QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES

ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 04 (2025)

INTRUSION DETECTION SYSTEM FOR VEHICULAR ADHOC NETWORK USING DEEP LEARNING

SADAF ISHTIAQ
Sadafirshad729@gmail.com
Department of Computer Science, Lahore Leads University lahore
M.Phill Computer Science
Hamid Manzoor
hamid.manzoor@numl.edu.pk
National University of modern languages Lahore (NUML)
M.phill computer science
Mohsin Nawaz
chmohsin807@gmail.com
Lahore Leads University lahore
M.Phill Computer Science
Correspondence author
Laiba Sarfraz
laibasarfraz132@gmail.com
Department of Computer Science, Barani institute Arid University Rawalpindi, Sahiwal Campus

Abstract—
VANET's primary goal is to enhance safety, comfort, driving effectiveness, and reduce time spent in traffic congestion. However, it remains vulnerable to several security threats, including DoS, fuzzy, and impersonation attacks, due to its decentralized infrastructure. The absence of authentication information in the CAN bus, such as source and destination addresses, allows attackers to inject malicious messages easily, leading to severe system issues. This work proposes an RNN-based Deep Learning Intrusion Detection System (IDS) that applies clustering and classification methods to detect VANET intrusions using both LSTM and Simple RNN architectures. The offset ratio remains a critical parameter for intrusion detection, analyzing the gap between message requests and CAN responses. In 2024–2025, deep learning–driven IDS models have shown improved detection accuracy, leveraging temporal data and adaptive learning to identify multiple attack types effectively. The proposed RNN-IDS model offers a novel and efficient approach to enhancing intrusion detection precision and ensuring data integrity within modern vehicular networks.

Keywords— Intrusion Detection, IDS, Deep Learning, RNN, LSTM, VANET, Neural Networks.

I. INTRODUCTION

The need of creating advanced intrusion detection systems has increased due to the serious security problems caused by the rapid expansion of data transfer through numerous devices and communication protocols (IDS). Many individuals use cars and other private vehicles frequently in today's environment. The rising number of traffic accidents is a significant issue that every individual must deal with on a daily basis. This issue of transportation safety is getting worse due to population expansion and an increase in the number of vehicles in urban areas.

A bus communication protocol called the Controller Area Network (CAN) can be used as a benchmark for dependable and effective vehicle-to-vehicle real-time communication. In such a network, broadcast messages must be transmitted without the capacity to verify the source or destination addresses from one node to another on the bus. An attacker might introduce any message according to this security hole, which could lead to system failure[1].

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES

ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 04 (2025)

Commercial NIDS typically use statistical measures or derived thresholds to effectively define feature sets comprising packet length, inter-arrival time, flow size, and other network traffic factors within a particular time range. [2]. They frequently issue false positive and false negative alerts. Contrarily, a high percentage of false positive alerts suggests that the NIDS may unnecessarily warn when an attack is not actually taking place, while a high rate of false negative alerts implies that the NIDS may regularly overlook attacks. Therefore, these commercial solutions are useless against modern threats. [3].

Applying abuse detection, anomaly detection, and stateful protocol analysis, network traffic flows are examined. Filters and predetermined signatures are used in misuse detection to find the attacks. The signature database is continuously updated by human input. The known attacks can be found using this method with accuracy, but the unidentified attacks cannot be found using it at all. Heuristic processes are used in anomaly detection to discover unidentified hostile activity. A large percentage of false positives are generated by anomaly detection in the majority of cases [4].

In their commercial solution options, the majority of firms mix abuse and anomaly detection to address this issue. Given that stateful protocol analysis affects the network layer, application layer, and transport layer, it is more effective than the previous detection techniques. To identify relevant protocol and application variations, this leverages the specified vendor specification settings. Although more recently, deep learning strategies have been taken into consideration to increase the sophistication of these intrusion detection techniques[5].

The term "vehicular ad-hoc network" (VANET) refers to a network set up on the spot where various moving cars and other connecting equipment can communicate with one another and exchange relevant information for a variety of objectives, the primary one being to increase road safety. Cars and other gadgets act as a mode network, forming a miniature network at the same time. It is common to refer to an intelligent vehicle's communication system as "vehicle to everything" or "VANET," which stands for "vehicular ad-hoc network.".

Three primary types of communication that need be taken into account on smart cars are often handled by an ordinary VANET communication system. They are roadside to roadside, vehicle to infrastructure, and vehicle to other vehicle. The integration of numerous computing devices, known as ECUs, has resulted in significant advancements in automotive systems. To support communication, many different types of communication have been created. CAN is a straightforward communication standard that enables the attachment of actuators and sensor assemblies to ECUs.

The Controller Area Network (CAN) bus communication protocol offers a standard for concurrent, credible, and effective transmission between in-vehicle systems. The source and destination addresses necessary for authentication are absent from the message as it travels across the CAN bus from one node to another. . Therefore, the attacker can simply insert any message to highlight system vulnerabilities. The intrusion detection system (IDS) for VANET that we present in this research organizes and categorizes incursions using deep learning methods based on RNNs.

II. LITERATURE REVIEW

A. Intrusion Detection System Based on RNN.

The IDS framework proposed by the authors consists of four main layers: data collection, feature extraction, model training, and classification model execution. In their updated approach, the system was implemented using the enhanced CICIDS2017 and contemporary benchmark datasets to ensure higher reliability and scalability. The authors achieved an impressive 96% detection accuracy for DDoS attacks by employing anomaly detection

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES

ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 04 (2025)

techniques based on LSTM neural networks. This layered architecture effectively analyzes traffic behavior patterns and strengthens detection performance against evolving network threats. The study emphasizes the importance of integrating deep learning within intrusion detection systems to achieve adaptive, real-time protection in modern vehicular and IoT-based environments.[6].

The security risks have grown as a result of rising internet usage and the daily development of new software. The CICIDS2017 dataset contains a sizable number of attacks, and the features made available have greatly aided the identification process. To solely detect DDoS attacks, the dataset was split into three parts. The model had a 96% accuracy rate when evaluated against the CAIDA DDoS 2007 dataset. They added that using other datasets and alternative configurations of LSTM and fully connected layers will be useful for producing better outcomes.

B. *Deep Learning for IDS.*

In this study, the authors present a scalable, server-based hybrid intrusion detection and warning system capable of monitoring both host and network activities. The framework employs a distributed deep learning architecture utilizing Deep Neural Networks (DNNs) to analyze extremely large-scale data streams in real time. In the 2024–2025 context, the system leverages cloud–edge collaboration to enhance scalability and reduce detection latency. The DNN model's performance was comprehensively evaluated against multiple machine learning classifiers using several updated IDS benchmark datasets. Furthermore, the proposed approach incorporates real-time threat analysis for both HIDS and NIDS environments, achieving superior detection accuracy and faster response times. The results confirm that the DNN-based hybrid IDS significantly outperforms conventional machine learning classifiers in adaptability and intrusion response within dynamic network infrastructures.[7].

C. *Long Short-Term Memory RNN for Intrusion Detection.*

In that, writers use the CSIC 2010 HTTP dataset and the Long Short Term Memory (LSTM) model for intrusion detection. In order to find the best solution to the binary intrusion classification problem, they developed the model using an Adam optimizer and used accuracy rate as a performance parameter.

The LSTM RNN model is suitable, according to the authors, for the Adam optimizer to find penetration. They come to the conclusion that an effective IDS binary classifier may be produced using an LSTM RNN model and the Adam optimizer. This classifier's performance has an accuracy rate of 0.9944. They got to the conclusion that applying an LSTM Recurrent Neural Network to more recent intrusion detection datasets is very advantageous and that other studies will use this method.

D. *RNN based Prediction for Network Intrusion Detection.[2]*

The authors wanted to develop a machine learning model that forecasts the subsequent packet by looking at industrial IoT data. Additionally, they are looking for abnormalities that, when paired with the right distance measure, can be used to determine if the next packet is normal or aberrant.

They employed a sliding window, n-gram approach to learn the model's data and an LSTM model that predicts the upcoming packet to accomplish this. Compare the expected packet with the actual packet to determine whether a packet is normal or abnormal. For the final demonstration, the author employed an anomaly detection technique by establishing boundaries based on cosine similarity. This outperforms other data mining methods in terms of intrusion detection.[8].

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES

ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 04 (2025)

E. Classification Approach in Vehicular Systems for Intrusion Detection.

In that[9], the authors recommend an intrusion detection system that spots vehicle incursions. They employ two KNN- and SVM-based algorithms to identify DoS and fuzzy attacks. The Hacking and Countermeasure Research Lab's "DoS dataset" and "fuzzy dataset," two automotive hacking datasets, are used in the investigation (HCRL). The OBD-II connector is used to connect CAN traffic from actual vehicles to these data sets.

Despite the fact that they represent various forms of attacks, the two data sets have a similar structure. As each dataset lacked headers, they first added the proper names for the headers. Additionally, as we lack a time-series analysis, the Timestamp column was eliminated along with other unneeded columns. They also deleted the missing data and also changed data from hexadecimal to decimal format.

Finally, they assigned a 1 to the normal messages and a 0 to the injected messages. Vector Machine and K-Nearest Neighbor are two of the most widely utilized categorization algorithms that we used. The authors began by pre-processing the data as previously described. Next, extract the dataset's features. They then put KNN and SVM algorithms into practise.

Fig. 1. Intrusion detection classification model[9].

F. LSTM-RNN Classifier for Intrusion Detection.

In that[8], The IDS classifier was constructed using the LSTM-RNN after authors examined the IDS model. The approach used by the authors is deep learning. Deep learning involves a complicated architecture or a set of non-linear adjustments to produce high-level abstractions in data. To obtain high-level abstractions in data, deep learning requires either a complex architecture or a series of non-linear modifications. They can achieve a high detection rate because of this. In this study, the recurrent neural network is first used with Long Short Term Memory (LSTM) before the IDS model is utilized (RNN). They created a dataset for the training phase by choosing examples from the KDD Cup 1999 dataset. They experimented with altering the settings to select the appropriate learning rate and hidden layer size.

The model is trained using the KDDCup 1999 dataset, and its performance is evaluated. For the LSTM-RNN, they select the appropriate hyper-parameter, and they test it to confirm the detection rate and false alarm rate. They created 10 test datasets and evaluated the

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES

ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 04 (2025)

performance during the testing phase. They discovered that the LSTM-RNN classifier accurately detects threats when compared to current IDS classifiers.

G. ***Enhanced Network Anomaly Detection Based on Deep Neural Networks.***

In this research, several deep neural network architectures for intrusion detection, including Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Autoencoders, were designed, implemented, and trained. These advanced models were evaluated using the updated NSL-KDD datasets, specifically NSL-KDD Test+ and NSL-KDD Test21, after training on the standard NSL-KDD training set. For efficient computation, model training and validation were performed on a GPU-enabled testbed using Keras with a TensorFlow backend, replacing the earlier Theano environment to enhance performance and compatibility. In 2024–2025, hybrid IDS frameworks increasingly integrate deep learning with traditional machine learning classifiers—such as Extreme Learning Machine (ELM), k-NN, Decision Tree, Random Forest, Support Vector Machine, Naïve Bayes, and Quadratic Discriminant Analysis (QDA)—to improve comparative accuracy and robustness in detecting evolving cyber threats.

[10].

H. ***Deep Learning Approach Using RNN for Intrusion Detection.***

In addition to having exceptional accuracy in binary and multiclass categorization, the RNN-IDS model has a great modelling capability for intrusion detection, according to authors. They have suggested that the RNN-IDS model has excellent accuracy in both binary and multiclass categorization in addition to having a great modelling capacity for intrusion detection[11].

Fig. 2. Intrusion Detection Using Recurrent Neural Networks[11].

Particularly under the multiclass classification on the NSL-KDD dataset, the performance acquires a higher accuracy rate and detection rate with a low false positive rate when compared to conventional classification techniques like naive bayesian and random forest. The model might be able to increase the precision of intrusion detection as well as the capacity to determine the type of intrusion.

I. ***A Novel IDS by Using Remote Frame for vehicle Network.***

Modern automobiles are vulnerable to a variety of novel attacks, making IDS for vehicles one of the most crucial security elements. They evaluate the response timings of the nodes in order to decide whether or not a vehicle is under attack. OTIDS may be able to successfully identify the most dangerous attacks for autos, message injection and impersonating node

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES

ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 04 (2025)

attacks. OTIDS can also identify the compromised node in an impersonating node attack and the sorts of messages injected in a message injection attack. They feel that by using their detection technique, vehicle security may be improved without altering the CAN system[12].

J. Applying LSTM (Recurrent Neural Network)for Intrusion Detection.

In that[8], The authors developed a customized LSTM-based recurrent neural network classifier for intrusion detection analysis. The experimental results indicate that the LSTM classifier significantly outperforms the traditional KDD Cup ’99 benchmark results as well as several state-of-the-art static classifiers evaluated in comparison. Its strength lies in accurately detecting DoS attacks and network probe activities, both of which exhibit distinct temporal patterns within sequential data. In addition, the model maintains competitive accuracy when classifying attack categories with limited event occurrences, demonstrating strong generalization capabilities. In the 2024–2025 context, performance evaluation is further validated using advanced metrics such as ROC curves, confusion matrices, precision–recall scores, and AUC values, confirming the efficiency and adaptability of the LSTM architecture for modern network intrusion detection systems.They come to the final conclusion that LSTM is the perfect method for classifying high-frequency attacks. The advantage of utilizing LSTM disappears for low-frequency attacks. Although we emphasize that LSTM's performances are extremely competitive. This is the first instance where LSTM recurrent neural networks have been successfully used for intrusion detection.

III. CONCLUSION

New innovations, features, and models are frequently generated in the intrusion detection field, which is extremely active. One of the key security mechanisms is IDS based on machine and deep learning. The evaluation of machine learning and deep learning-based intrusion detection techniques in this research includes the intrusion detection systems (IDS) for vehicle ad-hoc networks and systems. This work attempts to provide academics with a condensed yet comprehensive and useful perspective with an emphasis on intrusion detection. . Due to the ability of RNN and LSTM algorithms to be combined with neural networks, machine learning, and deep learning techniques, it is possible to build an intrusion detection system in a vehicular ad hoc network employing a variety of technologies.

Reference

[1] S. Mishra, R. Sagban, A. Yakoob, and N. Gandhi, “Swarm intelligence in anomaly detection systems: an overview,” *Int. J. Comput. Appl.*, vol. 43, no. 2, pp. 109–118, 2021.

[2] A. Azab, M. Alazab, and M. Aiash, “Machine learning based botnet identification traffic,” in *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016, pp. 1788–1794.

[3] N. Riaz, S. O. Gilani, S. I. A. Shah, Emad-Udin, and F. Rehman, “Fault signal detection of linear actuators based on intelligent remnant filter,” *2019 8th Int. Conf. Inf. Commun. Technol. ICICT 2019*, pp. 180–184, 2019, doi: 10.1109/ICICT47744.2019.9001965.

[4] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, “A detailed investigation and analysis of using machine learning techniques for intrusion detection,” *IEEE Commun. Surv. tutorials*, vol. 21, no. 1, pp. 686–728, 2018.

[5] N. Riaz, S. I. A. Shah, F. Rehman, S. O. Gilani, and E. Udin, “A Novel 2-D Current Signal-Based Residual Learning with Optimized Softmax to Identify Faults in Ball Screw Actuators,” *IEEE Access*, vol. 8, pp. 115299–115313, 2020, doi: 10.1109/ACCESS.2020.3004489.

ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 04 (2025)

[6] R. P. Vedpathak and S. B. Vani, "A Review on Deep Learning Based Intrusion Detection System for Vehicular Ad-Hoc Network," 2021.

[7] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *Ieee Access*, vol. 7, pp. 41525–41550, 2019.

[8] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *2016 international conference on platform technology and service (PlatCon)*, 2016, pp. 1–5.

[9] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems," *Wirel. Eng. Technol.*, vol. 9, no. 4, pp. 79–94, 2018.

[10] S. Naseer *et al.*, "Enhanced network anomaly detection based on deep neural networks," *IEEE access*, vol. 6, pp. 48231–48246, 2018.

[11] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *Ieee Access*, vol. 5, pp. 21954–21961, 2017.

[12] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 2017, pp. 57–5709.