iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5258

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

A Review on Intrusion Detection System in Vehicular Ad- hoc Network Using Deep Learning Method

Rasika S. Vitalkar[1], Samrat S. Thorat[2]
[1]*M. Tech. Student,* [2]*Assistance Professor, Department of Electronics Engg., Government College of Engineering, Amravati, Maharashtra, INDIA*

Abstract: ***In recent years, there is rapid development in smart vehicles for transmitting the information, all smart vehicles are now uses the internet services for communication. So security assurance in vehicular ad-hoc network is a crucial and challenging task due to open access medium. The main objective of VANET is to improve the safety, comfort, driving efficiency. This paper may solve the problems existing in intrusion detection in VANET using machine learning, neural network, including redundant information, large amount of data needed, etc. For proposed intrusion detection system in VANET 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.***

Keywords: Deep Belief Network, Deep learning, Intrusion Detection, Vehicular Ad-hoc network (VANET).

I. 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. There are two types of vehicle communication first is vehicle to vehicle communication 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. A VANET can be utilised to provide Peer to peer application, Internet connectivity and other services for the user apart from safety. Peer to peer applications are useful to provide services like sharing music, movies etc. among the vehicles in the network. People always want to connect with the Internet all the time, hence VANET provides the constant connectivity of the Internet to the users. VANET can be utilised in other user based application such as payment service to collect the tall taxes, to locate the fuel station, restaurant etc. The security in VANET is most critical issue because the information is propagated in open access environment. VANET's are exposed to various threats and attacks. It is necessary that all the data which is transmitted should not be changed by the attackers. So the ultimate goal of all works toward VANET is to provide road safety information among the nodes hence the frequent exchange of such type of data on the network clearly signifies the role of the security. An effective way to identify when an attack occurs in a VANET is the deployment of an Intrusion Detection System (IDS). 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. Among them, ANN has been widely used in intrusion detection system.

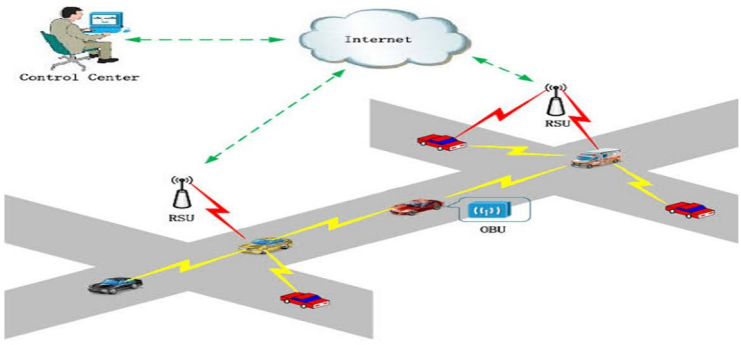


Fig.1 Structure of VANET

As shown in above diagram there is a structure of vehicular ad-hoc network, in which road side unit are connected to each vehicle also every vehicles are connected to each other. Controlling of road side unit was restricted up to some distance as clustering used in mobile communication, every cell in mobile communication contain one base station similarly in vehicle communication road side unit was assign to each area. All RSU are connected to the Internet and the control system which control every action occurred in vehicle communication such as location of vehicle, transmitting the signal from one vehicle to another vehicle or RSU, etc.

There are many types of attacks in VANET such as Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack, Sybil attack, Application attack, Timing attack, etc. To detect such types of attacks, in machine learning algorithms is difficult to train and set due to vast and complex input features required for training. Deep learning algorithms have significant attention and been widely used in various fields to improve the performance of the previous methods. Deep learning based methods can automatically extract and selects features using raw data. For proposed intrusion detection system in VANET to detect intrusion deep belief network algorithm of deep learning will use. It is an effective method of solving the problems from neural network with deep layers, such as low velocity and the overfitting phenomenon in learning. For train the system ISCX2012 dataset will use.

A. Overview Of Deep Learning

Deep learning is a new field of machine learning, which is essential a multi-layer neural network. The multilayer neural network usually has 5-10 layers or more hidden layer, which can be formed by learning a deep nonlinear network structure to combine low-level features to form a more abstract high-level representation of attribute categories or features. Neural networks played an important role in many fields such as object classification and data fitting due to its powerful self-learning and adaption. There are many algorithms used in deep learning that are convolutional neural network, recurrent neural network, long short-term memory network, deep Boltzmann machine, Deep Belief Network. Deep learning models make use of several algorithms while no one network is considered perfect same algorithms are better suited to perform specific task.

Deep Belief Network (DBN) is an unsupervised probabilistic deep learning algorithm where the network has a generative learning model. It is a mix of directed and undirected graphical network, with the top layer an undirected Raman Boltzmann Machine (RBM) and the lower layers directed downward. This enables a pre-training stage and a feed-forward network for the fine tuning stage. The DBN has multiple layers of hidden units, which are connected and the learning algorithms “greedy” from the stacked RBMs, meaning there is a one layer at a time, sequentially from the bottom observed layer. DBN has advantages such as network need small dataset, accuracy is high, training time is fairly short on GPU powered machine.

Restricted Boltzmann Machine is a two-layer network, each unit in inter-layer has a two-way connection, units within the same layer are not connected. Its structure shown in figure 2.

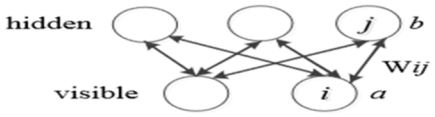


Fig. 2 Restricted Boltzmann Machine Structure

RBM is an energy model that defines the joint configuration energy:

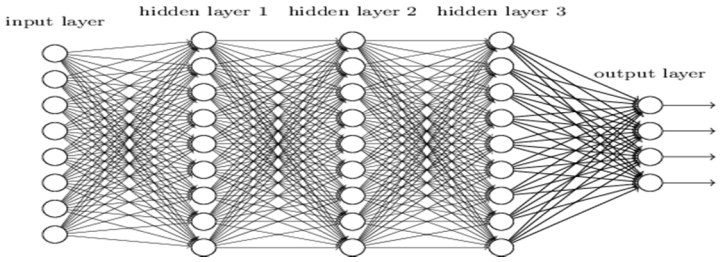


Fig.3 Structure of Deep Belief Network

DBN is a deep neural network model formed by stacking RBMs, its is a two-layer stochastic network. Its two layers are visible layer and hidden layer. 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 features. Learning of DBN is divided into pre-training and fine-tuning two parts. Pre-training is the process of unsupervised learning, starting from the first RBM input data, then the output of the first RBM as the input of the second RBM, so that training is done layer by layer until all layers trained to complete.

B. Attacks In Vanet

1) Denial of Service Attack: It is the most serious level attack in vehicular network. In this attack attacker jams the main communication medium and network is no more available to legitimate user.
2) Distributed Denial of Service Attack (DDOS Attack) : DDOS attacks are those attacks in which attacker attacks in distributed manner from different locations. Attacker may use different timeslots for sending the messages. Nature and time slot of the message can be varied from vehicle to vehicle of the attackers. The aim of attacker is same as DOS attack.
3) Sybil Attack: It is a critical attack. In this kind of attack attacker sends multiple messages to other vehicles. Each message contains different source identity. It creates confusion to other vehicles by sending wrong messages like traffic jam. So there is jam further and vehicles are forced to take another route. The main aim of the attacker is to provide an illusion of multiple vehicles to other vehicle so that vehicles can choose another route.
4) Application Attack: The main motive of attacker in this kind of attacker in this kind of attack is to content that are related to safety and non-safety related applications. Safety applications play very important role as they provide warning messages to other users. In this attack the attackers alter the contents of the actual message and send wrong messages to other users.
5) Timing Attack: The main objective of attacker is o add some time slot in the original message that creates delay in the original message and these messages are received after these requires a time. AS we know safety applications are time critical applications if delay occurs in these applications then major objective of these applications is also finished.

C. Proposed Methodology

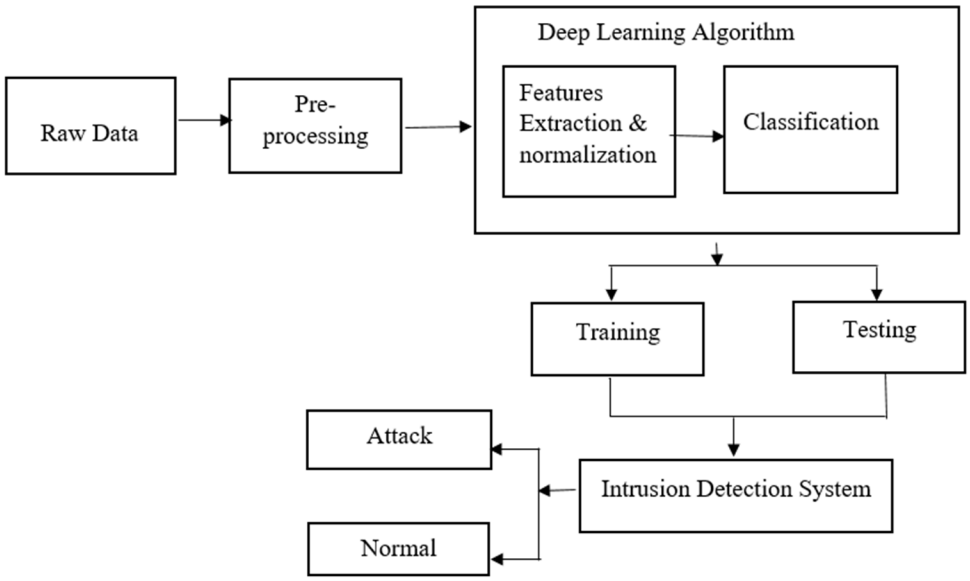


Fig. 2.: Block diagram of proposed work

The block diagram shows process of proposed methodology

1) Raw Data: The raw data contain input data and training dataset. The ISCX2012 dataset will use to train model, which contain the list of attacks. The input data is test data which will test in proposed system.
2) Pre-processing: Input data and training data will then give to the pre-processing, these block used for the process the data output of these block given as an input to the feature extraction block.
3) Feature extraction & normalization: in these block various features can be extracted from the given input data or from training dataset. In proposed methodology for feature extraction deep learning algorithm namely deep belief network is used. In deep learning algorithm feature extraction can done automatically.
4) Classification: Deep learning classifier used for the classify the input data as an attack or normal data.
5) Intrusion Detection System: This block gives output whether the input data is normal or any malicious data. For proposed methodology deep learning algorithm used, if the intrusion is detected then it gives alert to the system or vehicle.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

II. LITERATURE SURVEY

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 Neighbour) 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.

III. SUMMARIZED WORK DONE

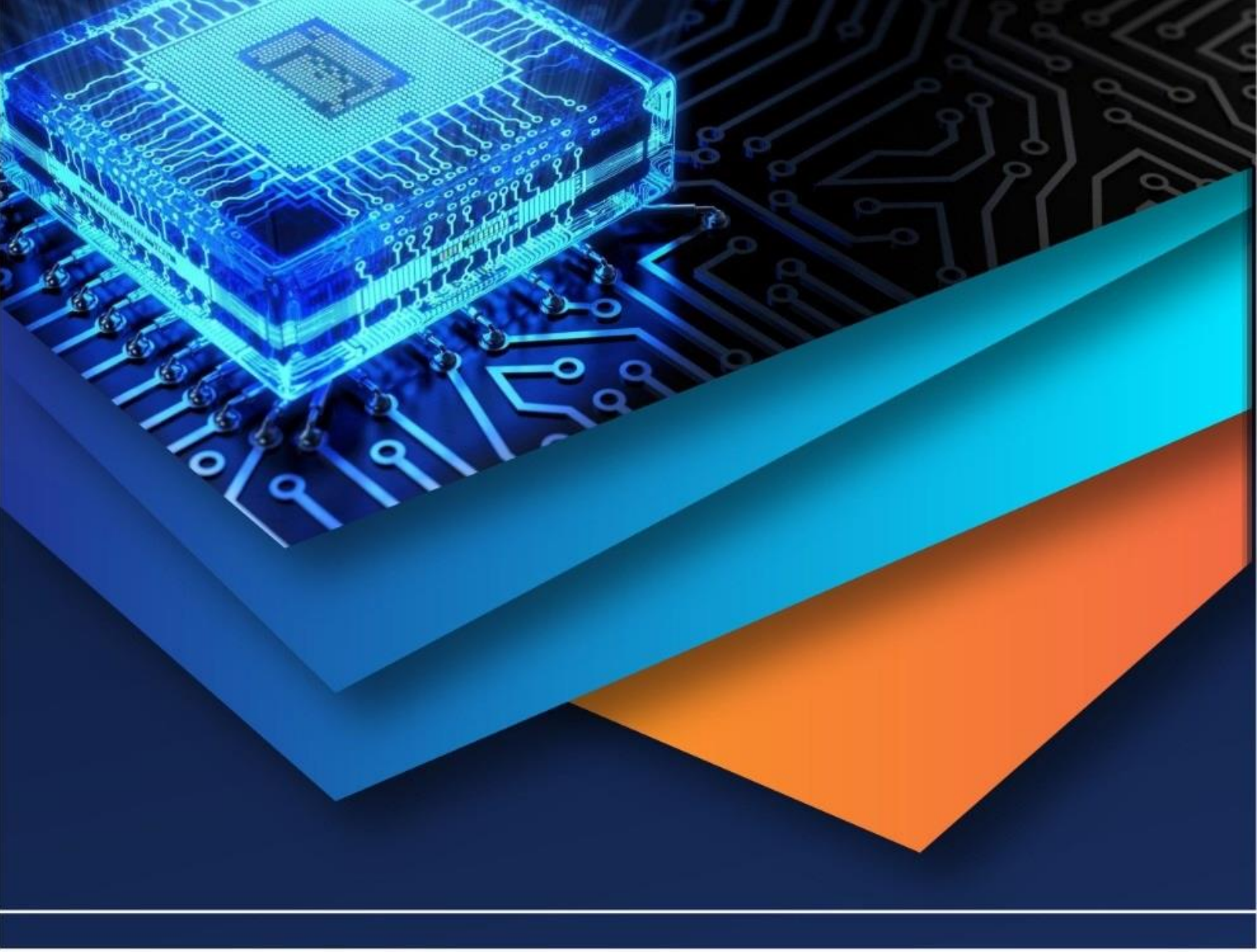
REF NO.	METHODOLOGY	RESULT
1	K Nearest Neighbor (KNN) algorithm used for classification and regression. (SVM) Support vector Machine used for detection.	Accuracy: between 80 % and 90%.
2	A multilayer Perception Algorithm is used.	Detection rate by using MLP 92%.
3	Rouge node detected by machine learning algorithm	Intrusion detection rate is 96%.
4	Deep learning Method used for detection, but detect the intrusion in network.	Accuracy rate of deep learning method in network is 95%.
5	Spark-ML-_RF based algorithm used for training, RFA used for classification & T decision tree perform classification.	Accuracy 96.05%.
6	Feature Extraction done by Convolutional Neural Network and LSTM used to learn characteristics from the time related prospective.	Accuracy is 94%.

IV. CONCLUSION

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 may 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.

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, 154560-154571,2019.
[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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY