International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

A Review on Deep Learning Based Intrusion Detection System for Vehicular Ad-Hoc Network

Rohit Pravinkumar Vedpathak[1], Sunita Babanrao Vani[2]

[1]*M.Tech. Student, Department of Computer Science and Engineering, Ashokrao Mane Group of Institutions, Kolhapur, Maharashtra, India.*
[2]*Asst. Professor, Department of Computer Science and Engineering, Ashokrao Mane Group of Institutions, Kolhapur, Maharashtra, India.*

Abstract - *The main objective of VANET is to improve safety, comfort, driving efficiency and waiting time on the road. However, it is vulnerable to various security attacks such as DOS Attack, Fuzzy Attack and Impersonation Attack, due to the lack of centralized infrastructure. This poses a serious threat to vehicle safety. In CAN bus there is no information about the source and destination address for authentication. The attacker can easily inject any message. This can lead to system faults. In this work, we propose RNN based Deep learning techniques for IDS to cluster and classify the intrusions in VANET such as Simple RNN and RNN with LSTM. The intrusion detection technique relies on the offset ratio analysis and the time interval between the messages request and also the response within the CAN. Intrusion detection plays a valuable role in ensuring information security, and thus the key technology is to accurately identify various attacks within the network. The RNN-IDS model provides a brand-new research method for intrusion detection and improves the accuracy of intrusion detection.*

***Key Words*: Intrusion Detection, IDS, Deep Learning, RNN, LSTM, VANET, Neural Networks**

1. INTRODUCTION

The rapid growth of data transfer through various devices and communication protocols has raised significant security concerns, which have increased the importance of developing advanced intrusion detection systems (IDS). In today's world, cars and other private vehicles are heavily used by many people. A crucial problem that each person has face every day is the increasing number of accidents occurred on road and this transportation safety problem continues to worse because of population growth and increase in number of vehicles in urban areas.

Vehicular Ad-hoc Network (VANET) refers to a network created in an ad-hoc manner where different moving vehicles and other connecting devices are available in contact over a wireless medium and exchange useful information to at least one another with different purposes, being the main purpose that of improving security on the road. a small network is formed simultaneously with cars and other devices that behave as a mode network. The communication system of an intelligent vehicle is usually referred to as vehicle to everything or it is also called as VANET which means Vehicular Ad-Hoc Network.

An Ordinary VANET, communication system is usually responsible for 3 main types of communication to be considered on smart automobile. Those types are vehicle to vehicle, vehicle to infrastructure and vehicle to roadside. There is major advancement in vehicle system has been made with integrating a number of computing device called ECU. Various forms of communication were developed to support communication. CAN is the simple communication protocol supporting to attach sensors and actuators with ECUs.

The Controller Area Network (CAN) is a bus communication protocol which defines a regular for reliable and efficient transmission between in-vehicle parts simultaneously. The message moves through CAN bus from one node to a different node, but it doesn't have information about the source and destination address for authentication. Thus, the attacker can easily inject any message to steer to system faults. In this work, we present IDS which is based on RNN based deep learning techniques to cluster and classify the intrusions in VANET.

2. LITERATURE SURVEY

A. Recurrent Neural Network Based Intrusion Detection System.[1]

In that, authors focus on IDS system which is classified into four layers namely, data collection, feature identification, model training and execution of the classification model. The dataset used is CICIDS2017. Authors present an efficient method to detect DDoS attacks using anomaly detection by LSTM based neural network with an accuracy of 96%. Since, there have been a lot of researches on the detection of DDoS attacks, they mostly focused on signature-based classification systems or the traffic generated during attack period. Our method uses a deep learning method that reduces the time required for the model to predict. With the increased use of the internet and new software being developed each day, the security threats have loomed on the horizon. The CICIDS2017

dataset provides large number of attacks and the features provided have contributed well in carrying out the detection mechanism. However, the dataset was divided into three phases i.e., to detect only DDoS attacks. The model, when tested on the CAIDA DDoS 2007 dataset, resulted in an accuracy of 96%. They said Also, it will be helpful to use different datasets with alternate combinations of LSTM and fully connected layers to generate better results.

B. RNN based Prediction for Network Intrusion Detection.[2]

In that, authors have aim to generate a machine learning model that predicts the next packet by analyzing industrial IoT data, and to detect abnormalities that determine whether the next packet is a normal packet or an abnormal packet using an appropriate distance measure. To do this, they created a model that predicts the next packet by learning the LSTM model, and applied a sliding window, n-gram to learn the data in the model. Then, compared the predicted packet with the actual packet to identify whether it is a normal packet or an abnormal packet. Author used cosine similarity for the final demo and performed anomaly detection technique by setting boundaries based on cosine similarity. This is better than other data mining techniques, and even higher intrusion detection performance is achieved.

C. Deep Learning Approach for Intelligent Intrusion Detection System.[3]

In that, authors have proposed a hybrid intrusion detection alert system using a highly scalable framework on commodity hardware server which has the ability to analyze network and host operations. The framework employed distributed deep learning model with DNNs for handling and analyzing very large-scale data in real-time. The DNN model was selected by carefully evaluating their performance in comparison with machine learning classifiers on various IDS datasets. In addition, features designed to be hosted and network-based in real time and used the proposed DNN model for attack and intrusion detection. The proposed expertise is able to do better than the pre-built machine learning classifier in HIDS and NIDS.

D. Classification Approach for Intrusion Detection in Vehicle Systems.[4]

In that, authors propose an intrusion detection system that determines the intrusions in vehicles. They use two algorithms based on KNN and SVM to detect the DoS and Fuzzy attacks. Through the analysis, they use two car-hacking datasets: “DoS dataset” and “fuzzy dataset”, which are provided by the Hacking and Countermeasure Research Lab (HCRL). These data sets come from real cars by connecting CAN traffic through the OBD-II port. The structure of the two data sets is similar, although they represent different types of attacks. First, they added appropriate header names to each dataset as they are unmarked with headers. Then, also removed unnecessary columns, which were the Timestamp as we do not have a time-series analysis. They removed the missing data as well. and also converted hexadecimal data into decimal format. At last, they marked the normal messages with 1 and the injected messages with 0. In classification, we used two algorithms of the most popular methods of classification: Vector Machine and K-Nearest Neighbor. First, the authors made a pre-processing for data as mentioned above. Then, extracted the features of each dataset. After that, they implemented KNN and SVM algorithms.

E. Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection.[5]

In that, authors use the Long Short Term Memory (LSTM) model for intrusion detection using the CSIC 2010 HTTP dataset. Then they compile the model utilizing an Adam optimizer, seeking an optimal solution for the binary intrusion classification problem using accuracy rate as a performance measure. Authors have found that Adam optimizer is appropriate for the LSTM RNN model in detecting intrusion. They conclude that LSTM RNN model using Adam optimizer can construct an efficient IDS binary classifier. This classifier performance is measured with an accuracy rate of 0.9944. In short, they said in future work, using LSTM Recurrent Neural Network to more recent intrusion detection datasets is very helpful.

F. Enhanced Network Anomaly Detection Based on Deep Neural Networks.[6]

In that, Intrusion detection models were proposed, implemented and trained using different deep neural network architectures including Recurrent Neural Networks, Convolutional Neural Networks and Autoencoders. These deep models were trained in the NSLKDD training dataset and were tested on both NSLKDD test datasets namely NSLKDDTest + and NSLKDDTest21. For training and evaluation of deep models, a GPU powered test-bed using keras with theano backend was employed. To make model comparisons more reliable, use standard ML IDS models with a variety of well-known divisive techniques including Extreme Learning Machine, k-NN, Decision-Tree, Random-Forest, Support Vector Machine, Naive-Bays, and QDA.

G. OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame.[7]

As modern vehicles are exposed to a new range of threats, IDS for vehicles becomes one of the most important security components. In that, they analyze the response performance of nodes to detect whether a vehicle is under attacks or not. OTIDS can successfully detect the message injection attack and impersonating node attack which can be the most dangerous attacks for vehicles. Moreover, OTIDS can find out what types of messages are injected during message injection attack, and which node is compromised during impersonating node attack. They believe their detection method contributes to enhancing vehicle security without changing the CAN protocol.

H. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks.[8]

In that, authors have proposed the RNN-IDS model not only has a strong modelling ability for intrusion detection, but also has high accuracy in both binary and multiclass categorization. Compared with traditional classification methods, such as naive bayesian, and random forest, the

performance obtains a higher accuracy rate and detection rate with a low false positive rate, especially under the multiclass classification on the NSL-KDD dataset. The model can effectively improve both the accuracy of intrusion detection and the ability to detect the intrusion type.

I. Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection.[9]

In that, authors applied the IDS classifier according to the LSTM-RNN and examined the IDS model. The authors use a deep learning approach. Deep learning achieves high-level abstractions in data through a complex architecture or composition of non-linear transformations. Therefore, they can acquire a high detection rate. In this paper, they use Long Short Term Memory (LSTM) on the Recurrent Neural Network (RNN) and then use the IDS model. For the training phase, they generated a dataset by extracting instances from KDD Cup 1999 dataset. In order to find the proper learning rate and hidden layer size, they took an experiment with changing the values. Authors train the model by using KDDCup 1999 dataset and measure the performance. Through the testing, they find an optimal hyper-parameter for LSTM-RNN and confirm the detection rate and false alarm rate. For the testing phase, they made 10 test datasets and measured the performance. By comparing it to other IDS classifiers, they found that the attacks are correctly detected by the LSTM-RNN classifier.

J. Applying Long Short Term Memory Recurrent Neural Network for Intrusion Detection.[10]

In that, authors have applied their own implementation of the LSTM recurrent neural network classifier to intrusion detection data. The results show that the LSTM classifier provides a superior performance in comparison to the results of the KDD Cup '99 challenge and as well other tested strong static classifiers. The strengths are in the detection of `dos' attacks and network probes, which both produce a distinctive time series of events. The performance on the attack classes that produce only a few events is comparable to the results of the other tested classifiers. Performance is measured in terms of mean-squared error, confusion matrix, accuracy, ROC-curve and the corresponding AUC value. And they finally conclude that LSTM is very suitable for classifying high-frequency attacks. For low-frequency attacks, the benefit of using LSTM vanishes. Although we stress that the results achieved by LSTM are very competitive. This is the first reported demonstration of the successful application of LSTM recurrent neural networks to intrusion detection.

3. CONCLUSION

The intrusion detection arena is extremely dynamic, with new findings, functions, and models being created all the time. Machine and deep learning based IDS is one of the key techniques for security. In this work, a survey of Machine Learning and Deep Learning based Intrusion Detection techniques used in IDS for vehicular ad-hoc networks and systems is presented. This work attempts to provide the researchers with the summarized but comprehensive and useful insight with a focus on intrusion detection. Hence the intrusion detection system in vehicular ad-hoc network can be successfully achieved through different technologies that involve the use of RNN and LSTM algorithms that can be clubbed with neural networks, machine learning and deep learning techniques.

4. REFERENCES

[1] S. Nayyar, S. Arora and M. Singh, "Recurrent Neural Network Based Intrusion Detection System," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0136-0140

[2] S. H. Park, H. J. Park and Y. Choi, "RNN-based Prediction for Network Intrusion Detection," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 2020, pp. 572-574.

[3] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in IEEE Access, vol. 7, pp. 41525-41550, 2019.

[4] Alshammari, A., Zohdy, M.A., Debnath, D. and Corser, G. (2018) Classification Approach for Intrusion Detection in Vehicle Systems. Wireless Engineering and Technology, 9, 79-94.

[5] S. Althubiti, W. Nick, J. Mason, X. Yuan and A. Esterline, "Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection," SoutheastCon 2018, St. Petersburg, FL, USA, 2018, pp. 1-5.

[6] S. Naseer et al., "Enhanced Network Anomaly Detection Based on Deep Neural Networks," in IEEE Access, vol. 6, pp. 48231-48246, 2018.

[7] H. Lee, S. H. Jeong and H. K. Kim, "OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, 2017, pp. 57-5709.

[8] C. Yin, Y. Zhu, J. Fei and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," in IEEE Access, vol. 5, pp. 21954-21961, 2017.

[9] J. Kim, J. Kim, H. L. Thi Thu and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea (South), 2016, pp. 1-5.

[10] Ralf C. Staudemeyer. (2015) “Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection.” IEEE Research Article - SACJ No. 56.