and create new dataset which required for our project is done.

This data is then given as input to the feature extraction for feature selection. Some of this having no values in columns that will be eliminated, to avoided confusion in learning as well as testing.

5.3 Feature Selection / Feature Extraction:

In dataset total 78 features are given. The data set contains 78 features in addition to one feature representing the traffic category (label). By viewing some basic statistical details of those data set features, 8 features were detected to have zero values. That means those features have no effect on any calculation on the data set. Therefore, we removed them from the data set, the shape of the data set become 832,373 rows, 70 feature Columns, 1 label Column.

This label converted into two categories:

Binary Classification- (0,1); 0 = normal traffic, 1 = malicious traffic.

Multiclass classification- Attacks were assigned with real values in new field called x Attack

Features given in CICIDS2017 is given in table 1:

Feature no.	Features	Feature no.	Features
1.	Destination Port	41.	Packet Length Mean
2.	Flow Duration	42.	Packet Length Std
3.	Total Fwd Packets	43.	Packet Length Variance
4.	Total Backward Packets	44.	FIN Flag Count
5.	Total Length of Fwd Packets	45.	SYN Flag Count
6.	Total Length of Bwd Packets	46.	RST Flag Count
7.	Fwd Packet Length Max	47.	PSH Flag Count
8.	Fwd Packet Length Min	48.	ACK Flag Count
9.	Fwd Packet Length Mean	49.	URG Flag Count
10.	Fwd Packet Length Std	50.	CWE Flag Count
11.	Bwd Packet Length Max	51.	ECE Flag Count
12.	Bwd Packet Length Min	52.	Down/Up Ratio
13.	Bwd Packet Length Mean	53.	Average Packet Size
14.	Bwd Packet Length Std	54.	AvgFwd Segment Size
15.	Flow Bytes/s	55.	AvgBwd Segment Size
16.	Flow Packets/s	56.	Fwd Header Length
17.	Flow IAT Mean	57.	FwdAvg Bytes/Bulk
18.	Flow IAT Std	58.	FwdAvg Packets/Bulk
19.	Flow IAT Max	59.	FwdAvg Bulk Rate
20.	Flow IAT Min	60.	BwdAvg Bytes/Bulk
21.	Fwd IAT Total	61.	BwdAvg Packets/Bulk
22.	Fwd IAT Mean	62.	BwdAvg Bulk Rate
23.	Fwd IAT Std	63.	SubflowFwd Packets
24.	Fwd IAT Max	64.	SubflowFwd Bytes
25.	Fwd IAT Min	65.	SubflowBwd Packets
26.	Bwd IAT Total	66.	SubflowBwd Bytes
27.	Bwd IAT Mean	67.	Init_Win_bytes_forward
28.	Bwd IAT Std	68.	Init_Win_bytes_backward
29.	Bwd IAT Max	69.	act_data_pkt_fwd
30.	Bwd IAT Min	70.	min_seg_size_forward
31.	Fwd PSH Flags	71.	Active Mean
32.	Bwd PSH Flags	72.	Active Std
33.	Fwd URG Flags	73.	Active Max
34.	Bwd URG Flags	74.	Active Min
35.	Fwd Header Len	75.	Idle Mean
36.	Bwd Header Length	76.	Idle Std
37.	Fwd Packets/s	77.	Idle Max
38.	Bwd Packets/s	78.	Idle Min
39.	Min Packet Length	79.	Label
40.	Max Packet Length		

Table1 : Features of CICIDS2017 dataset

5.4 Deep Belief Network Model :

After feature selection there is a deep belief network model which trained using hidden layers and visible layers for intrusion detection dataset.

Implementing a Deep Belief Network demands training each layer of RBM. For this purpose, the units and parameters are first initialized. It is followed by two phases in Contrastive Divergence algorithm — positive and negative. In the positive phase, the binary states of the hidden layers can be obtained by calculating the probabilities of weights and visible units. Since it is increases the probability of the training data set, it is called positive phase. The negative phase decreases the probability of samples generated by the model. The greedy learning algorithm is used to train the entire Deep Belief Network. The greedy learning algorithm trains one RBM at a time and until all the RBMs have been taught.

Next step is validation, in which packets are validate for training and testing.

5.5 Predicted Output:

Once the deep belief network is trained then intrusion detection model is generated. For testing the packets whether it is normal or malicious it gives to the intrusion detection system model. The output given in two types if we select binary classification then it gives output in the form normal packet or malicious packet, and if we select multiclass classification then it gives output in the form of attack name which define in dataset.

Class Labels
BENIGN
DoS Hulk
PortScan
DDoS
DoS GoldenEye
FTP-Patator
SSH-Patator
DoS slowloris
DoS Slowhttptest
Botnet
Web Attack – Brute Force
Web Attack – XSS
Infiltration
Web Attack – Sql Injection
Heartbleed

Table2 : Name of Attacks in CICIDS2017

5.6 Performance Parameter:

To show the performance of proposed methodology confusion matrix is used. A confusion matrix is a table that is often used to describe the performance of a classification model (or "classifier") on a set of test data for which the true values are known. Each row in a confusion matrix represents an actual class, while each column represents a predicted class. The confusion matrix gives you a lot of information, such as accuracy, precision, sensitivity, specificity etc.

		Actual class	
		P	N
Predicted class	P	TP	FP
	N	FN	TN

Figure 4 : Ideal Confusion Matrix

Where: P = Positive; N = Negative; TP = True Positive; FP = False Positive; TN = True Negative; FN = False Negative.

$$Sensitivity = \frac{TP}{TP+FN} (1)$$

$$Specificity = \frac{TN}{TN+FP} (2)$$

$$F1 - Score = \frac{2TP}{TP+TN+FP+FN} (3)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} (4)$$

6. EXPERIMENTAL RESULTS

6.1 System Information:

For proposed methodology we used OS name Microsoft Windows 10 Pro, Processor Intel® Core(TM) I36006u CPU, 8GB RAM, NVIDIA Graphic Cards. Software used MATLAB 2019b.

6.2 Confusion Matrix for Binary Classification

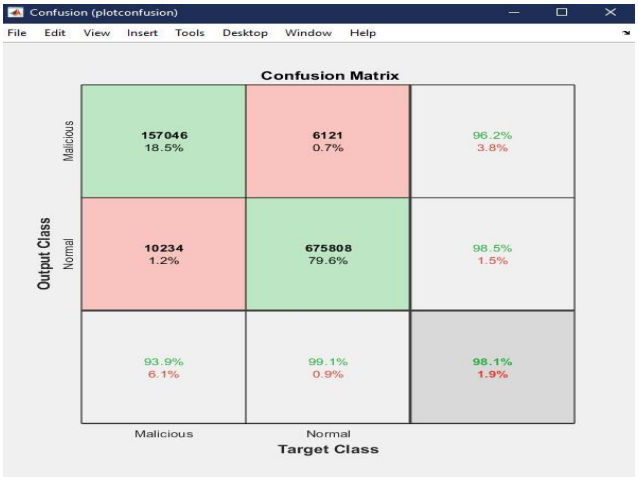

Figure 5: Confusion Matrix for Binary Classification

Parameters	Value
True Positive	157046
False Positive	10234
True Negative	675808
False Negative	6121
Accuracy	98.0741
Error Rate	1.9259
Sensitivity	93.8821
Specificity	99.1024
F-score	95.76
Positive Predictive Rate (Precision)	96.2486
Negative Predictive Rate	98.5083
Matthews correlation coefficient	93.8665

Table 3: Parameters of Binary Classification

6.3 Confusion Matrix for Multiclass Classification

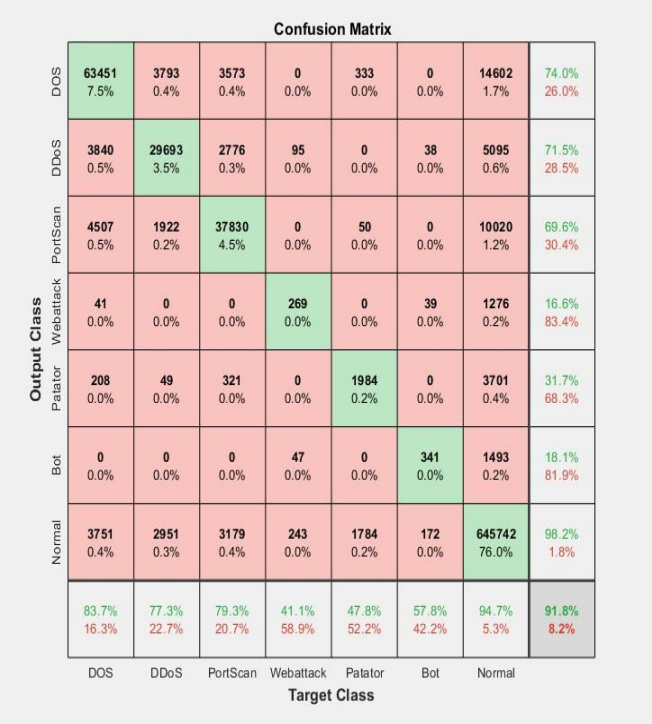

Figure 6 : Confusion Matrix for Multiclass Classification

For proposed work overall accuracy is 95.06% for multiclass classification. Specificity is 97.84%.which is better than other existing classifier.

Following Comparison Table Shows the comparison between existing methods and proposed methods:

Ref.	Accuracy	Precision	F-Measure	Recall or Sensitivity
[13]	-	0.96	0.96	0.96
[14]	95.42%	-	0.948	-
[15]		0.894	0.911	0.928
[16]	0.94	0.94	0.94	0.94
[17]	0.697	0.80	0.65	0.70
Proposed Work	98.07%	96.24%	95.76%	94.58%

Table 4: Comparative Table

7. CONCLUSION

In modern systems such as self-driving and semi self-driving vehicles, intelligent intrusion detection systems have become a vital security application. These vehicles, networks and devices are subjected to different types of attacks that have a direct effect on the development and use of self-driving vehicles. Attackers always develop new technique to hack system information and in case of VANET if the attacker hack the information or change the information then the possibility of accident are rises. To avoid the accident and provide road safety intrusion detection is needed. Intrusion Detection System use as solution to VANET security issues, effectively detects attacks by analyzing and classifying the messages in the VANET. In previous method used for intrusion detection system in VANET are developed with artificial intelligence, machine learning but the accuracy of that system is low while using deep learning algorithm the accuracy and efficiency of the intrusion detection system in VANET is increase. Because the deep learning algorithms are updated and having many features than previous algorithm, the feature extraction is automatically done in deep learning algorithm. By using an algorithm of deep learning in MATLAB software, intrusion detection can be done more effectively in vehicular ad-hoc network.

In future work for intrusion detection system in VANET used real world dataset which generated from real world driverless automated vehicles.

REFERENCES

[1] Abdulaziz Alshammari, Mohamed A. Zohdy, Debatosh Debnath, George Corser "Classification approach for intrusion detection in vehicle system", Science Research Publishing, Wireless Engineering and Technology,79-94,2018

[2] Ayesha Anzer and Mourad Elhadef "A multilayer Perceptron-Based Distributed Intrusion Detection System for Internet of Vehicles", IEEE 4th international conference on collaboration and internet computing ,438-445,2018.

[3] Sunil M. Sangve, Reena Bhati, Vidhya N. Gavalli "Intrusion Detection System for Detecting Rogue Nodes in Vehicular

Ad-hoc Network", International Conference on Data Management, Analytics and Innovation, 127-131,2017.

[4] Guangzhen Zhao, Cuixiao Zhang and Lijuan Zheng, "Intrusion Detection using Deep Belief Network and Probabilistic Neural Network", IEEE International Conference on Computational Science and Engineering and IEEE International Conference on Embedded and Ubiquitous Computing, 639-642,2017

[5] Ying Gao, Hongrui Wu, Binjie Song, Yaqia Jin, Xiongwen Luo, And Xing Zeng "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network", IEEE Access, special section on artificial intelligence – empowered intelligent transport system, 154560154571,2019.

[6] Yi Zeng, Meikang Qiu, Dan Zhu, Zhihao Xue, Jian Xiong "DeepVCM: A Deep Learning Based Intrusion Detection Method in VANET", IEEE 5th Intl Conference on Big Data Security on Cloud, 288-293,2019.

[7] Leandros A. Maglaras," A Novel Distributed Intrusion Detection System for Vehicular Ad-Hoc Network" (IJACSA) Int. Journal of Advanced Computer Science and Applications, 101-106,2015.

[8] Yuminga Hua, Junhai Guo, Hua Zhao," Deep Belief Networks and Deep Learning" IEEE, International Conference on Intelligent Computing and Internet of things, 2015.

[9] Ram Shringar Raw, Manish Kumar, Nanhay Singh "security challenges, issues and their solutions for vanet" International Journal of Network Security & Its Applications,95-105, 2013.

[10] Ujwal Parmar, Sharanjit Singh," Overview of Various Attacks in VANET", International Journal of Engineering Research and General Science,120-125,2015.

[11] Rui Xing, Zhou Su, and Yuntao Wang," Intrusion Detection in Autonomous Vehicular Networks: A Trust Assessment and Q-learning Approach", The First International Workshop on Intelligent Cloud Computing and Networking,79-83,2019.

[12] Y. Zeng, M. Qiu, Z. Ming and M. Liu, "Senior2local: A machine learning based intrusion detection method for vanets", international conference on Smart Computing and Communication, Springer, 417-426, 2018.

[13] Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. "Toward generating a new intrusion detection dataset and intrusion traffic characterization". In Proceedings of the Fourth International Conference on Information Systems Security and Privacy, ICISSP, Funchal, Madeira, Portugal, 22–24 January 2018.

[14]Watson, G. A Comparison of Header and Deep Packet Features When Detecting Network Intrusions; Technical Report; University of Maryland: College Park, MD, USA, 2018.

[15] Marir, N.; Wang, H.; Feng, G.; Li, B.; Jia, M. Distributed Abnormal Behavior Detection Approach based on Deep Belief Network and Ensemble SVM using Spark. IEEE Access 2018.

[16]AksuD.Üstebay,S.;Aydin,M.A.Atmaca,T."IntrusionDetectionwithComparative Analysis of Supervised Learning Techniques and Fisher Score Feature Selection Algorithm". In International Symposium on Computer and Information Sciences; Springer: Berlin, Germany, 2018

[17] Aksu, D.; Aydin, M.A." Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms1". In Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018.

[18] Ustebay, S.; Turgut, Z.; Aydin, M.A. "Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier". In Proceedings of the 2018.