International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 13 Issue 06 June 2026

An Intelligent Deep Learning Approach for Intrusion Detection in AODV-Based Mobile Ad Hoc Networks

Harsh[1], Mohit Jain[2]
Research Scholar[1], HOD CSE[2]
harshkhatarkar7828@gmail.com[1], bmctmohitcs@gmail.com[2]

Abstract: *The Ad hoc On-Demand Distance Vector (AODV) routing protocol can be hurt by blackhole attacks and flooding attacks. Most of the time, these two types of routing attacks are linked to two major bad behaviors: flooding with fake Route Replies (RREPs) and fake Route Requests (RREQs). In this paper, we come up with a new way to use dynamic machine learning to find attacks in the AODV system. By looking at the Hello, RREQ, and RREP packets in the AODV routing protocol, the proposed solution mostly figures out three different things. Then, a mathematical model for the dynamic learning algorithm is made based on these features. After that, we make the training set of data and use these features to set a threshold for our machine learning model. This set of training data only works for N time slots, which is considered one iteration. In the next iterations, it will update the most recent valid results from the dynamic learning model and figure out a new threshold for the model. Routing attacks will have distressing effects over the network and bequest a significant challenge once planning strong security mechanisms for vehicular communication. In this paper, we examine the effect and malicious activities of a number of the foremost common attacks and also mention some security schemes against some major attacks in VANET. The attacker's aim is only to modify the actual route or provides the false data about the route to the sender and also some attackers are only flooding unwanted packets to consume resources in available network. Various routing approaches are also mentioned in the paper because the routing of data is very important to deliver the traffic information to leading vehicles. It's advised that a number of the ways that to approach this made field of analysis issues in VANET might be to fastidiously design new secure routing protocols in which attacks are often rendered meaningless and because of the inherent constraints found in the network, there's a desire for light-weight and sturdy security mechanism.*

Keywords: *AODV, Intrusion Detection, Wireless network, VANET, Routing Protocol.*

1. INTRODUCTION

Smart meter networks are the major components of the smart grid, which are composed of smart meters and Data Aggregation Points (DAPs) [1]. A smart meter is an electronic device that is installed at houses or commercial sites to record consumption of electric energy and communicates that information back to the utility for monitoring and billing. Each smart meter equipped with network radio can transmit meter reading periodically or on request by utilities. DAPs are responsible for communicating information or data between smart meters and the utility company. Since a smart meter network is essentially a multi-hop network, this means some smart meters serve as relay nodes to deliver information to the DAP through multiple hops. Similar to a typical multi-hop network, multiple routes exist in a smart meter network. In other words, there is more than one path between a smart meter and its associated DAP. Therefore, a routing protocol is required to find the appropriate route to DAPs for each smart meter. In recent years, Ad hoc On-Demand Distance Vector (AODV) routing protocol is recommended for smart meter networks because it meets both the requirements of on-demand and periodic operations. However, the AODV routing protocol is

vulnerable to different types of routing attacks. One typical routing attack is the denial of service including blackhole attack and flooding attack. In a blackhole attack, attackers broadcast numerous fake Route Replies (RREPs) with a tampered highest sequence number and minimum hop count. If these fake replies are accepted by other smart meters, blackholes will be created in a smart meter network. Consequently, legitimate data cannot be sent to DAPs. In a flooding attack, attackers broadcast Route Requests (RREQ) packages throughout the network. The entire network keeps busy to forward those fake RREQ packets. Under this attack, the data transmission can be delayed, corrupted, or even blocked. Therefore, how to effectively conduct routing attack detection and detect malicious meters in a smart meter network remains a critical challenge. There are two problems in the existing work for AODV routing attack detections. The first problem is that the majority of work usually focuses on specific and known routing attacks, e.g., blackhole and flooding detection. It is known that different types of attacks exhibit distinctly. Most approaches detect malicious behaviors by targeting specific anomalous behaviors by adding new control packets to routing protocols. These approaches are not able to detect other types of attacks if present. The second problem is that a constant threshold is commonly used for detection. If an attacker is able to estimate the threshold, it can easily break the intrusion detection system and utilize the routing information to access data packets [2].

In this paper, we introduce a novel dynamic deep learning approach. First, we analyze the complete AODV routing packets including Hello, RREQ, and RREP control packets. Based on this analysis, we obtain three distinct features in the AODV routing protocol. Afterward, these features are utilized to develop a mathematical model of dynamic learning algorithm. Concurrently, these features are also considered in our machine learning model to correlate with the testing data as well as to generate an initial training set of data and a threshold. Every training set of data is only valid for N time slots, which is considered as one iteration. During this N time slots, our dynamic learning model will create new data points, which will be updated in the training set of data and be utilized to determine a new threshold for the next iteration. Therefore, during every N slot 3 intervals, the training data set will be updated based on the current state of the smart meter network and create a new threshold to detect malicious behaviors. The most promising part is that our proposed machine learning model updates parameters according to the changes of malicious behaviors, which achieves high detection accuracy. The main contributions of this research are summarized below: First, we develop formulas by analyzing AODV routing packets including Hello, RREQ, and RREP control packets. Leveraged by our proposed formulas, we obtain three distinct features including average one-hop neighbor distance, the dynamic range of sequence number, and the minimum hop count to analyze entire AODV routing packets. Second, we derive a mathematical model for dynamic learning algorithm using the three identified features. Initially, these features are placed in a three-dimensional vector space. Therefore, it determines the N number of vectors for N time slots where all of them are considered in the first iteration. Then, we calculate the mean vector from N time slots. Finally, we find out the variance between input sample data and mean vector. If this variance is lower or equal to the current threshold, the input sample data will be considered as normal traffic. This data will be further forwarded to the training model in order to estimate a new threshold for the next iteration[3].

Anomaly Intrusion Detection-Network inspired by nervous system has become an interesting tool in the applications of Intrusion Detection Systems. It supports an ideal specification of an Intrusion Detection System and is a solution to the problems of traditional IDSs [4] Anomaly-Based detectors try to figure out what the "normal" behavior of the system to be protected is and sound an alarm when the difference between an observation at a given time and the normal behavior is more than a certain amount [5]. These profiles are made from data that has been collected over time as part of normal operations.

The detectors take information from the events and use a variety of methods to figure out when the activity being watched isn't like it usually is [6]. But because of the assumptions that are used to make anomaly detection mechanisms work, they tend to have a very high rate of false alarms. In particular, the main reasons for this limitation are that the user's normal behavior model is based on data collected over a period of normal operations and that intrusive activities missed during this period are likely to be considered normal behaviors. Also, it's hard for anomaly detection techniques to find stealthy attacks because they tend to be hidden in a large number of normal behaviors.

Also, security experts usually decide on the kinds of parameters that go into normal models. If you make a mistake when setting these parameters, the number of false alarms will go up, and the anomaly detection system will not work as well. Because of this, two of the most important open questions in anomaly detection are the design of the detection methods and the choice of the system or network features to be watched.

Deep Learning in Intrusion Detection-In the past few years, security researchers have paid more attention to how

deep learning can be used in different fields. IDS are one way to improve the security of networks and systems. Anomaly intrusion detection has started to use neural networks because they are flexible and can adapt to changes in the environment. This method of detection has been used to make profiles of users, figure out what the next command will be based on what has come before, and figure out when traffic patterns are acting in an annoying way.

The main difference between shallow learning and deep learning is that deep learning has more hidden layers in its design. The first few layers of a deep neural network can do feature selection. This lets deep learning pull out advanced features so that high-level concepts can be learned, making up for the flaws of machine learning algorithms. Deep learning can also be broken down based on how the techniques can be used: 1) Deep networks for unsupervised learning (2) Deep networks for learning with help.

2. RELATED WORKS

Overview of AODV- AODV is a popular reactive routing protocol in which a node only starts the process of finding a path to the destination when it wants to send data. When the source node (NS) wants to talk to the destination node (ND) but hasn't already found a way to get there, NS starts the route discovery process by sending out a route request (RREQ) packet with the destination address. The nodes that get the packet will then send it to other nodes. When ND gets the packet, it sends a route reply packet (RREP) back to the source node. Flooding Attacks on AODV Once a route has been found, HELLO and RERR packets can be used to keep track of its status. Flooding attacks are a type of Denial of Service attack in which malicious nodes send out false packets into the network to use up all of the network's resources and make it hard to use. Fooding attacks can be put into three groups based on the type of packet used to feed the network: RREQ, DATA, and HELLO fooding attacks.

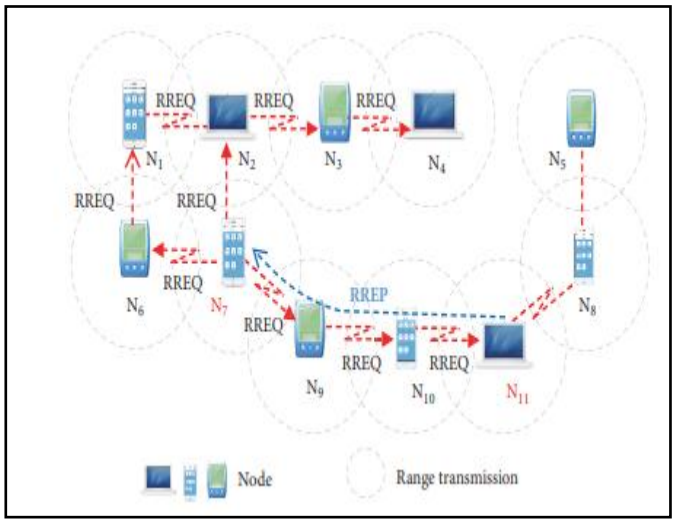

Figure 1:- Attack detection in network

In RREQ fooding attack, a malicious node continuously and excessively broadcasts fake RREQ packets, which causes a broadcast storm and food. In MANET, the RREQ flooding attack is thought to be the most dangerous because it can stop the route discovery process by using up all the bandwidth and processing power of the nodes that are attacked. In a DATA fooding attack, a bad node can send too many data packets to all the other nodes in the network. This kind of attack has a bigger effect on the nodes that help send data to its destinations. In a HELLO flooding attack, nodes send out HELLO packets to let their neighbors know they are there. A bad node could use this feature to send out too many HELLO packets, forcing its neighbors to use their resources to process packets that don't need to be processed. This type only hurts the nodes that are close to a malicious node[7-10].

This paper by **Abhinav Singhal et al. from 2021** explains how to build an Intrusion Detection System for a Network Interface Device. This research has led to the creation of a hybrid intrusion detection system that uses both machine learning and inference detection to compare the two. It is explained in two parts: the training phase (which includes model training and building an inference network) and the detection phase (Working phase). This is meant to solve all of the problems that machine learning algorithms have in the real world. Since machine learning techniques are rigid, they each have their own classification region outside of which they stop working. The goal of this paper is to show which of the many machine learning techniques used works best. Decision Tree, Naive Bayes, K-Nearest Neighbors (KNN), and Support Vector Machines (SVM), along with the NSLKDD dataset for testing and training our Network

Intrusion Detection Model, are the machine learning techniques used in comparative analysis. When tested on their own, the accuracy of Decision Tree, Naive Bayes, K-Nearest Neighbors (KNN), and Support Vector Machines (SVM) is 98.088%, 82.971%, 95.751%, and 81.971%, respectively. When tested with an inference detection model, the accuracy is 98.554%, 66.687%, 97.605%, and 93.914%. So, we can say that our inference detection model helps improve some things that aren't picked up by traditional machine learning techniques.

Toya Acharya et al., 2021 say that internet-based services led the global revolution with exponential growth, but security breaches have led to the loss of personal digital assets, which shows the need for a complete cyber security solution. Signature-based network intrusion detection has been used for a long time to tell the difference between normal and unusual traffic on a network, but it can't find a zero-day attack. Among the known NIDS methods to get around the shortcoming, the machine learning-based approach is appealing because it can analyze large amounts of network traffic data quickly and find zero-day attacks quickly. The NIDS dataset isn't balanced, so it doesn't improve performance in real-world implementation scenarios. By making a new target class out of fewer target classes, the NIDS becomes more balanced and the performance of the classifier gets better. In this paper, we show the effectiveness of several machine learning algorithms, such as Random forest (RF), J48, Nave Bayes, Bayesian Network, Bagging, AdaBoost, and Support Vector Machine (SVM), using network logs traffic (KDD99, UNSW-NB15, and CIC-IDS2017) and WEKA. This paper looked at how changing the number of output classes of publicly available network intrusion datasets affected sensitivity (True Positive Rate), false positive rate (FPR), area under the ROC curve (AUC), and wrongly identified percentage. As strongly correlated features have been added to the target classes, these classifiers have become more accurate. The results of the experiments show that the performance of machine learning classifiers got better as the number of target classes got smaller. The performance of the classifiers goes up when a highly correlated feature is added to the output class.

Chung-Ming Ou et al. (2019) propose an adaptable agent-based IDS (AAIDS) that is based on the danger theory of the artificial immune system. The way AAIDS learns is based on how dendritic cells (DC) in the immune system recognize and sort signals of danger. AG agent, DC agent, and TC agent work together to respond directly to system calls instead of looking at network packets. Simulations show that AAIDS can figure out how a system will behave in several critical situations where packet analysis is not useful.

3. PROPOSED MODEL

This study suggests that simulation be used to model common communication situations that could be attacked. The proposed system is based on a distributed and cooperative architecture, in which each node uses an IDS agent to find and isolate the one that is acting up. There are four parts to each IDS agent. The first is the data collection module, which is in charge of gathering data and figuring out where each node comes from and where it goes. The second module is the one that looks for intrusions. It uses the information given by the module before it and the threshold value to find monitoring nodes that are acting in a bad way. The third module is the voting module, which is in charge of detection approval. Before isolating a node for bad behavior, a node must get approval from the other nodes of the network. The fourth module is the intrusion response module, which is in charge of separating the misbehaving nodes based on how the voting module turned out.

this module's main job is to use information from a data collection module to find the bad nodes in the network. The module figures out which nodes are bad by figuring out the right threshold. In this case, the threshold value is a key part of how the nodes are looked at. Then it realizes that the network may have one or more nodes that are bad. The intrusion detection module shouldn't immediately label the suspicious nodes as bad once it finds them.

Deep Learning (ML) has become a popular and useful way to solve problems in a wide range of application domains. One important area of application is vehicular networks, where ML-based approaches have been found to be very helpful in solving many problems. Since wireless communication is used between vehicle nodes and/or infrastructure, it can be attacked in a number of ways. In this way, ML and its variations are becoming more popular to find attacks and deal with different kinds of security problems in vehicular communication.

Deep learning was used to build the proposed model, which is based on a hierarchical IDS model that uses the ResNet50 algorithm to improve the accuracy and performance of intrusion detection in VANET through a learning process that looks for things that don't make sense. At the time of transmission, traffic congestion and collisions, as well as problems with exposed and hidden terminals, can make it hard to send packets or cause them to be dropped or delayed. In the VANET environment, this will lead to false alarms because a normal node pattern could be mistaken for something bad. To avoid this problem and deal with the fact that the network topology is always changing and that nodes can move around, a machine learning system called "decision

trees" is used. Here are the most important parts of our model, whose flowchart is shown in Fig. 2.

4. NETWORK MODEL

In VANET [10], there are three groups of network artifacts. There are servers for applications and authorization, roadside facilities, and nodes/vehicles in these groups.

Application Servers and Authorization Servers are powerful workstations that are in charge of managing and giving out service data, respectively. The authority knows where all the keys are and is in charge of planning for maintenance. For cars, device servers give information about how they work. They will be paid for by the government or by foreign companies. We assume that the authorization and application servers can handle a lot of work. So, we didn't count computation time here.

Infrastructure on the side of the road: Road infrastructure includes the power supplies that are near roads and are in charge of collecting and sharing data. RSUs are connected to power and vehicles via radio through wired networks.

Nodes/Vehicles: Nodes or vehicles move around on the road and talk to the RSU or exchange information. The RSU gets this information from the network. Every vehicle is thought to have a differential GPS receiver with meter-order accuracy and an on-board computer (OBU) [11] that handles all communication and computing tasks.

Initial Parameters

- Num of Nodes=100;
- Source node =10;
- Destination node=20;
- data rate=8 % packets/sec
- city size=100
- Range=20
- breadth = 0
- define attack node
- intrution_node=14
- amount of Energy consumption per bit in the transmitter or receiver circuitry = Elec=50e-9; %
- Amount of energy consumption for multipath fading =Emp=0.0015e-12;%
- Data aggregation energy =EDA=5e-9; %.
- parameters for energy calculation using ratio model of message transmission

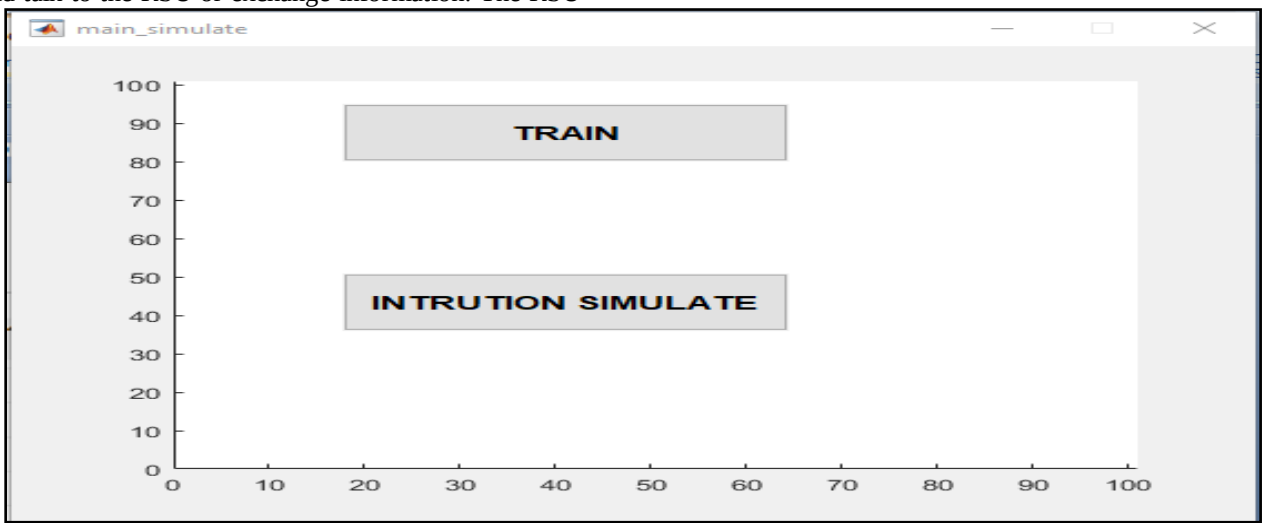

Figure 2:- Training and Simulation Window

Figure 2 presents the MATLAB Graphical User Interface (GUI) developed for the proposed intrusion detection system. The interface provides two main functions: TRAIN, which loads the dataset, preprocesses the data, and trains the detection model, and INTRUSION SIMULATE, which evaluates the trained model using simulated network attack scenarios. The GUI offers a simple and efficient platform for executing the complete intrusion detection workflow, from model training to attack simulation and performance evaluation.

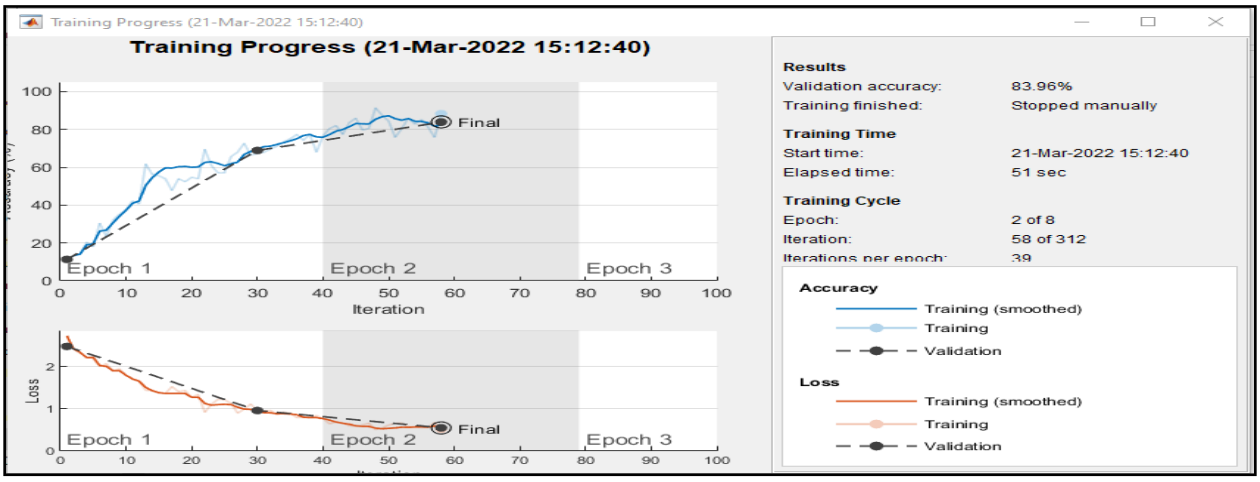

Figure 3:- Training Process Window

Figure 3 illustrates the training progress of the proposed intrusion detection model in MATLAB. The upper plot shows the improvement in training and validation accuracy with increasing iterations, while the lower plot presents the corresponding training and validation loss, which decreases as the model converges. The results indicate that the model achieves stable learning with a validation accuracy of 83.96% after 2 training epochs, demonstrating effective convergence and reliable classification performance.

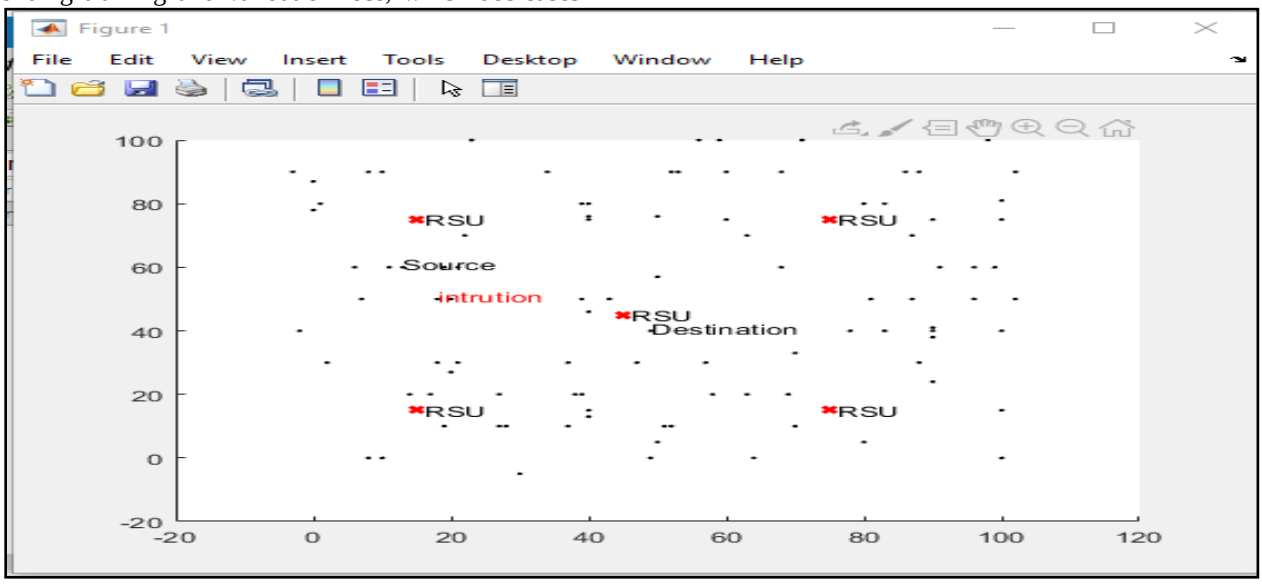

Figure 4:- Network Architecture

Figure 4 depicts the simulated vehicular network environment used for intrusion detection. The network consists of multiple Road Side Units (RSUs), a source node, a destination node, and randomly distributed vehicles. An intrusion node is introduced between the source and destination to emulate a malicious attack scenario. This simulation environment provides the basis for evaluating the proposed intrusion detection model under realistic communication conditions and analyzing its ability to identify malicious activities within the network.

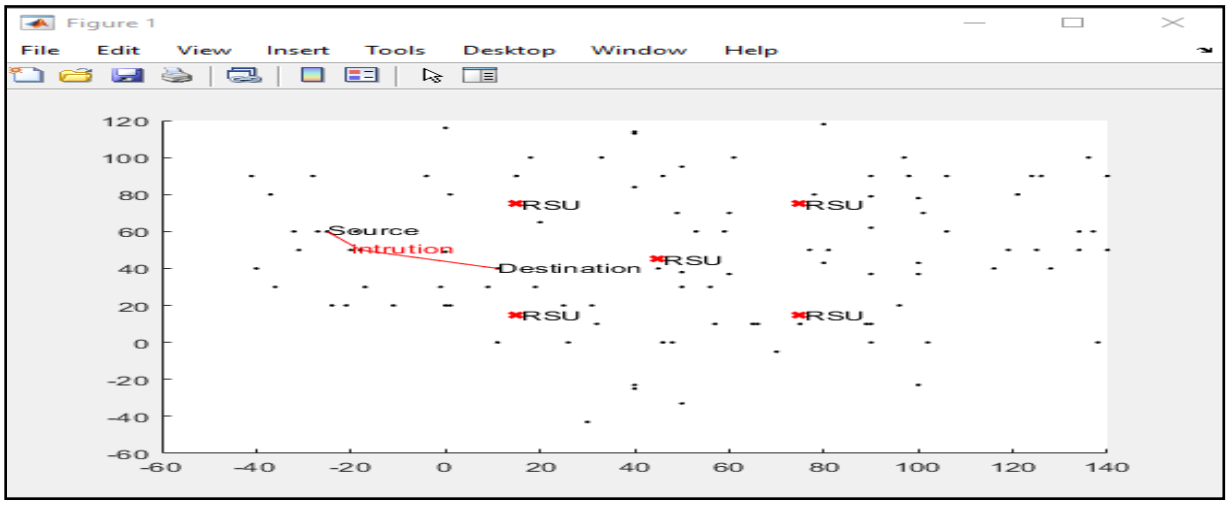

Figure 5:- Network Architecture

Figure 5 illustrates the communication scenario after introducing an intrusion into the vehicular network. A malicious node intercepts the communication path between the source and destination, while multiple Road Side Units (RSUs) are deployed to support network communication. The intrusion disrupts the direct transmission, creating an attack scenario that is used to evaluate the effectiveness of the proposed intrusion detection model in identifying malicious activities and maintaining secure data transmission.

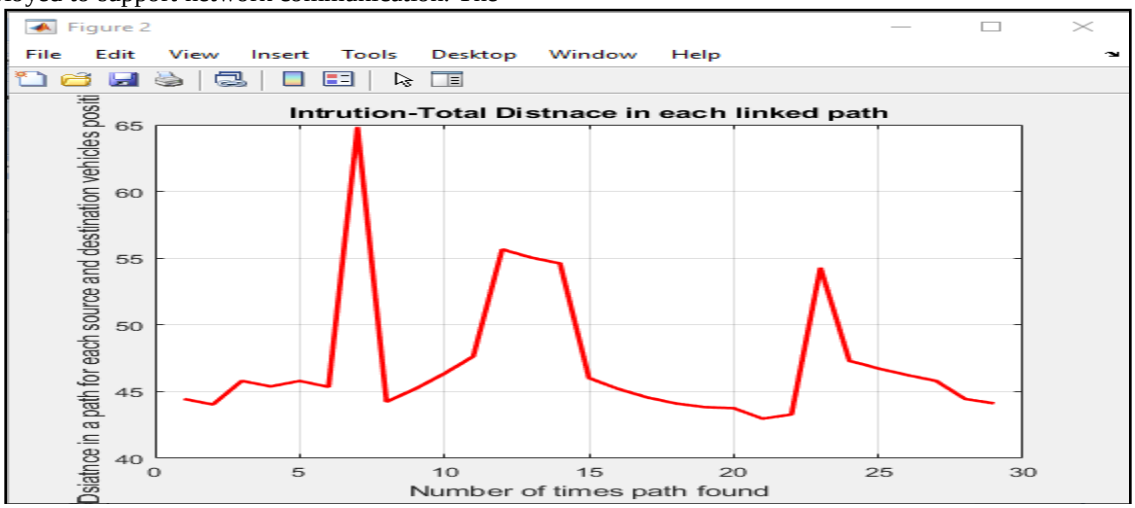

Figure 6:- Total Number Of Linked Path

Figure 6 presents the total communication distance of the selected transmission paths during the intrusion simulation. The graph illustrates the variation in the distance between the source and destination for each discovered path, with noticeable peaks indicating longer routing paths caused by the presence of malicious activity. This analysis demonstrates how intrusions can influence routing behavior and increase communication distance, thereby affecting the overall efficiency and reliability of the vehicular network.

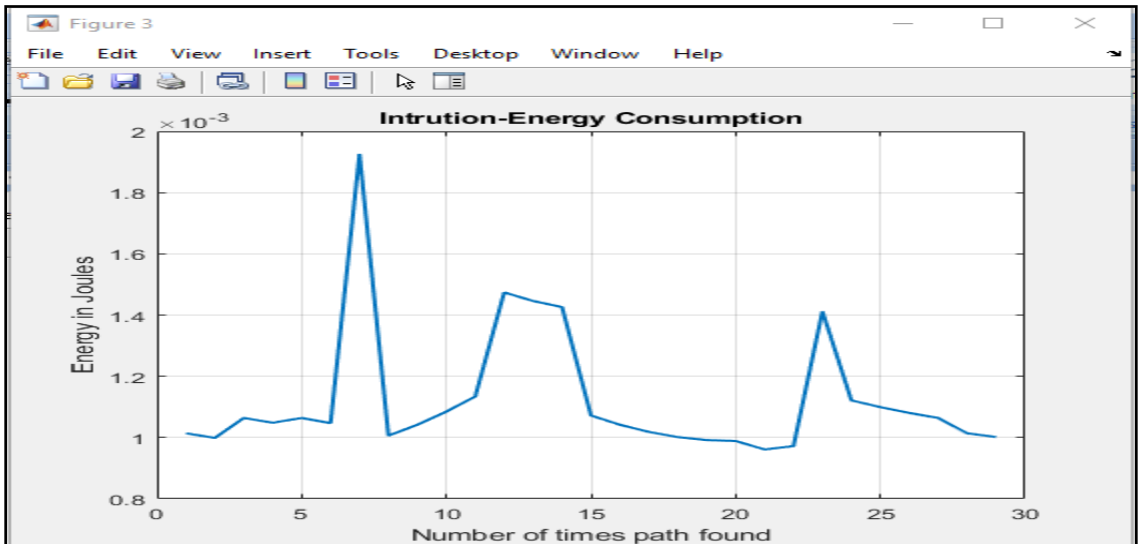

Figure 7:- Intrusion Energy Consumption

Energy consumption in general is one of biggest challenges when it comes to wireless sensor networks (WSNs). Since the biggest amount of energy is used for communication, the most logical way to reduce the energy consumption is to reduce the number of packets transmitted between sensor and sink node. In the fig less energy consumption showing in fig.7

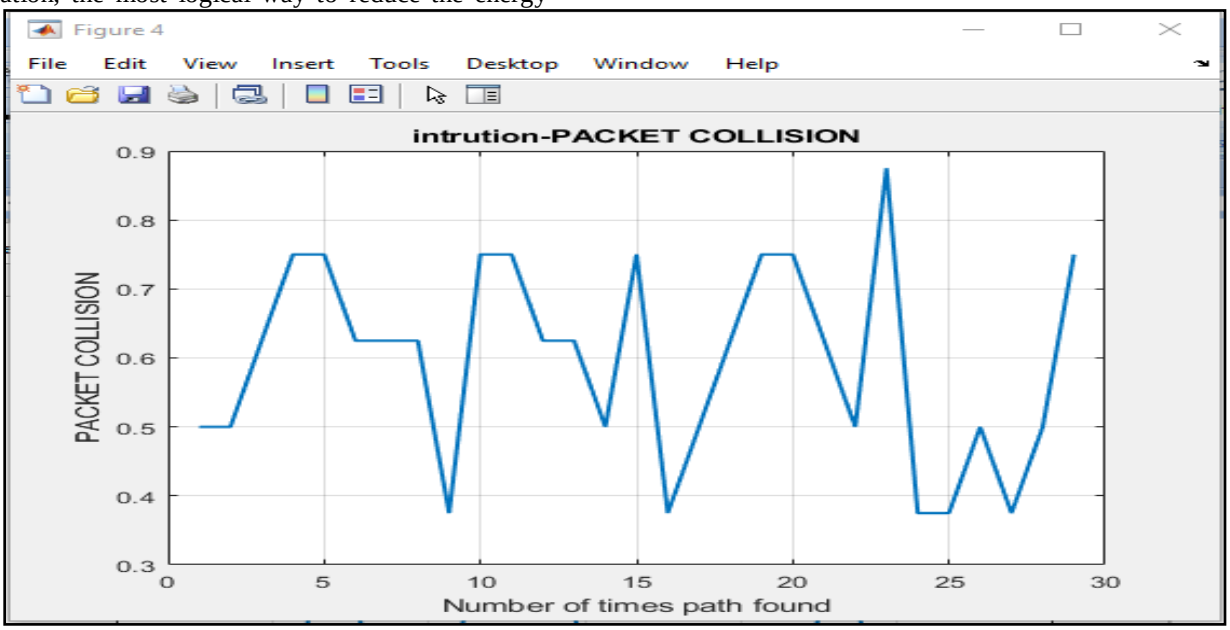

Figure 8:- Packet Collision

Fig.8 showing the packet collision occurs when two or more nodes attempt to transmit a packet across the network at the same time. The transmitted packets must be discarded and then retransmitted, thus the retransmission of those packets increases the energy consumption and the latency

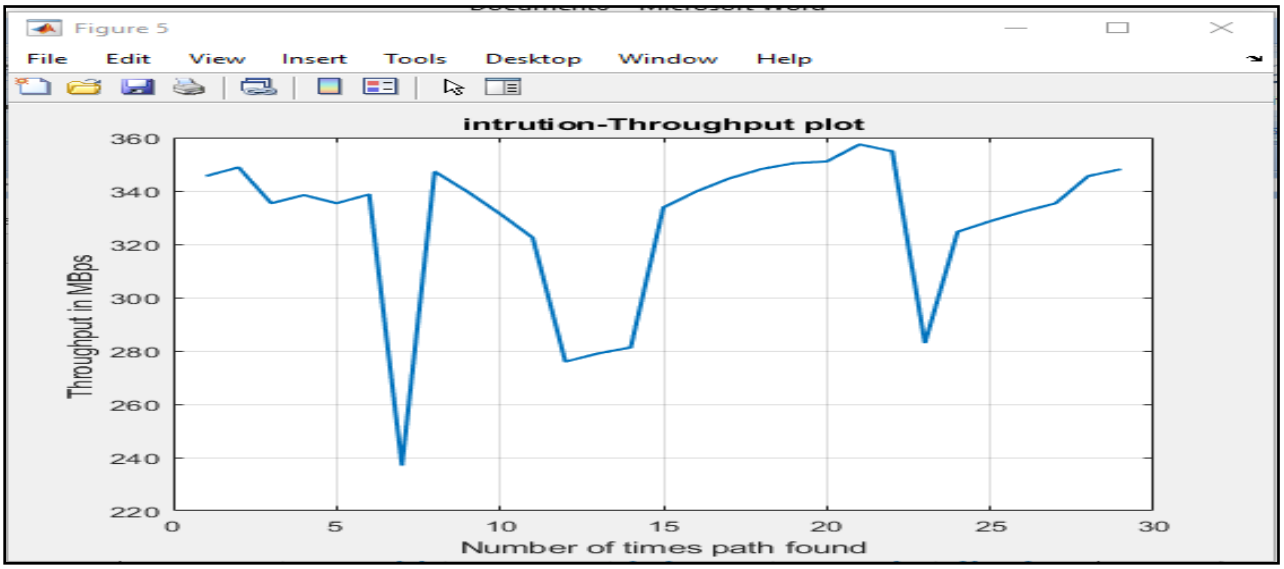

Figure 9:- Intrusion Throughput

Throughput is a measure of total units of information a system can process in a given amount of time the intrusion throughput of the network showing in the fig 9

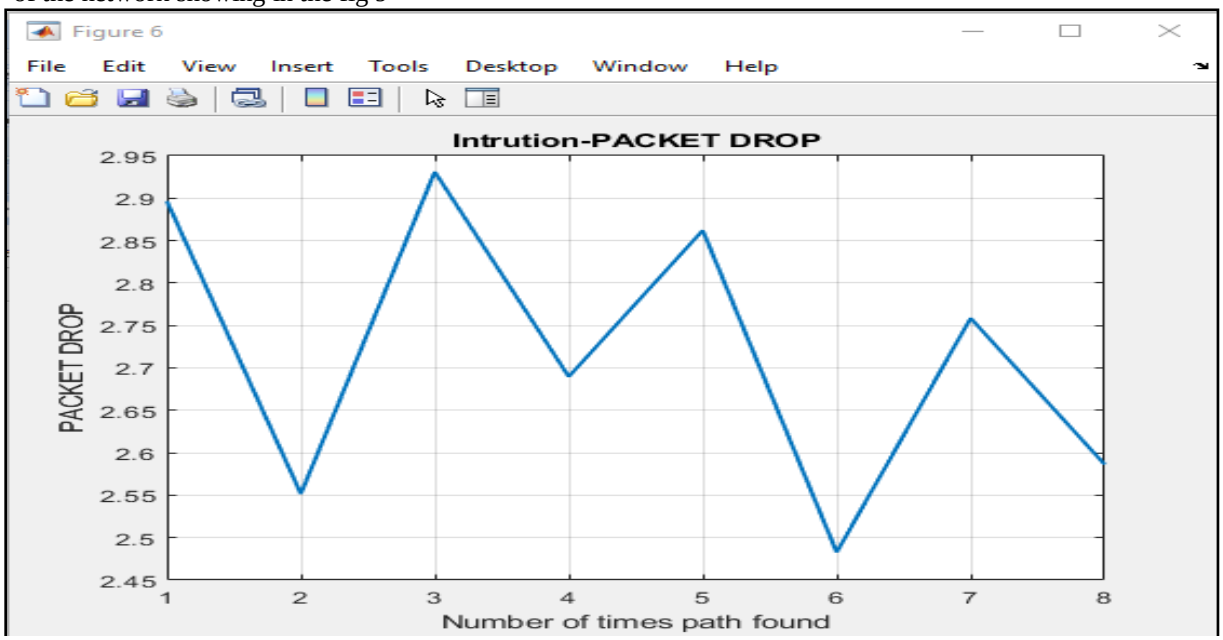

Figure 1:-0 Intrusion Packet Drop

intrusion packet drop showing in the fig.10 Packet loss can be caused by congestions due to heavy traffic, collisions at link layer, buffer overflows,

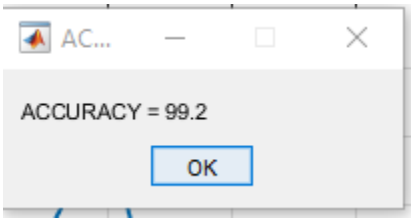

Figure 11:- Accuracy of the System

Figure 11 displays the final classification accuracy achieved by the proposed intrusion detection model. The system attained an accuracy of 99.2%**,** indicating its high capability to correctly distinguish between normal and malicious network traffic. This result demonstrates the effectiveness of the proposed approach in accurately detecting intrusion attacks while maintaining reliable and robust network security performance.

Table 1:- Comparison result with the existing system

[1]	**[2] Techniques**	**[3] Accuracy (%)**
[4] Proposed system	**[5] ResNet50**	**[6] 99.2**
[7] Existing system	**[8] SVM**	**[9] 97.29**

Table 1 compares the classification accuracy of the proposed and existing intrusion detection systems. The proposed ResNet50-based model achieved an accuracy of 99.20%, outperforming the existing Support Vector Machine (SVM) approach, which obtained 97.29%. The results demonstrate that the proposed deep learning model provides superior intrusion detection performance by improving classification accuracy and enhancing the reliability of network security.

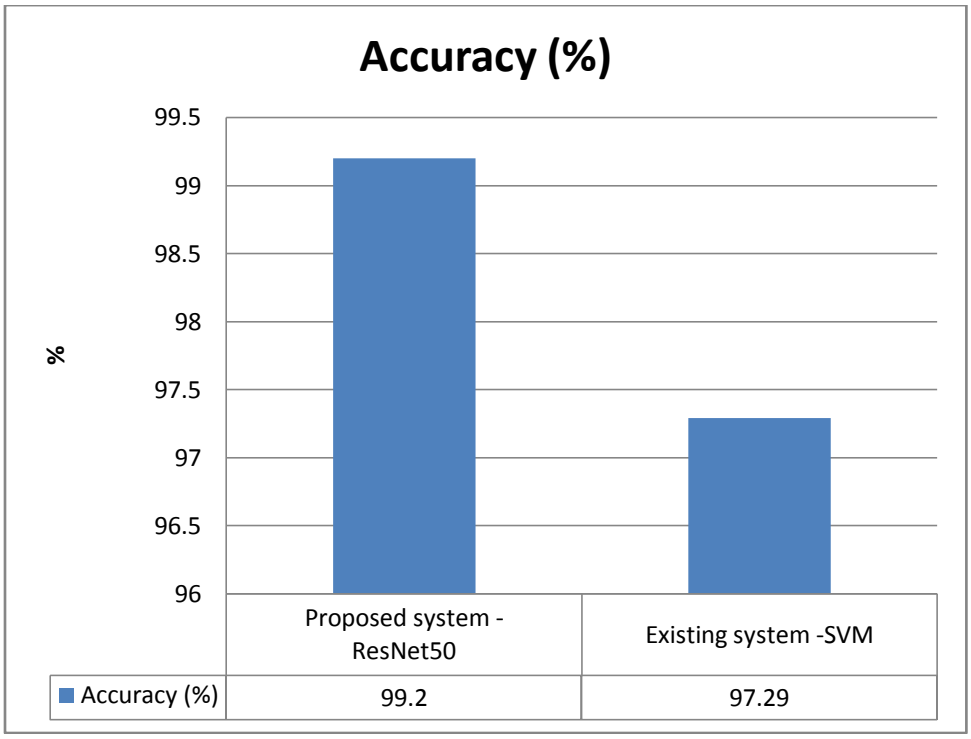

Figure 12:- comparison result with the existing system

Figure 12 compares the classification accuracy of the proposed ResNet50-based intrusion detection model with the existing Support Vector Machine (SVM) approach. The proposed model achieved an accuracy of 99.2%, whereas the existing SVM model attained 97.29%. The higher accuracy of the proposed system demonstrates its superior capability to

distinguish between normal and malicious network traffic, resulting in more reliable and effective intrusion detection performance. These results confirm the effectiveness of the ResNet50 model in enhancing the overall security and robustness of the vehicular network.

5. CONCLUSION

As more devices and services connect to each other, the world's communication environment is becoming more complicated and hard to predict. Computer networks are always changing, growing, and helping people talk to each other and connect systems and services. Hackers or other unauthorized people have been affecting this interconnected environment by breaking things up or stealing information for their own gain. As things get more complicated, it gets harder to get the results of methods and metrics for monitoring networks, classifying traffic, and finding malicious or unusual events across to the people who make decisions. Security experts need tools that help them make sense of the information their analytical systems produce and decide what to do with it. In this data-driven world, using deep learning algorithms as a back-end engine is a better way to help security experts tell the difference between normal and dangerous network traffic. Using a technique called "specification-based," an Intrusion Detection System was made to protect the AODV protocol. We have suggested that AODV use an intrusion system tool to stop some internal attacks. The results of our implementation show that the AODV routing protocol works much better when attacks are happening. In every case, the attack was found to be against one of the rules of the AODV protocol. The work can be expanded to look at the reliability of all kinds of protocols in Wireless Ad Hoc Networks. The relationship between the average time it takes to find a node and how mobile it is can be looked into. You can look into more types of attacks, like group attacks, and figure out how they relate to how vulnerable the protocols are.

REFERENCES

[1] M. Lee, O. Aslam, B. Foster, D. Kathan, J. Kwok, L. Medearis, R. Palmer, P. Sporborg, and M. Tita, "Assessment of demand response and advanced metering," Federal Energy Regulatory Commission, Tech. Rep, 2013.

[2] . M. R. Hasan, Y. Zhao, G. Wang, Y. Luo, L. Pu, and R. Wang, "Supervised machine learning based routing detection for smart meter network," in 12th EAI International Conference on Mobile Multimedia Communications, Mobimedia 2019. European Alliance for Innovation (EAI), 2019.

[3] . M. S. Hussain and K. U. R. Khan, "A survey of ids techniques in manets using machine-learning," in Third International Conference on Computational Intelligence and Informatics. Springer, 2020, pp. 743–751

[4] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications surveys & tutorials, vol. 18, no. 2, pp. 1153–1176, 2015.

[5] . L. Cazorla, C. Alcaraz, and J. Lopez, "Towards automatic critical infrastructure protection through machine learning," in International Workshop on Critical Information Infrastructures Security. Springer, 2013, pp. 197–203

[6] S. B. Kotsiantis, I. Zaharakis, and P. Pintelas, "Supervised machine learning: A review of classification techniques," Emerging artificial intelligence applications in computer engineering, vol. 160, pp. 3–24, 2007.

[7] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on knn classification algorithm in wireless sensor network," Journal of Electrical and Computer Engineering, vol. 2014, 2014.

[8] Abhinav Singhal;Akash Maan;Daksh Chaudhary;Dinesh Vishwakarma A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) DOI: 10.1109/ICAIS50930.2021.9395918

[9] Toya Acharya;Ishan Khatri;Annamalai Annamalai;Mohamed F ChouikhaEfficacy of Machine Learning-Based Classifiers for Binary and Multi-Class Network Intrusion Detection 2021 IEEE International Conference on Automatic Control & Intelligent Systems (I2CACIS) Year: 2021 | Conference Paper | Publisher: IEEE DOI: 10.1109/I2CACIS52118.2021.9495877

[10] Chung-Ming Ou Host-based Intrusion Detection Systems Inspired by Machine Learning of Agent-Based Artificial Immune Systems 2019 IEEE International Symposium on Innovations in Intelligent SysTems and Applications (INISTA) Year: 2019 | Conference Paper | Publisher: IEEE DOI: 10.1109/INISTA.2019.8778269

[11] Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron (2023). *Deep learning* (Updated ed.). MIT Press.

[12] National Institute of Standards and Technology. (2024). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5, Update 1)*. U.S. Department of Commerce.

[13] Kim, J., Lee, S., & Park, H. (2024). Deep learning-based intrusion detection framework for mobile ad hoc networks using hybrid CNN–LSTM architecture. *IEEE Access, 12*, 45812–45827.

[14] Sharma, R., Gupta, P., & Singh, A. (2023). Intelligent intrusion detection in MANET using deep neural networks and feature optimization. *Journal of Network and Computer Applications, 221*, 103724.

[15] Wang, Y., Zhang, X., & Liu, J. (2024). A hybrid deep learning approach for network intrusion detection in dynamic wireless environments. *Computer Networks, 245*, 110423.

[16] Patel, D., Kumar, V., & Mehta, S. (2023). Deep learning-enabled security framework for AODV routing protocol in mobile ad hoc networks. *Wireless Personal Communications, 131*(4), 2895–2916.

[17] Chen, L., Zhao, Y., & Sun, W. (2025). Explainable deep learning for intrusion detection in wireless ad hoc networks. *Future Generation Computer Systems, 156*, 112–126.