“Blockchain Based Collaborative Intrusion Detection System with Privacy Protection in Vehicular Ad-Hoc Networks”

Thesis

Submitted for the award of

Degree of Doctor of Philosophy

Computer Science and Engineering

By

Azath M.

Enrollment No: MUIT0119038102

Under the Supervision of

Dr. Vaishali Singh

Assistant Professor, Maharishi University of Information Technology, Lucknow

Under the Co-Supervision of

Dr. Himanshu Pandey

Assistant Professor, Faculty of Engineering & Technology, University of Lucknow, Lucknow

Under the Maharishi School of Computer Science and Engineering,

Session 2019-20

Maharishi University of Information Technology

Sitapur Road, P.O. Maharishi Vidya Mandir,

Lucknow, 226013

Declaration by the Scholar

I hereby declare that the research work embodied in this thesis entitled "**Blockchain Based Collaborative Intrusion Detection System with Privacy Protection in Vehicular Ad-hoc Networks"** in fulfillment of the requirements for the award of Degree of Doctor of Philosophy, submitted in the Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Lucknow is an authentic record of my own research work carried out under the guidance and supervision of **Dr. Vaishali Singh** and Co-supervision of **Dr. Himanshu Pandey .** I also declare that the work embodied in the present thesis –

i. is my original work and has not been copied from any journal/ thesis /book; and
ii. has not been submitted by me for any other Degree or Diploma of any University/ Institution.

Date:

Place: Lucknow **Azath M.**

Maharishi University of Information Technology
Lucknow, 226013, India

Supervisor's Certificate

This is to certify, that **Mr. Azath M.** has completed the necessary academic turn and the swirl presented by him is a faithful record of bonafide original work under the guidance and supervision of **Dr. Vaishali Singh.** He has worked on the topic **"Blockchain Based Collaborative Intrusion Detection System with Privacy Protection in Vehicular Ad-hoc Networks",** under the School of Engineering & Technology, Maharishi University of Information Technology, Lucknow. No part of this thesis has been submitted by the candidate for the award of any other Degree or Diploma in this or any other University around the globe.

Dr. Vaishali Singh
Supervisor

Dr. Himanshu Pandey
Co- Supervisor

Acknowledgment

Foremost, I am thankful to Almighty for giving me the strength, knowledge, ability and opportunity to undertake this study. To step strong and smooth in this beautiful world of science, I have been supported and supervised by many people. In this regard, I am grateful to the University and express my deep sense of gratitude to its **Honorable Vice-Chancellor** for delivering this great opportunity. I would like to thank the **Registrar** of MUIT, who continuously motivated me for this research work. I express my heartfelt thanks to my supervisor **Dr. Vaishali Singh** and co-supervisor **Dr. Himanshu Pandey**, for being a great advisers to fulfil this work. I would like to thank you for your constant encouragement and motivation to become an investigator. I am grateful for your valuable feedback and your interest during my entire research work. I am deeply grateful to the **Research Dean** for his support, appreciation, encouragement and keen interest in my academic achievement. I am greatly indebted to the committee members of MUIT for supporting me with required data and informations needed for this work. My great respect also goes to my family and friends. It is always a pride for me to live with such people who gives importance to education. Lastly, I would like to thank everyone who inspired me to stimulate this research work without any hindrance.

Azath M.

Dedication

I would like to panegyrize my mother, beloved wife and my son who gave me space and their interminable advocacy to complete this Thesis.

Abstract

The vehicle group is connected through a wireless network called the Vehicular Ad hoc network (VANET). Vehicle-to Infrastructure Communication and Vehicle-to-Vehicle Communication are the two primary types of communication in VANET. It has developed the seamless flow of data between vehicles and thus enabled researchers to look forward to innovative development in this field. It is a particular type of Mobile ad hoc network (MANET) that can be used to make the right decision about road safety and also critical situations. VANET otherwise known as Intelligent Transport Systems came into limelight when it offered newly available safety applications. VANET is typically produced in an ad-hoc structure using a variety of moving vehicles and connecting equipment connected with one another using wireless technology in order to transfer the necessary sensitive information and form a small network in which the devices and vehicles act as nodes. Due to its features and applications, the VANET has more attractive attention in recent studies. Road safety and efficiency increase is the major aim of adopting VANET technology which periodically broadcast the vehicles in VANET. Blockchain is a critical security mechanism for protecting the anonymity of the vehicles in the network. The Blockchain's primary goal is to digitally store and disseminate information without the ability to alter it. The detection of intrusion vehicles is the other component of the VANET. Because most network systems operate on an open network, it is simple to attack vehicle nodes by forwarding misleading information to intruders. In collaborative systems, intrusion detection is typically accomplished using machine and deep learning methods. Most works have failed to identify intrusion, which is required to protect the safety of the vehicles. As a result, the goal of this work is to come up with modernistic approaches for cluster formation, CH selection, and increase security with improved scalability, and integrity collaborative intrusion detection approach.

The proposed methodologies employ three novel approaches for secured communication in VANET with collaborative approaches. This thesis presents a novel collaborative intrusion detection model in VANET. It consists of three phases, (i) investigation of vehicular ad-hoc networks' intrusion detection system (ii) an optimized support vector machine-based collaborative vehicular ad hoc networks' intrusion detection system, and (iii) an optimized convolution neural network-based private collaborative vehicular ad hoc networks' intrusion detection system. In phase 1, malicious activities are detected in

VANET. Many other intrusion algorithms are compared. Regular update is required according to the changing techniques. Cluster structure is done by the K-means algorithm in phase 2, the best cluster heads are chosen using Tabu Search-based Particle Swarm Optimization (TS-PSO) algorithm. Furthermore, Blockchain improves its security and dependability. The novel War Strategy Optimization (WSO) based on Support Vector Machine (SVM) or Optimized SVM model performs a confidential collaborative intrusion detection in VANET. In phase 3, an improved K- harmonics mean clustering (IKHMC) replica carries out cluster creation. Subsequently, the Hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm optimally selects the cluster heads. The blockchain-based privacy preservation model is enabled. Finally, the seagull optimization-based convolution neural network (SO-CNN) is used to spot the VANET interruption. In this thesis, the experimental findings of the anticipated work are implemented using a GPU-based computer based on NS-2 software with a GTX1050 GPU at 16GB RAM and an Intel Core i5-8300H CPU running Tensorflow 1.15. The KDD99 and https://www.kaggle.com/bigquery/ethereum-blockchain datasets are used in this study for experimental dissection. The KDD99 dataset consists of five million records that are described by 41 features. In comparison with the state-of-art techniques, the action matrices like accuracy, precision, recall, detection rate, security, and delay and energy consumption are accustomed to validate the efficiency of the conceptual model thereby providing fine accurate outcomes. The proposed study on seagull optimization-based convolutional neural network (SO-CNN) had a superior security level performance evaluation of 97.6% and a detection accuracy of 94.3%, 2.53 J energy consumption, 8.12s delay, 0.96% Del ratio are compared to the other methods.

Keywords:

Vehicular Ad hoc network, Intrusion detection, Tabu search based particle swarm optimization, War strategy optimization, Support vector machine, Blockchain, Security, Convolutional Neural Network, Ad-hoc, Vector routing protocol, Security Attacks, Malicious Nodes, Artificial Intelligence, Clusters, Cluster head, Convolutional Neural Network, Deep Learning, Machine Learning, Handover and Vehicle to Vehicle.

List of Abbreviations

Abbreviation		Description
AAC	-	Attribute Audit Center
ABE	-	Attribute based Encryption
AE	-	Auto Encoder
AEFS	-	Adaptive Elephant Fuzzy System
AES	-	Advance Encryption Standard
AHP	-	Analytic Hierarchy Process
AI	-	Artificial Intelligence
ANN	-	Artificial Neural Network
BS	-	Base Station
CH	-	Cluster Head
CM	-	Cluster Member
CNN	-	Convolutional Neural networks
CR	-	Cognitive Radio
CSP	-	Cloud Service Provider
DBN	-	Deep Belief Networks
DDoS	-	Distributed Denial of Service
DHCV`	-	D-hop clustering algorithm
DL	-	Deep Learning
DLT	-	Distributed Ledger Technology
DNN	-	Deep Neural Networks
DRABC	-	Distributed Role-based access control
EGT	-	Evolutionary Game Theoretic
GPS	-	Global Positioning System
HCRSO	-	Hybrid Capuchin based Rat Swarm Optimization
HDDM	-	Hybrid Data Driven Model
H-ID	-	Host-based intrusion detection
HO	-	Handover
I2I	-	Infrastructure to Infrastructure
IBE	-	Identity based Encryption
ID	-	Intrusion Detection

IDS	-	Intrusion Detection Systems
IKHMC	-	Improved K-harmonics mean clustering
KGC	-	Key Generation Center
KNN	-	K-nearest neighbors
LSTM	-	Long Short Term Memories
LTE	-	Long Term Evolution
MANET	-	Mobile Ad hoc Network
ML	-	Machine Learning
ML	-	Multi-Layer
MRE	-	Multi-branch Reconstruction Error
MRMR	-	Minimum Redundancy Maximum Relevance
MRMR	-	Minimum Redundancy Maximum Relevance
NAC	-	Nimble Asymmetric Cryptography
OBU	-	On Board Unit
QoE	-	Quality of Experience
QoS	-	Quality of Service
RF	-	Random Forests
RSU	-	Road Side Units
SO-CNN	-	Seagull optimization based convolution neural network
SPPA	-	Stream Position Performance Analysis
SSS	-	Shamir’s Secret Sharing
SVM	-	Support Vector Machine
TMC	-	Traffic Message Channel
TS-PSO	-	Tabu Search based Particle Swarm Optimization
V2I	-	Vehicle to Infrastructure
V2V	-	Vehicle to Vehicle
V2X	-	Vehicle to everything
VANET	-	Vehicular Ad-hoc Networks
VMaSC	-	Vehicular Multi-hop algorithm
Wi-Fi	-	Wireless Fidelity
WOA	-	Whale Optimization Algorithm
WSO	-	War Strategy Optimization
WSO-SVM	-	War strategy optimization - support Vector Machine

List of Symbols

Symbol	Nomenclature
h	Height
S	Surface
Re	Radius
T	Transmitter
P	Point
TP	Tangent Place
D	Dimensional real vector
Tp	True Positive
Tn	True Negative
Fp	False Positive
Fn	False Negative
Σ	Sigma
Φ	Phi

List of Figures

List of Tables

Contents

CHAPTER 1

INTRODUCTION

1.1. OVERVIEW OF VANET

Recently, there is an increased inveigle in the applications and features of the Vehicular Ad-hoc Networks (VANET). The enhanced safety and efficacy of automobiles on road is the reason why VANET has been adopted by many users. Privacy of the vehicles is important to safeguard the vehicles with the systematically receiving messages from Roadside units (RSU), and other vehicles. In spite of these advantages, the VANET is used in many applications, however, sometimes security and privacy has failed to accomplish with the unauthorized tracking of the messages by hackers and violating the privacy-preserving necessity. Hence it is necessary to provide a message authentication scheme and significantly improve the safety of the VANET system. VANET is a kind of Mobile Ad hoc Network (MANET) but instead of roving nodes here vehicles and RSUs are considered. The communication in VANET occurs between the vehicles or between vehicles to RSUs. **Figure 1.1** illustrates the VANET architecture with the important components.

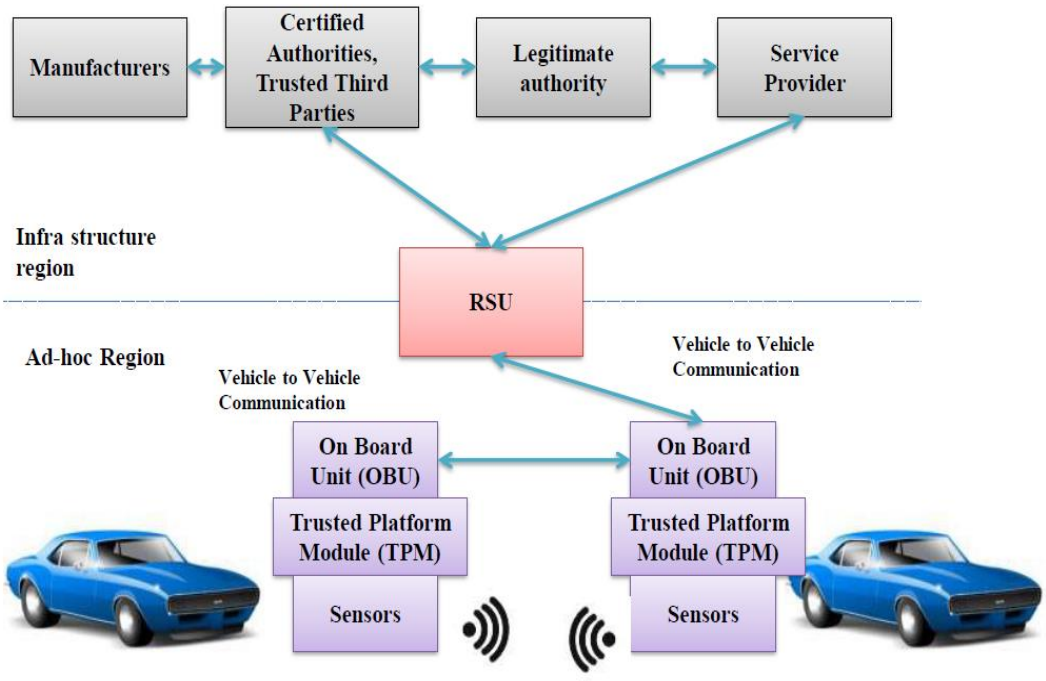


Figure 1.1: VANET architecture with important components

With the emerging development of the automotive industry paved the way for vehicles with equipped sensors for onboard as well as processing purposes with well-communicative devices. Vehicular Ad hoc network (VANET) (Hasrouny et al. (2017)) has developed the seamless flow of data between vehicles and thus enabled the researchers to look forward to innovative development in this field. This particular sort of Mobile ad hoc network (MANET) (Raja et al. (2020)) can be used to make the right decision about road safety in critical situations. VANET otherwise known as intelligent Transport Systems came into limelight when it offered newly available safety applications. VANET is created in an ad-hoc structure that connects numerous moving objects and connecting devices in a wireless medium to transfer the required sensitive information and form a small network in which the devices and vehicles act as nodes (Hussain et al. (2019)). Henceforth, the informations are transmitted between the nodes in the formed structure in an easy manner. The data are collected to receive the useful message and subsequently forward the formed information to other nodes. Most of the VANET networks are open networks and hence joining and leaving the network is easy. Moreover, most of the newly launched vehicles contain an onboard sensor, and joining the VANET is easy and thereby leverages the benefits of the VANET. However, these might have pushed the network to think about security, since any vehicle can join the network without prior knowledge, and hence some of the vehicle users could use this platform for illegal purposes. Hence it is ineluctable to safeguard the VANET platform (Al-Heety et al. (2020)). Many security algorithms were introduced directly by the researchers for security purposes and also to boost confidentiality, reliability, scalability, and privacy.

Blockchain is an important security tool to safeguard the secrecy of the automobiles in the organization. The main aim of the blockchain is to store the information digitally and distribute it without any editing option. Since it is named as immutable ledgers or storage of transaction, the details are seldom deleted, altered, or destroyed with the name distributed ledger technology (DLT) (Anyanwu et al. (2022)).

To achieve the maximized packet delivery ratio with the mitigation of delay and energy utilization clustering and the options for cluster head (CH) concepts were introduced in VANET. Clustering is the group of two or more nearby vehicles with the same features from the hierarchical framework. CH is primarily responsible for cluster formation and

each cluster member is termed as cluster (CM) (Akhter et al. (2021)). Here, CH resembles the mobile router, and CM is considered the mobile node. While forming the cluster some of the parameters are deemed such as transmission range of the vehicle, degree, location, acceleration, relative velocity, direction, the density of the vehicles, etc. The most stabled vehicle is considered as CH, and selected ML and DL approaches are used by the researches. The other nodes act as CM, the CH and CM routing tables are maintained for the intra-cluster communication. Thus the clusters are formed in this platform (Khayat et al. (2020)).

The other part of the VANET is the detection of intrusion vehicles. Since most of the network system follows an open network it is easy to attack the vehicle nodes by forwarding fake information to intruders. For the detection of intrusion collaborative system is mainly used with machine and deep learning approaches (Kebande et al. (2021)) (Bangui et al. (2022)). The detection of intrusion is must to insure the security of the vehicles but majority of efforts have been unsuccessful. Hence this work aims to provide newly developed approaches for cluster formation, CH selection, and enhanced security with improved confidentiality, scalability, and a trust-based collaborative intrusion detection approach.

1.2. Main Components of the VANET System

Figure 1.1 displays the VANET's primary elements. The next section provides an explanation of the components.

1.2.1. Vehicle to Vehicle (V2V) communication

Many problems have emerged as the number of vehicles and mobile network subscribers has increased. Massive amounts of data traffic, transportation, and traffic collisions on Long term evolution (LTE) networks are all issues (Raw et al. (2011)). It has been an enormous rise in the volume of internet traffic on LTE networks and on the internet over the last few years, and interpretations are being devised to increase the adequacy of LTE networks, and manufacture aircraft safer. The results in a V2V structure built on VANETs decreases huge amounts of traffic from LTE networks while also providing opportunities to LTE network users.

Before going into the second process of interaction, V2V necessitates a first step of discovering that allows it to decide the distance between two vehicles that are interacting

with one another and attempts to establish a stable link (Narayanan et al. (2019)). Based on the direct method, various frequencies have been considered; even so, the above method does not guarantee any good QoS due to band instability, which also decreases the capacity of the automobiles to discover other neighboring automobiles and to limit their coverage area. The network on its own identifies and detects bands in the situation of exploration with network assistance (Limbasiya et al. (2016)). The BS is requested to transmit User Equipment and to activate a V2V link that provokes the BS to enable communication to devices throughout in order to determine the uniqueness of the link.

Advantages:

- It enables medium and short-range interaction while requiring no alongside-the-road facilities.
- It is less expensive and allows delivery of simple comments.
- It reduces transmission delay as it is quick and reliable, as well as offers actual safety.
- Improves safety by protecting vehicles from future traffic incidents.

Disadvantages:

- Frequently occurring topography divides up because of high mobility and long-distance communication issues
- Utilizing conventional protocols is difficult and problematic when live-streaming texts in areas with significant traffic and external forces.

1.2.2. Vehicle to Infrastructure (V2I) communication

V2I is a wireless infrastructure vehicle design and the structure distributes data from endpoints using innovations such as Global System for Mobile, WiMax, and others. A customer data flow diagram scheme was devised to assess the effectiveness of V2I transmitting data utilizing Wi-Fi and LTE Het-Net facilities for just a traffic data group request (Soni et al. (2021). The client transmits information to the server about GPS destinations, time stamps, and connection intensities of several network integrations. The test system is made up of Wi-Fi, LTE and RSU assistance experiment road surface section, as well as in-car (On board unit) OBUs to Wi-Fi and LTE support.

The experiment was carried out in Clemson, South Carolina, on an accessible route to a parking garage with such a horizontal configuration and light to medium roadside grass

and trees. The motorist started from an LTE and Wi-Fi network segment and linked to the collecting data server through Wi-Fi (Ali et al. (2020)). The linkage switched to LTE to connect to the server as the vehicle drove out of the Wi-Fi range. The network association was used to enable vehicle-to-TMC (Traffic Message Channel) and vehicle-to-RSU data statements in a Wi-Fi and LTE-facilitated Het-Net situation. The link was lost before an effort to rejoin and it was a hard handoff. To ascertain the tough handover period, data was gathered and the time among consecutive packaging so during handovers.

Advantages:

- There is no need for a routing protocol, and the latency is lesser for practical uses.
- Greatly reduces bandwidth consumption by exchanging only incomplete forwarding updated data with neighbors.
- Decreased network overhead and changes to the forwarding table would not happen if a connection fails due to the lack of control communication for node failures.

Disadvantages:

- Unutilized pathways consume a large amount of the available bandwidth.
- In small ad hoc networks, the achievement is extremely poor, and fewer understanding of different nodes.
- As the size of the network grows, so do the memory complexity and computational cost of the forwarding table.

1.2.3. Infrastructure to Infrastructure (I2I) communication

Whenever a vehicle is linked to a near area RSU, the RSU connects to the web and generates the necessary data for the user. The GPS module in the vehicle only with VANET implementation identifies the near area RSU (Khan et al. (2022)). When the vehicle detects a near area RSU, it sends the packet to obtain confirmation. Whenever a user registers with RSU, people would be given all of their data.

The digital signature method is used for authentication. The above provides a single passcode for all RSU customers who already have enrolled. RSUs are stationed at every end of the roadway. The handoff system happens when the vehicle moves beyond a

specific range (Wantoro et al. (2014)). This same flexing data will be moved from the old Roadside unit to the new one. RSU's services are referred to as service-based VANET.

Advantages:

- The periodic flooding of the network does not update the routing table, when it is demanded and requires flooding.
- The due destination sequence number is beaconless so it saves the up-to-date path and bandwidth.

Disadvantages:

- Requires several time for initial communication and connection setup.
- When the switching nodes have out dated entries, the routing could become unpredictable.
- There are large control overheads when there are several route reply packets for a single route reply packet.

1.3. NETWORK SELECTION MODEL IN VANET

The system model of coverage-based network selection is illustrated in **Figure 1.2.** The source vehicle (Red color car) is moving towards the left side to reach the destination, which its receiving signals from different BS like RSU1, RSU2, Neighbors' cars, and Pedestrians. Now, the vehicle has to choose the perfect inclusion of BS based on three parameters like coverage distance, Number of connections in the BS, and Signal channel quality, etc. Depending upon these parameters; the vehicle is going to initiate the handover (HO) process to maintain the link to the destination (Hamdi et al. (2020)).

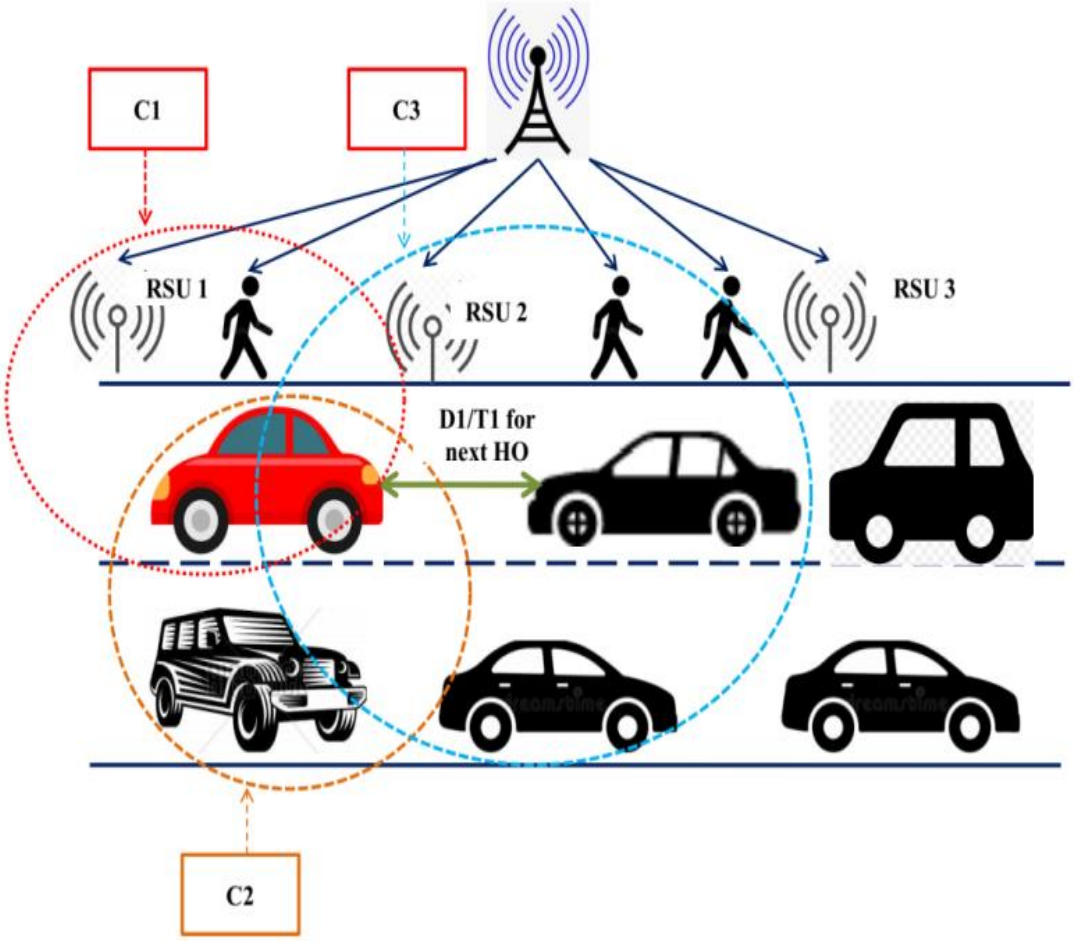


Figure 1.2: Illustration of coverage based network selection

1.3.1. Coverage

Network coverage is the fundamental issue of Vehicle to everything (V2X) and the coverage of the network reaches the maximum under the constraints of possible quality of the services with the estimation of network coverage for the availability of the communication blind area and thus enables the VANET monitoring area. The vehicles are added to the network coverage based on the constraints. Moreover, the changing network coverage density guarantees the reliability of the vehicles added. The coverage can be used not only for the monitoring of area coverage and communication but also to meet the quality of services of the V2X (Cheng et al. (2015)). Network selection can be defined as how the vehicles choose the Wi-Fi network for making the new connection. In general, it can be defined as the geographical area covered by the V2X user with the connection made by the network to make transmission of data or access various services. The key parameters to estimate the coverage for the network selection are coverage area calculation and time calculation which are explained below.

1.3.2. Handoff/ Handover

In comparison to macro cells, small cells need less signal strength and have a smaller coverage area. Nevertheless, a tiny cell contains a smaller radius and uses less energy than a macro cell. While the small cell technique contains multiple technological advantages, the intensive small cell deployment has increased radio node failure since the frequent user mobility has resulted in needless handovers (Mu et al. 2013). In V2X the vehicles are in a moving state and changing of network region covered by an access point to another takes place and this is known as handoff/ handover. To achieve a seamless connection the network and vehicle should remain intact as illustrated in **Figure 1.3.**

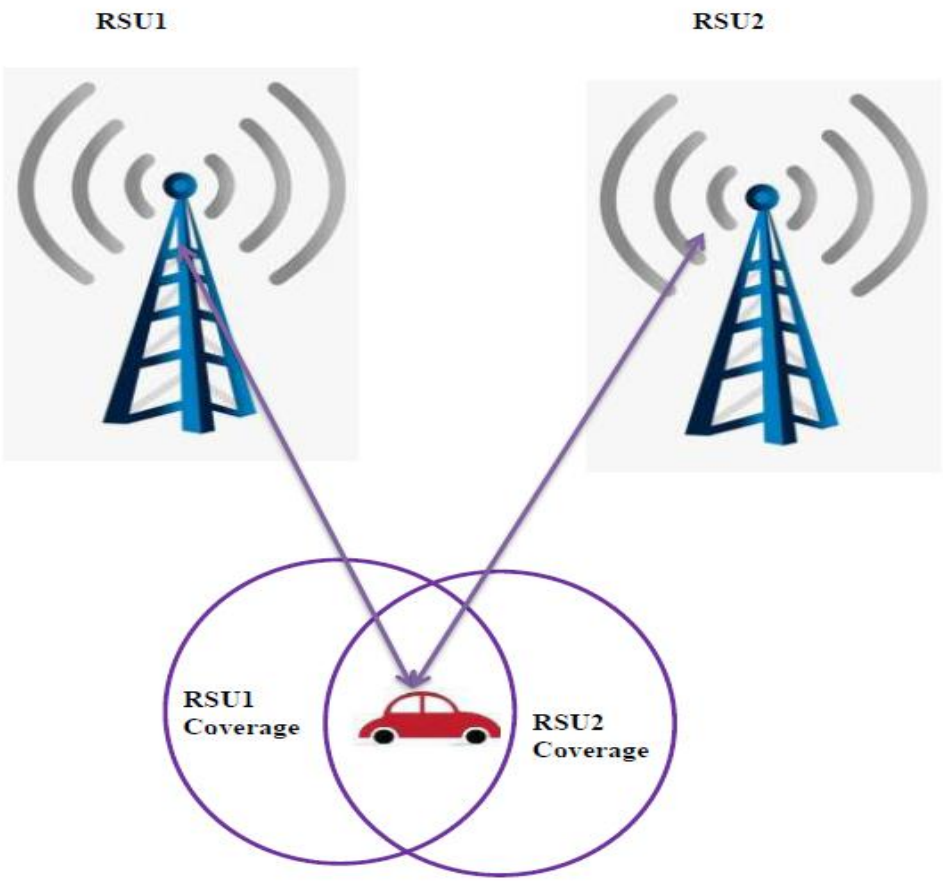


Figure 1.3: Handoff

1.3.3. Coverage Area Calculation

The coverage signal transferred through the base station to another series of action is called Handover in cellular systems. The unnecessary handovers are reduced in virtue of the significant role and this process is controlled by Handover parameters (Qian et al. (2015)). Hence, the higher Quality of Experience (QoE) to the users were provided and it

contains an effective handover mobility system. While increasing system throughput, the unnecessary handovers were minimized.

In a V2X, the quality of the wireless connections among mobile nodes could change over time. In severe instances, a transmission link's total lifespan is forced because of the road's constrained transmission network coverage as nodes are mobile towards it and far from one another (Li et al. (2017)). The network control algorithms' performance is affected so the Link dynamics could also cause network connectivity to change over time. When the predefined road constraints with various transmission coverage areas numerous different link dynamics are provided.

The speed limit restricts the vehicles' velocities as well as predefined road constraints node movement. The transmission ranges of a node are not equivalent to the efficient transmission coverage areas of nodes. Different link characteristics were captured by considering the efficient coverage area (Son et al. (2011)). An efficient transmission coverage area is the major aim of this study.

By considering V2X in a highway scenario, there are various number of vehicles moving along the highway in the opposite as well as same directions. For wireless communication, the Onboard Unit devices equip all the vehicles (Liu et al. (2015)). Every vehicle do have a relaying ability to connect with other multicast route when it is beyond its transmission range. The transmission radius is frequently higher than the elevated way's breadth because cars go in the opposite and similar direction along the road and their motion is restricted by the road's edge. While it is enclosed with a node's transmission range in the area outside the road only vehicles that enter the costs and benefits coverage area of a given vehicle can communicate with it.

The presumptions made in defining the connection dynamics are listed below:

- The antenna's height '*h*' is located at point '*S*' on the surface.
- Let, '*O*' be the centre of the antenna and '*Re*' be the radius of the place.
- Let '*P*' be the point on the place at a distance of 'd' from '*S*'.
- Beyond '*S*', the device cannot receive any signal from the transmitter '*T*'.
- Point *TP* is the tangent of the place, hence the height of the tower is *SP*=*PT*=d as shown in **Figure 1.4.**

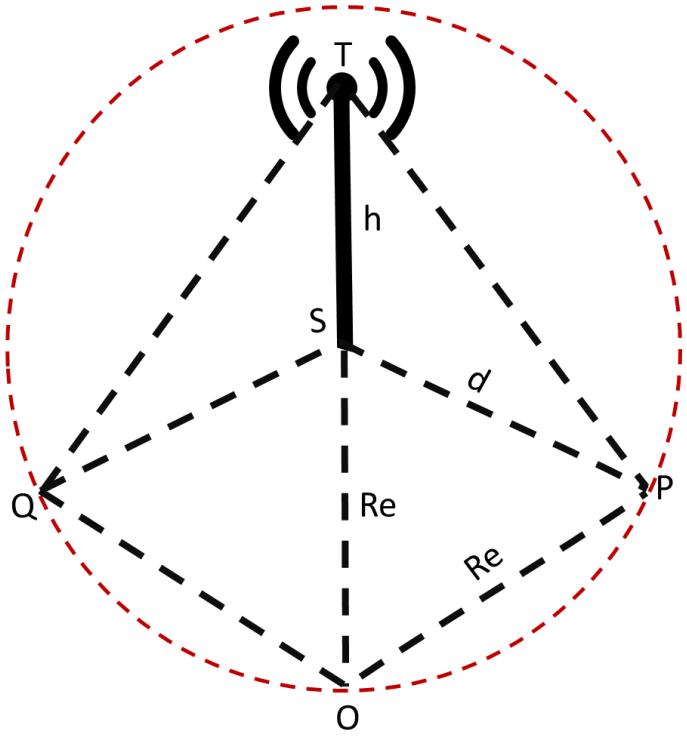


Figure 1.4: Coverage area calculations (Jabar Mahmood et al. (2021))

In the above **Figure 1.4**, Pythagoras theorem is applied to calculate the coverage area. It is defined that in a right-angled triangle, the square of the hypotenuse side is equal to the sum of square of other two sides. The sides of this triangle are named as The Hypotenuse, Base and Perpendicular. When it is opposite to the angle of 90°, the hypotenuse is the longest side (Lipowsky et al. (2009)). Let us consider the right triangle as Δ OPT.

As per Pythagoras theorem,

$$OT^2 = OP^2 + PT^2 \tag{1.1}$$

Therefore,

$$(\mathrm{Re}+h)^2 = \mathrm{Re}^2 + d^2 \tag{1.2}$$

$$\mathrm{Re}^2 + 2\,\mathrm{Re}\,h + h^2 = \mathrm{Re}^2 + d^2 \tag{1.3}$$

The expansion of d^2 is formulated as,

$$d^2 = 2\,\mathrm{Re}\,h + h^2 \tag{1.4}$$

Hence, 'h' is a small value to the radius of the earth, so h^2 can be removed,

$$d^2 = 2\,\mathrm{Re}\,h \tag{1.5}$$

From this,

$$d = \sqrt{2\,\mathrm{Re}\,h} \tag{1.6}$$

The coverage area is calculated using the formula given,

$$A = \pi d^2 \tag{1.7}$$

1.3.4. Time Calculation

In V2X, the real-time services are obtained by assisting the users and the significant Quality of Service (QoS) parameter is delay (Palas et al. (2021)). When the group of packet source is involved, the amount of time required transmitting a packet is indicated as a delay. Based on the real-time delay-sensitive applications, the QoS drastically minimized higher delays. The handover failure rate were reduced by utilizing transmission delay while increasing system throughput.

$$Time = \frac{Dis\tan ce}{Speed} \tag{1.8}$$

From this,

$$S = \{BS_1,\ BS_2,\ BS_3,\ldots..,\ BS_n\} \tag{1.9}$$

$$\forall d, t \in BS \tag{1.10}$$

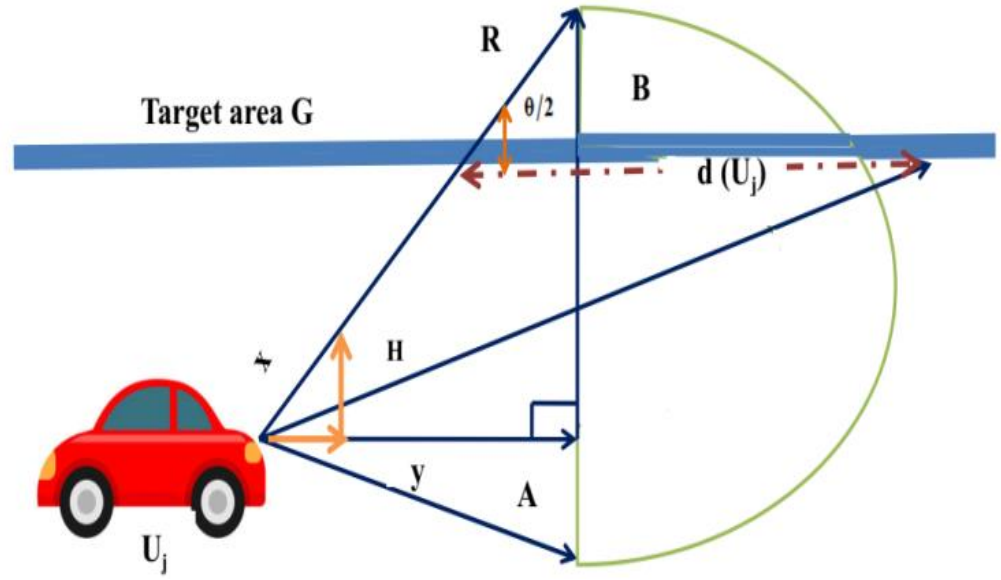
In the above Equation (1.9), *BS* is the base station. The delay time and the distance are defined in terms of *t* and *d* respectively.

If the Source vehicle is moving in the direction of the destination, it has to regularly switch its BS. To avoid the number of HO, the Source Vehicle has to figure out and prepare the neighbour BSs distance (d) and reaching time (t). It also helps to prepare the HO process. These values are stored in the Queue of the Vehicle's buffer. Based on the highest‘d’ value and minimum‘t’ value, the source vehicle has to choose maximum coverage BS for changing its HO using BS(*d, t*).

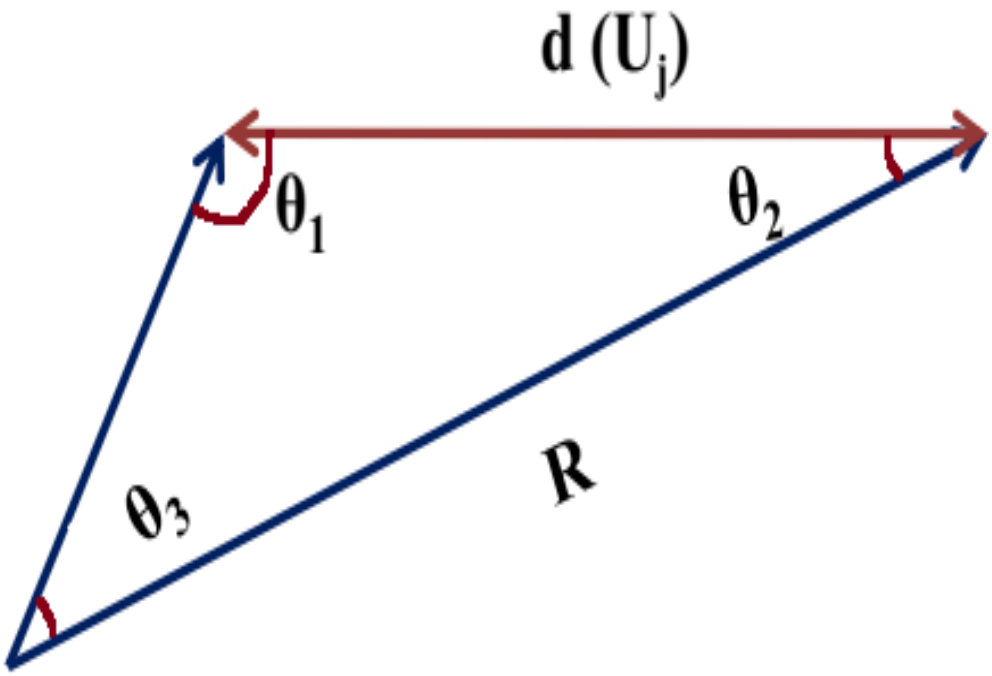
1.3.5. Source Behavior

The GPS unit is used to mimic the vehicle's location and map the destination's information. The sensor view of the vehicle is taken as u_{fi} and the sensing range is taken

as R and the distance between the destination and the vehicle position (L (A_i, B_i) is taken as H. The values of the A and B are evaluated utilizing the cosine equation as $\cos\frac{\theta}{2} = \frac{R}{A}$ and Pythagoras theorem $R^2 = A^2 + B^2$.



(a)



(b)

Figure 1.5: V2X coverage distance (Fabian de Ponte Müller, (2017))

The value of *y* can be evaluated as $H:B=y:A$ and using these evaluation results, the coverage distance can be estimated using the sine equation as $\frac{R}{\sin\theta_1}=\frac{x}{\sin\theta_2}$ and $\frac{H}{\sin\theta_3}=\frac{R}{\sin\theta_1}$. This is given in the above from **Figure 1.5.**

1.4. KEY SERVICES IN VANET

The nature of communication in VANET leads to so many attacks. Some of the services of VANET related to security and privacy-preserving are authentication, availability, integrity, confidentiality, etc (Zhou et al. (2019)). They are elucidated below:

- **Availability**: It is the important key factor since the nodes (vehicles) in the VANET rely on the resources such as Wi-Fi, other vehicles, and data services while transmitting the data.
- **Confidentiality**: This service is performed to ensure the trustworthiness of the data. This service can be used to circumvent the leakage of data to an unauthorized node. That is only the authorized user/ vehicle can access the information by maintaining its privacy of the data. It includes two steps authorization and privacy. The former permits only the authorized user to access the information while the latter protects the sensitive data from attackers or unauthorized users (Hussain et al. (2015)).
- **Integrity**: It mentions the overall certainty, and completeness of the received reports, and this service verifies whether the destination receives the accurately transmitted data. The adaptability of the sensitive data in deliberate, accidental, or improper ways are monitored and rectified with this property.
- **Authentication**: The main requirement of VANET is authentication which confirms the identity of the sender in the network through verification steps. Any node can pretend to act as a legitimate one. Only the authentication process ensures the legality of the node.

Along with these key factors, VANET includes special concerns since it deals with human lives. In concern with this, the responsibility of the driver is also considered while maintaining the privacy of the driver. Moreover, the details about drivers and vehicles are exchanged securely without any delay. The delayed message is responsible for the

catastrophic consequences of the vehicles. Providing a better security system for VANET is a challenging task since breaching it will lead to hazardous impacts. The other challenges are dynamic connections, instant arrival, and departure of vehicles, and often prone to attacks with the open and broadcast nature of communication.

1.5. DIFFERENT TYPES OF THREATS IN VANET

The VANET system is subjected to many assaults. Vehicles provide the required electricity and hence the OBU does not worry about the limited supply of battery life like mobile phones and other wearable devices. In concern of this, the processors and chips are integrated along with the OBU to enable workstation computing capability. However, it also possesses a disadvantage in terms of computational capability, which enables the attackers with higher computational intensity and is not applicable for ad-hoc networks.

The unique features of VANET enable various types of attacks and threats with significant computing. The different types of attacks are illustrated in **Figure 1.6** and it is based on the security requirement of the system to compromise. The attacks are classified as integrity, confidentiality, authentication, accountability, and availability. Some of the attacks are explained below.

1.5.1. Interference and Jamming

The jamming or interference of a signal is defined as the corruption or loss of the messages while transmitting. For example, if the attacker possess a strong and powerful transmitter the generated signal can distract the original signal and lead to corruption. Random noises and pulses are examples of this type of signal jamming (Punal et al. (2014)).

1.5.2. Masquerade Attack

This type of attack takes place when one entity or user behaves as another entity/user and changes modifications on the transmitting data. During this attack, the attacker utilizes a fake identity to obtain unauthorized access to resources like legitimate access. It can be circumvented by providing better protection for the information of the authorized user. This can take place by stealing the login passwords, enabling gaps in the programs, or finding a way to access the authentication process (Al Junaid et al. (2018)).

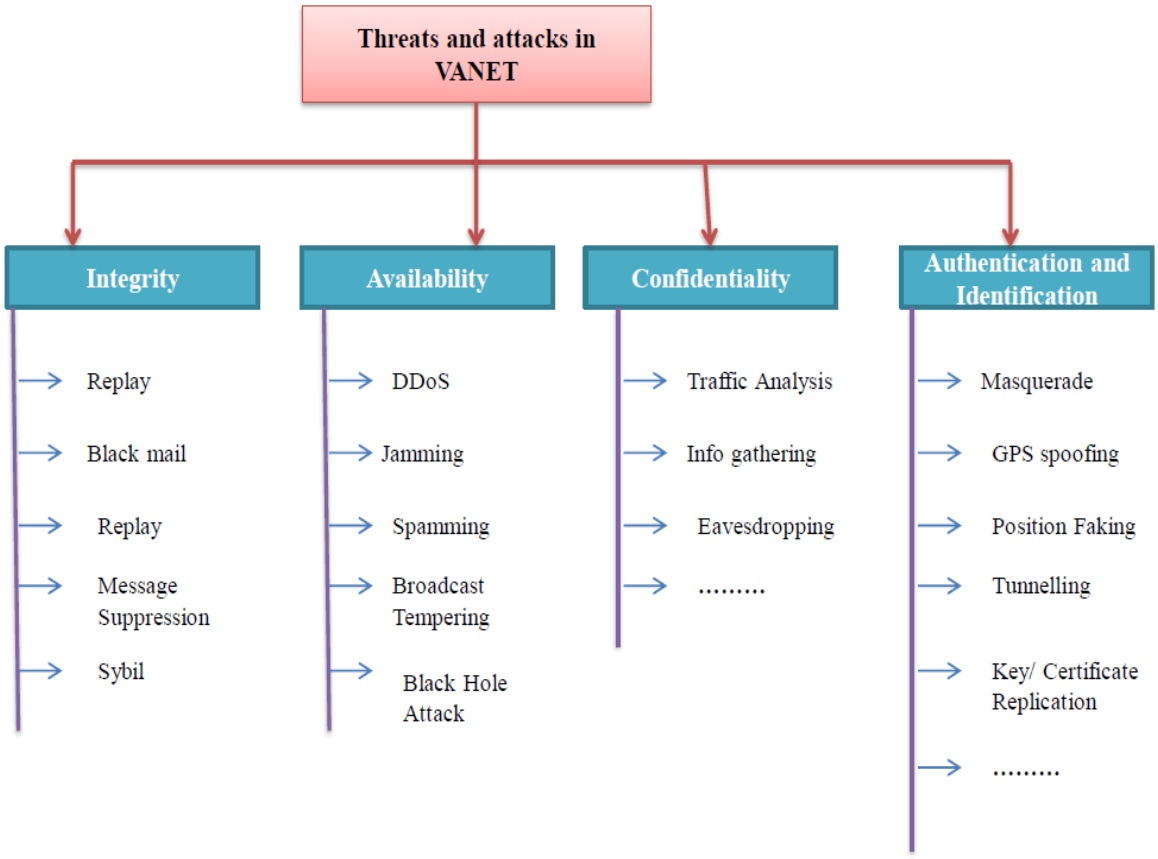


Figure 1.6: Different types of attacks in VANET (Syed Mohd Faisal et al. (2020))

1.5.3. Replay Attack

A session attack is a type of stealing the authorized session ID of the client to perform fraudulent transactions or activities. This might occur when there is no expiration time for the transaction session in a network or the data are stored in an unencrypted manner. For example when web applications reuse the old session Ids for authentication purposes then they can easily be affected by the session replay attack. The session ID is nothing but assigning a unique ID for accessing the web applications by the user. While assigning the session ID it is must to maintain confidentiality to avoid attackers.

1.5.4. Distributed Denial of Service

A distributed denial-of-service (DDoS) is a type of active attack in VANET. This type of attack mainly distracts the traffic of the targeted node. Usually, this type of attack increases the internet traffic around the target and surroundings. Hence it will circumvent the passage of data from the target node to the destination at a particular time. **Figure 1.7**

illustrates an example of a DDoS attack. In the figure, the attacker sends a massive amount of packets to slow down the transmission process of the targeted node. Hence the resources are utilized by all the packets sent by the attacker and thus making it impossible for the targeted node to access the actual packets (Alrehan et al. (2019)). From the figure, we can see that the attacker sends unwanted packets to all other vehicle nodes and so its flooded with thousands of packets thus making the targeted node act slowly.

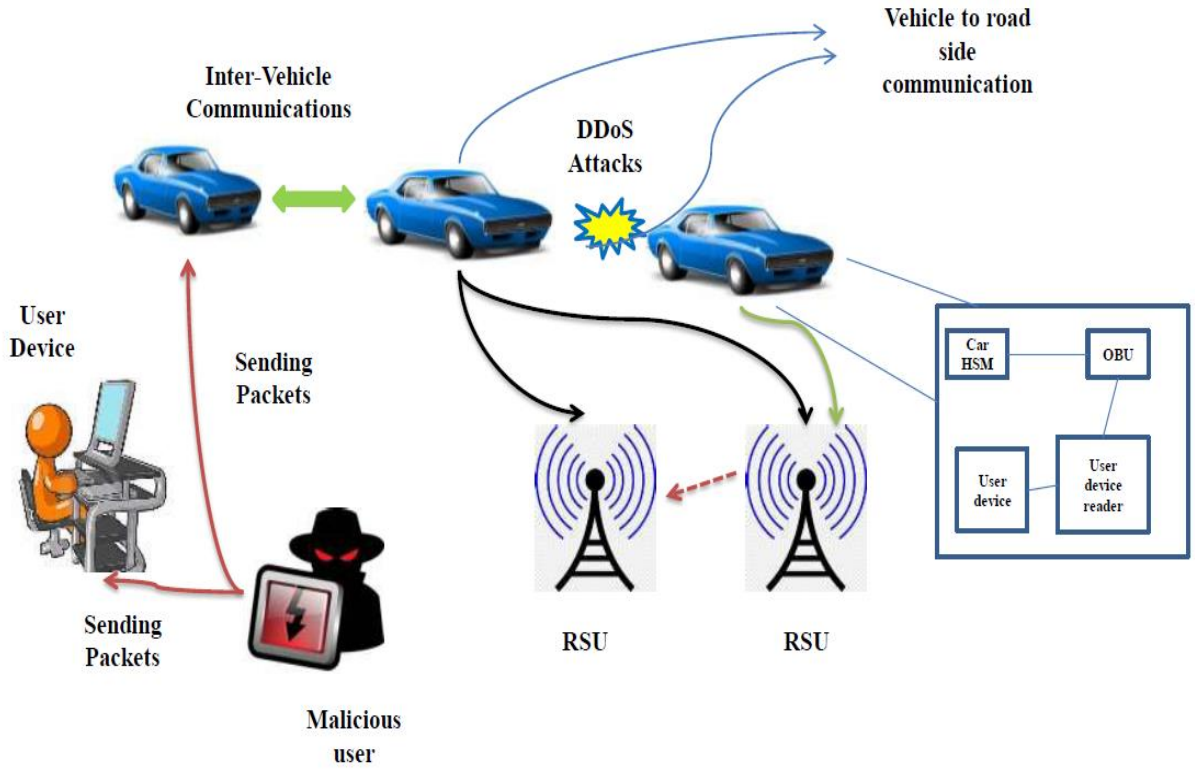


Figure 1.7: DDoS attack in VANET

1.5.5. Monitoring and Eavesdropping

This is a type of stealing information from authorized nodes. This usually occurs in smartphones and computers via unsecured Wi-Fi connections. The attackers violate the policies of communication to find the communication channel. In eavesdropping the attacker is an unauthorized user who reads the messages. In mobile Adhoc networks, the hosts share the wireless medium and most of the medium utilizes RF spectrum for the broadcast. However, while broadcasting the signals via airwaves the receiver who all tunes the exact frequency can access the signals. Thus an unauthorized user can also overhear the messages that are transmitted and insist the fake messages into it.

1.5.6. Sybil

Sybil's attack is usually caused by the legitimate vehicular nodes which was once the authorized node in the VANET. The node sends fake messages with various identities which leads to traffic jams and often causes accidents and thus counterfeits the traffic scenario.

1.5.7. Interruption

This is a type of attack in which the attacker makes the network service unavailable or degraded for the authorized user. Some examples of interruption attacks are breakage of the communication line, redirecting the requests of the valid user to invalid services, overloading the server host, and overloading the intermediate network devices.

1.5.8. Traffic Analysis

The revealing of patterns followed in communication is known as traffic analysis. In this type of attacks the patterns are stolen and revealed to the active attackers. This can be prevented by regular monitoring of the network.

1.6. CLUSTER FORMATION

Cluster formation is an important process in VANET and it deploys CH selection. The cluster formation relies on the input metrics and are erratic. The members in the cluster are called CM and the cluster formation relies on the metrics such as acceleration of the vehicle, velocity, direction, location, the density of the vehicle, degree, transmission range, etc., the most stable one is selected as the CH and the routing tables are perpetuated by it. Different types of cluster formation based on different techniques are depicted in **Figure 1.8.** The following section elucidates the techniques in detail.

1.6.1. Intelligence based Strategies

Clustering is the main process in data mining, machine learning, and many other clustering algorithms. Some of the main clustering algorithms are the K-means algorithm, hierarchical clustering, and more. These algorithms are used for clustering the vehicles and sometimes these algorithms are modified with fuzzy logic and act as a hybrid algorithm.

i. **Machine learning algorithms**

Machine learning such as the K-means algorithm is often used for clustering the VANET. In this k number of clusters are formed from the vehicles. The coordinate vehicles are fed as input and the centroids are assumed by the system. With the help of Euclidean distance, the new centroids are evaluated and act as the CH. This will continue if a vehicle joins the cluster or leave the cluster. At first, the mean of the cluster is susceptible and changes the k-means algorithm. On the other hand, Euclidean distances are evaluated for the vehicle in connection with the other vehicles starting from the minimum distance in the Hierarchical clustering.

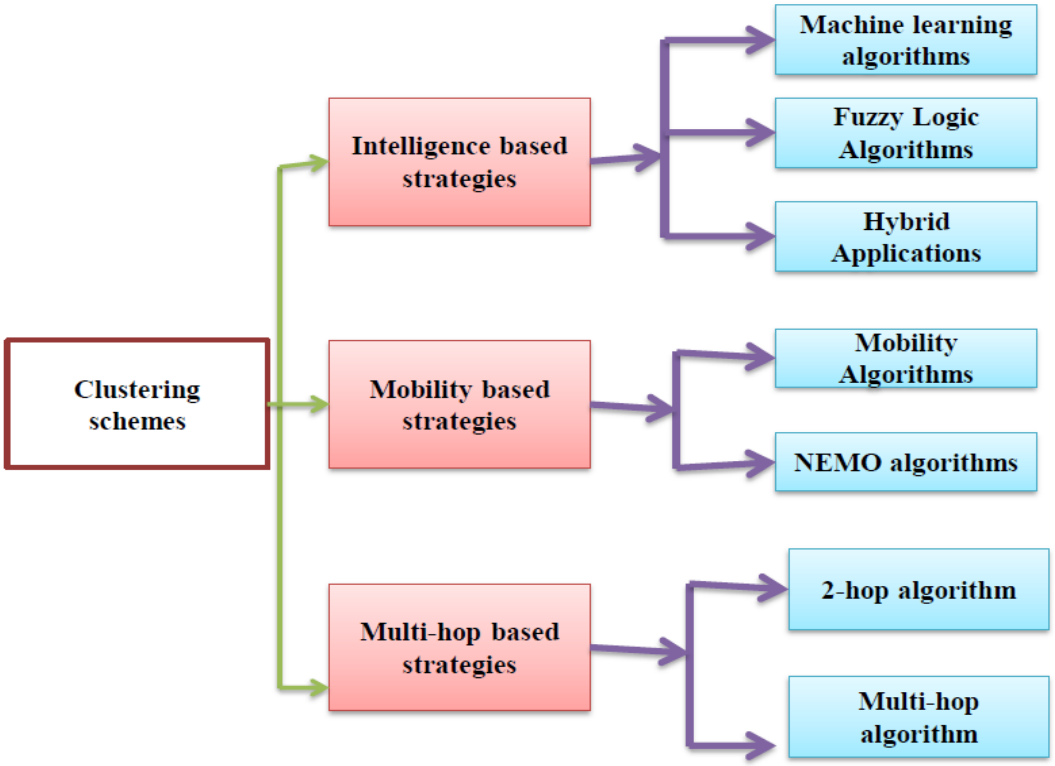


Figure 1.8: Different types of clustering techniques

ii. **Fuzzy logic**

Since the degree of certainty is considered in the VANET system instead of true or false most of the researchers utilized fuzzy logic for the cluster formation. While using the Fuzzy logic five parameters are considered such as moving direction, relative speed, acceleration, and vehicle distance. Following this fuzzification is performed to convert the input metrics to the fuzzy set. Subsequently, fuzzy rules are assigned based on the knowledge obtained to acquire the output fuzzy sets via the inference engine.

iii. **Hybrid algorithms**

This is based on the integration of fuzzy logic and machine learning approaches for cluster formation and CH selection.

iv. Mobility based strategies

This is the most widely used method in VANET where cluster formation is a mobility-based strategy. The parameters such as the position of the vehicle, relative speed, acceleration, etc., are taken into consideration. Since the clusters break down frequently with the high movement of vehicles stability of the clusters is deemed instead of efficacy. Two types of mobility-based strategies algorithms are (i) mobility algorithm and (ii) NEMO algorithm.

v. Multi-hop based strategies

The mitigation of cluster numbers is an important task in VANET. The numbers are reduced with the Multi-hop transmission and the selected CH can be applicable for a larger area to provide stability. There are two types of multi-hop-based approaches, (i) 2-hop algorithm, and (ii) above 2-hop algorithm.

1.7. VANET SECURITY

Vehicle communication is required to connect RSU, vehicles and IoT devices. Communication and transmission are required to link all automobiles for optimal data transfer. Vehicle communication results in new communications technologies known as VANET. Vehicular network offers information among its RSU in VANET. VANET was made up of OBU and RSU. The vehicles transport items in VANET and RSUs are deployed on roadways. The major aim of VANET communications are classified as Infrastructure to Infrastructure (I2I), Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V).

The main concern of VANET is safety security. Here, the security service means communication and transferring that has to be secured. Error detecting, revocable, traceability, access protection, data management, confidentiality, repudiation, transparency, trustworthiness, and security are all provided by security capabilities. The scheme that is presented in the work makes drivers of moving vehicles more aware of

walkways that are close to crossing points (Yu et al. (2011)). The presented system is connected to RSU that are cognizant of the state of intersection and vehicular traffic to the automobiles in order to disseminate information about walk ability existence through traffic. To stop the propagation of erroneous data, RSUs sign the warning signals which are transferred, and all vehicles can verify the fingerprint. It thus establishes stringent real-time contact requirements, such as a least message affirmation time frame for automobiles which enter a crosswalk of involvement, as well as strict safety criteria, such as not replicating warnings. It is advised to manage signature notices using nimble asymmetric cryptography (NAC), which subtly verifies messages that are sent. NAC reduces the need for non - symmetric coffers, which then increase efficiency expenses and are essential for guaranteeing non-reproductive usage.

Only wireless communication allows vehicles to communicate with one another. Based on fixed infrastructure, communications are feasible in V2I via established RSUs and in I2I. RSUs are usually deployed on motorways and highway roadsides to serve as a transmission infrastructure. The example of malicious nodes in the VANET scenario is illustrated in **Figure 1.9.**

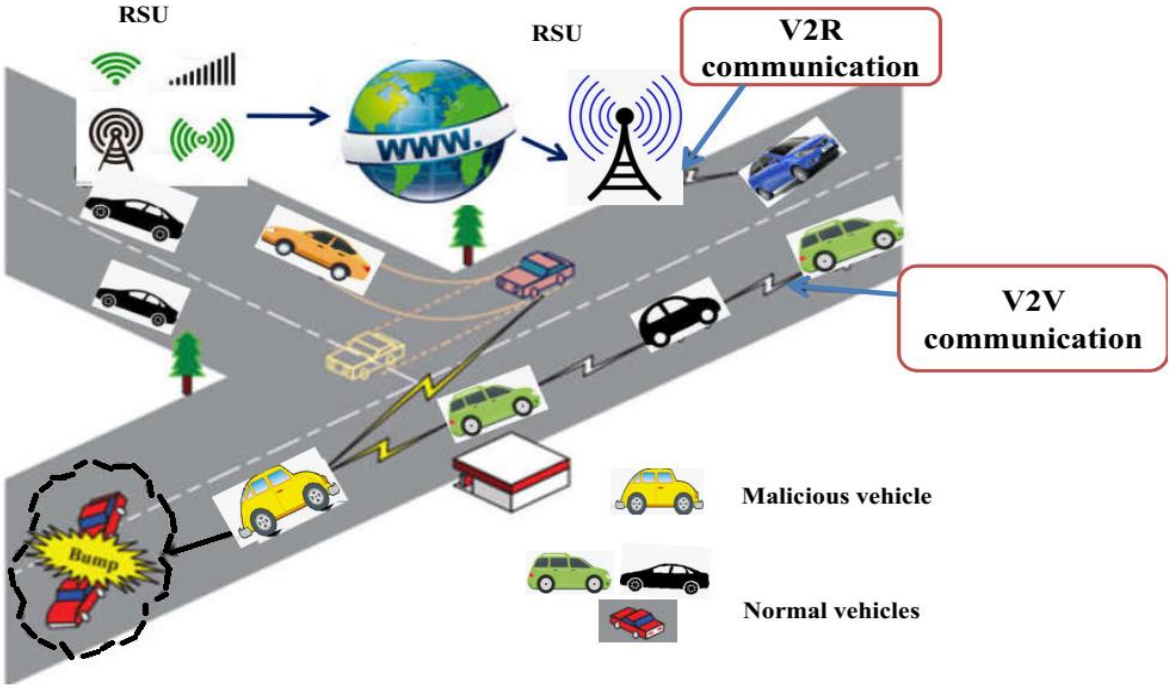


Figure 1.9: An example of malicious nodes in the VANET scenario

1.7.1. Blockchain in VANET Applications

The most emerging distributed storage technology is Blockchain technology. The system privacy and security were effectively improved via blockchain that uses a decentralized consensus mechanism. The data exchange is convenient among the linked smart devices. The blockchain has different applications in different areas such as security trust, privacy protection, identity authentication, and data storage in vehicular networks. Based on blockchain technology, a few of the typical security models are summarized in VANET. Based on the targeted applications, the previous studies state a successful and effective model but it met a few shortcomings such as protection of privacy enhancement and accuracy of detection improvement. Recently, forged message detection and malicious node identifications are performed via blockchain technology. The cooperative behaviors of RSUs were encouraged and designed the privacy protection for vehicles. The network overhead is minimized and enables decentralized management in VANET. The overlay of blockchain for secured routing is depicted in **Figure 1.10.**

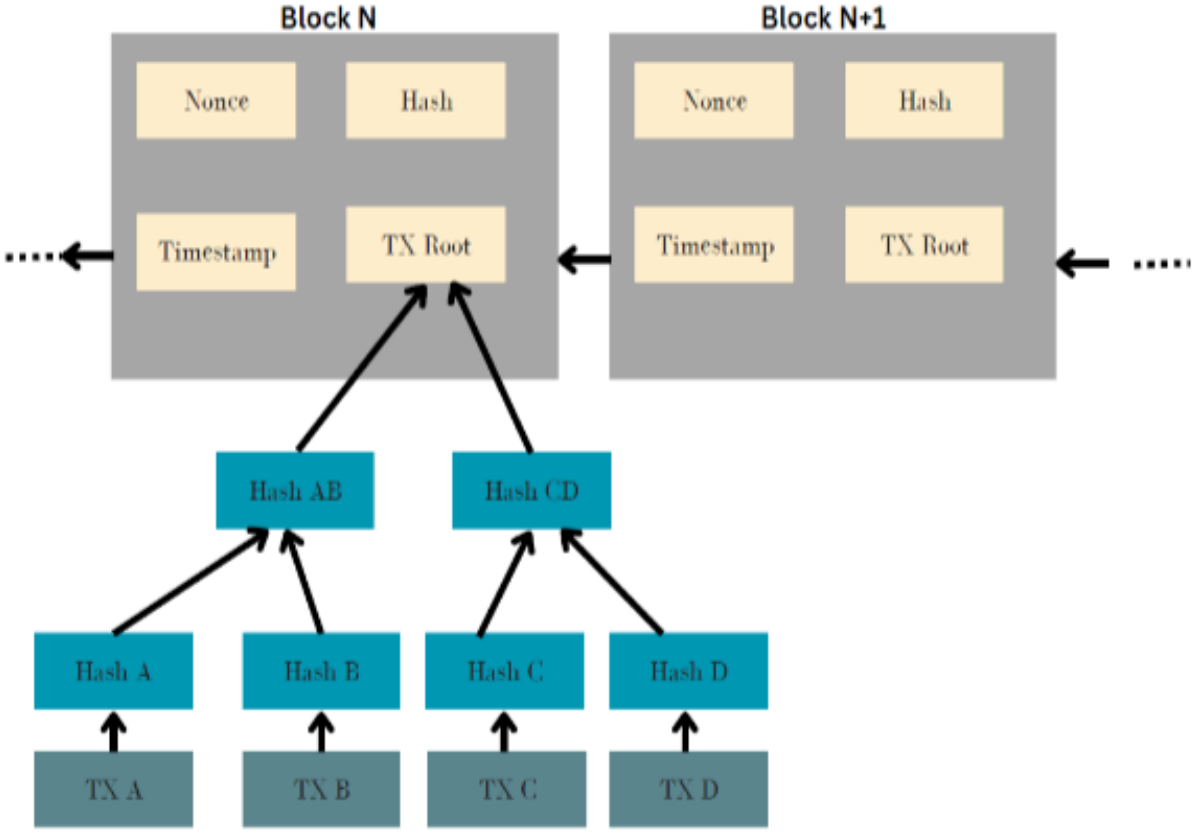


Figure 1.10: Overlay of blockchain for secured routing

1.7.2. Private preserving Encryption Algorithms used in VANET

To enable robust MSDB several computing algorithms were used. Here are some of the algorithms; Role-based Access management, Identity-based Encryption, Attribute-based Encryption, and Shamir's Secret Sharing (SSS) algorithm are some encryption methods.

i. Role-based access control

Access-based control is nothing, but providing information about whether the user/ program has the authorization to access or exchange the services (Alimohammadi et al. (2014)). Role-based access bestows information about the role of the users within the organization. This granted the role of authorization and flexibility to perform the tasks required for their job. This has certain norms like Role Assignment, Role Authorization, and Transaction Authorization.

- **Role Assignment:** Each operation can be carried out by the person, to whom the assignment has been allotted. Roles may be assigned by a separate party or by the user attempting to act (Paliwal et al. (2022)).
- **Role Authorization:** This is to ensure that only the authorized user accesses the assigned project, thereby protecting the data from vulnerabilities. The administration grand permission to access the data by an authorized person.
- **Transaction Assignment:** to exchange data the administration have to assign a particular person from the organization. That individual has the authorization to transact the information.

The concept of Role-Based Access Control is that it proposes R as a middle variable, which separates the subjects and the authorizations (Elsadig et al. (2016)). The certification space of size is divided into two parts: $S \times R$ (the user-role assignment) and $R \times P$ (role-permission assignment), thereby reducing its size, and making the certification more convenient (Waters et al. (2005)).

Distributed Role-based access control (DRABC) is also a standard used to incorporate the user and the service provider. Though it has several protocols and standards to link users and providers, it is not widely used. Since it uses the existing infrastructure and protocols, it is not a commonly used type.

ii. Identity-based Encryption

Identity-based encryption is the simplest form of encryption method. This is a type of public-key cryptography, in which a third-party server uses simple recognition techniques, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. Probably this reduces the complexity of the encryption process for both users and administrators when compared to traditional public-key cryptography. Moreover, the message recipient doesn't need advanced preparation or specialized software to access the key (Canetti et al. (2004)). It works totally depending on the third-party IBE server, which is used to generate the keys. The only information this server stores permanently is indeed a secret master key. The server uses this master key to generate a common set of public-key parameters that has to be given to each user who installs the IBE software, and recipients' private keys as required.

Whenever the sender generates an encrypted message, the IBE software in the system considers three key parameters to trigger the generation of the public key for the message. They include; a starting value, the current week number, and the recipient's identity (mostly the e-mail address). Since the calendar is included, the public key that is produced will get expire automatically.

iii. Attribute-based Encryption

Attribute-based encryption is a type of one-to-many public key encryption. This encryption is based upon attributes such as the country of the user and the kind of subscription to the cloud services. The user whose attributes satisfy the access policy set of the encryptor can decrypt the ciphertext. Here the secret key of a user and the ciphertext dependents on the attributes. So whenever the user wants to access the data stored in the cloud, the attributes of the user key must match the attributes of the ciphertext. Basically, this concept got originated from the Identity-based-encryption (IBE) method. In fact the conventional Attribute-based-encryption (ABE), the key generation phase has all the attribute information of each user which may cause security issues for the user.

To eliminate the above said, the modern method uses the two functions of attribute auditing and key extracting phase. In order to authenticate the attributes of users, the

Attribute Audit Center (AAC) has been introduced. This AAC will authenticate the attributes of users and will produce a blind token for them (Bouabdellah et al. (2016)). This center is only responsible for generating the keys, nevertheless it doesn't know the respective attributes of these keys. The user submits its attributes and relevant evidence to the AAC. The AAC audits the user's attributes and returns a blind token with the signature of AAC to the user. These blind tokens are evidence for users own some attributes. After receiving the blind token, the user submits it to the Key generation center (KGC) (Huang et al. (2009)), which is the technical institution for this encryption. This KGC checks the legitimacy of the token; if the token is invalid, it denies it; otherwise, it executes the key generation algorithm over the token and sends back a blind key. After receiving this blind key from the user, it extracts the secret key locally.

The process involved in ABE is shown below.

a) The client depicts its attributes and most relevant affirmative to the attribute audit center.
b) The AAC examines the user's attributes and sends back a blind token to the user along with its seal.
c) The user submits its blind token to the key generation center (KGC). The KGC cannot involve the user's attributes but it can confirm that the user indeed has related attributes.
d) KGC first verifies the legitimacy of the token, and if the seal is illicit, it denies it. Otherwise, it runs the key generation algorithm and outputs a blind key.
e) The user extricates the private key from the blind key which was received from the KGC.

iv. SSS Algorithm

Since single cloud service provider (CSP) is less popular due to service availability failure and insider attacks, companies in take the multi CSP. Moreover, this service provider has some issues, some algorithms took this to reduce the threats. A secret sharing algorithm is used to constrain access to sensitive and confidential data. Threshold secret sharing algorithm, in which the number of participants in the reconstruction phase is important for recovering the secret. This SSS algorithm is used to secure the encrypted data. The secrets are distributed as multiple shares. To reconstruct or unlock the original secret minimum number of shares is required. For example, a company named BTR needs to

secure its vault's passcode and uses some Advance Encryption Standard (AES), but lost its key or might have been attacked by a malicious hacker or the holder of the unavailable means, then the company losses its ability to access the passcode.

The SSS algorithm does means, first it encrypts the vault's passcode and split it into a certain number of shares. Then these shares are allocated to a certain executive in the company BTR. If anybody wants to access/unlock the passcode, one should gather all the shares and thereby unlock the passcode. Thus the SSS algorithm reduces the complication in computing using multiple CSP.

- **Basic concepts in the SSS algorithm:** Shamir's Secret Sharing algorithm is used to provide secure communication among two shared parties. Already mentioned, the information is stored by sharing it into N number of secrets and it is shared to a certain number of people in that organization. So, the basic concepts of SSS are Secret, Share, and Threshold which is given below.
    - **Secret:** The secret may be in any form multimedia, text, or number that is to be shared secretly.
    - **Share:** Dividing the information into a number of pieces.
    - **Threshold:** The number of shares required to derive the original information literally depends on this threshold value.

These algorithms are used to safeguard the privacy of the user, by providing certain protocols for their security. Moreover, these approaches reduce the complexity of data exchange.

1.8. AI BASED APPROACH FOR VANET INTRUSION DETECTION

The intrusion attacks in VANET can be detected by utilizing Artificial Intelligence (AI) techniques. AI approaches are categorized as machine learning approaches and deep learning approaches. The details are explained in the following section.

1.8.1. Machine Learning Techniques

Machine learning approaches involve two types of learning approaches (i) supervised learning and (ii) unsupervised learning. A few of the machine-learning approaches are explained in the following section.

i. K-nearest Neighbor Algorithm

It is a type of data mining algorithm with low computational complexity. The idea behind this type of algorithm is that in the network the nearest nodes are in the same class then it automatically groups the nodes to form a cluster. (Li et al. (2014)) stated the intrusion detection in VANET by using the KNN classification algorithm. While conducting the detection operation the vectors are indicated as nodes and represented as N1, N2,…Nn. The normal nodes are identified easily since they possess the same characteristics and thus distinguish the abnormal nodes. It utilizes two types of parameters as k value and the cutoff value. The cutoff value denotes the threshold value and differentiates the abnormal nodes from the normal and the K value denotes the nearest adjacent nodes.

ii. Support Vector Machine

Support Vector Machine (SVM) usually divides the datasets into two categorized testing and training sets. SVM is mainly used to design a model with the help of a training dataset and thus predicts the targeted values. SVM is memory efficient and is used to detect intrusion in many applications. Nonetheless, it is arduous to use SVM in a noisy environment and with overlapping networks. Sharma et al. (2021) suggested a novel approach known as SVM based immune algorithm to detect intruders from the VANET.

iii. Decision Tree Algorithm

It is a type of supervised learning algorithm and is used to solve regression and classification issues. In the decision tree, the detection of abnormal nodes starts from the root node and compares the attribute values with the recorded values (Mahbooba et al. (2021)). If both values are appeased the decision tree will add the node to the safe node and jump into the other node. There are two types of decision tree algorithms. Categorical variable tree algorithm and Continuous variable tree algorithm.

1.8.2. Deep Learning Techniques

The deep learning technique (Singh et al. (2022)) is a combination of both machine learning and artificial intelligence algorithm and imitates human beings in several types. It is an important technique to detect different types of attacks in the VANET since it involves both statistics and predictive approaches. It is otherwise known as automatic predictive analysis. In machine learning, the learning process is supervised and the programmer has to set the type of object to be detected. This also includes the feature

extraction process. However, in deep learning, the program itself builds the feature set without the inclusion of anyone's supervision. Thus it not only achieves faster-unsupervised learning but also the results are more accurate. The below sub-section explains a few of the deep learning techniques.

i. Auto-encoder

It is a three-layered unsupervised neural network that contains the input layer, hidden layer, and output layer (Kanazawa et al. (2019)). The output layer is also considered a reconstruction layer. It can effectively convert particular feature vectors into abstract feature vectors. That is transforming the high dimensionality nonlinear data into low dimensionality data space. Meanwhile, the auto-encoder follows two stages namely encoding and decoding.

ii. Artificial Neural Network

This type of algorithm utilizes the characteristics of the human brain (Zhang et al. (2018)). Hence the structure is totally different from the digital computing technology. Moreover, the Artificial Neural Network (ANN) itself arranges some structure to perform computational activities such as pattern recognition and is much better than the computational activities. There are different types of artificial neural networks that are used in many applications like pattern recognition, intrusion detection, medical applications, and so on. Most often the neural networks involve a trial and error process and hence they utilize an enormous amount of data while performing the training process. The data that are exploited during the training process are labeled and hence it is made easier for the model to perform accurately.

iii. Multi-Layer Perceptron

Multi-layer perceptron (MLP) is introduced to overcome the limitations of the single-layer perceptron. In this more neurons are interlinked in a cascaded form. The MLP includes layers such as the input layer, hidden layer, and output layer. The input layer consists of n number of nodes and forwards the input to the hidden layers. The neurons in the hidden layer will estimate the calculations and forward them to the subsequent units. Then the output is accessed through the output layers. Anzer et al. (2018) utilized the MLP algorithm to detect intrusion in VANET.

1.9. RESEARCH OBJECTIVES WITH ITS PROBLEMS

Several methods based on intrusion detection systems have been developed over the past few decades to address security flaws. In general, the analysis of traffic data and attack detection are done using a variety of machine learning methods, including support vector machines (SVM), random forests (RF), K-nearest neighbors (KNN), ensemble learning, and others, as well as deep learning methods, including convolutional neural networks (CNN), deep neural networks (DNN), long and short term memories (LSTM), deep belief networks (DBN), and others. There is currently no comprehensive analysis of how Machine Learning (ML) and Deep Learning (DL) approaches can help academics and professionals to navigate dissemination safety in VANET, despite the fact that ML techniques improve reliable detection procedures.

By utilizing it in the VANET domain, blockchain is able to address the security issue. It maintains contracts and processes data more quickly for secure contracts. Data is stored in the blockchain for prediction and analysis, to assess the accuracy of artificial intelligence's classification and feature-based categorization in blockchain configuration. Machine learning predicts the correct features and also manages the protected information on a smaller scale. The data is distributed throughout the network in a clear, secure, and traceable manner. Time- and energy-consuming, scalable, and difficult are the drawbacks.

The research objectives are:

- To intend a security-based collaborative intrusion detection system in VANET by using an optimized support vector machine.
- To propose an optimized convolution neural network based privacy collaborative intrusion detection system for vehicular ad hoc network using blockchain.
- To assess the comparative analysis in terms of accuracy, energy consumption, delay and security with blockchain.
- To design and implement a computer simulation technique based on the proposed method.

1.10. RESEARCH CONTRIBUTION

Three steps make up the suggested structure. This research study's main contributions are as follows:

- In phase 1, investigation of the existing research gaps to identify the threat issues in VANET. Defamation activity in VANET is detected here.
- In phase 2, both cluster formation and cluster head selection in VANET is performed using the K-means algorithm and Tabu Search-based Particle Swarm Optimization (TS-PSO) algorithm.
- The implemented blockchain will improve security and dependability. Additionally, the trust-based collaborative intrusion detection on the VANET can be achieved by adopting the ingenious War Strategy Optimization (WSO) based Support Vector Machine (SVM) model (Optimized SVM).
- In phase 3, both cluster formation and cluster head selection in VANET is performed using improved K- harmonics mean clustering (IKHMC) and hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm.
- After that, collaborative blockchain-based solitude conservation is performed, and enhanced CNN is used for VANET intrusion detection.

1.11. THESIS ORGANIZATION

The thesis organization of blockchain based collaborative intrusion detection system in the vehicular ad-hoc networks is delineated below:

Chapter 1: Introduction

Chapter 1 explains in general introduction of collaborative intrusion detection in vehicular ad-hoc-network, safety analysis and secrecy preservation.

Chapter 2: Literature Survey

Chapter 2 demonstrates the brochure analysis of collaborative intrusion detection in VANET and attack detection using both machine learning and deep learning models is reviewed.

Chapter 3: **Investigation of Intrusion Detection Systems in Vehicular Ad Hoc Networks**

Chapter 3 analysis different algorithms to detect the present malicious attacks on VANET.

Chapter 4: Collaborative-based vehicular ad hoc network intrusion detection system using optimized support vector machine:

Chapter 4 describes the collaborative-based vehicular ad hoc network intrusion detection system by adopting an optimized support vector machine.

Chapter 5: Optimized convolutional neural network-based privacy-based collaborative intrusion detection system for vehicular ad hoc network:

Chapter 5 delineates an optimized convolutional neural network-based privacy-based collaborative intrusion detection system for vehicular ad hoc networks.

Chapter 6: Result and Discussion

This chapter compares the apt technique suitable for intrusion detection system.

Chapter 7: Conclusion & Future Works

The overall outcomes of both works are described in this section as well as the limitations and future work is mentioned.

CHAPTER 2
LITERATURE REVIEW

2.1. OVERVIEW

One of the major significant subsets of MANETs is Vehicular Ad hoc Networks (VANET).A VANET is a network of cars that are wirelessly connected to one another. In recent days, the major issue is VANET security. A minor privacy weakness can result in a massive life loss. For detecting any intrusion, implement Intrusion Detection Systems (IDS) in VANETs to ensure security. If an obnoxious node is available, the IDS analyses the system and detects it. This chapter provides a detailed assessment of the most significant and relevant intrusion prevention scientific studies, in addition to a comparative evaluation of the approaches used to detect invasions and targeted attacks.

2.2. RELATED WORKS BASED ON COLLABORATIVE INTRUSION DETECTION IN VANET

The collaborative intrusion detection model in VANET based on the existing works is reviewed in this section. Literature survey of VANET is depicted in **Figure 2.1**. From this, the existing studies are categorized into cluster-based, machine learning and deep learning-based collaborative intrusion detection models in VANET, which are reviewed as follows:

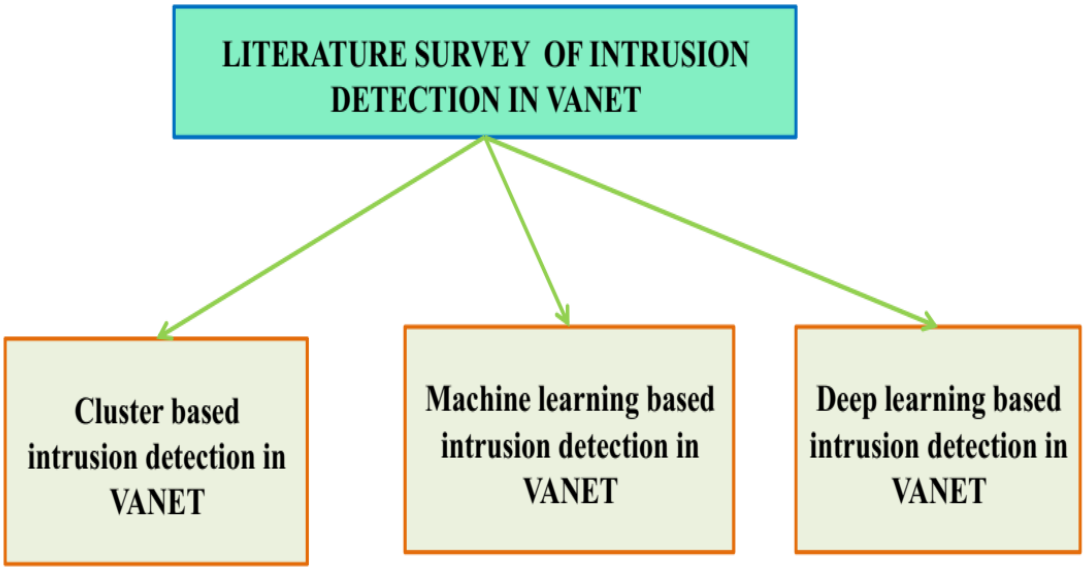


Figure 2.1: Literature survey of VANET

2.2.1. Cluster-based Intrusion Detection in VANET

Saleem et al. (2019) have described a Cognitive Radio (CR) vehicular Adhoc network from a fuzzy cluster head selection strategy that employs a spectrum sensing algorithm based on cognitive radio technology. The correlation is excluded to utilize the free spectrum of secondary and primary users from the network connectivity level, vehicles, velocity, and distance are the input parameters. It is efficient, stable, clear, secure, and reliable. However, for better performance, the clustering time should be improved.

Maan et al. (2021) have demonstrated a 2-level approach for Primary User detection in the network. The trust value is gained to detect the spectrum of vehicles to vacate the primary vehicle of the network. The cluster head has the best likelihood for the selected trust factor to determine the signal energy of the cluster head executing the network layer of security. The cluster time and false detection detect the higher probability. Thus, the cluster head stability should be increased.

Ucar et al. (2015) suggested the Vehicular Multi-hop algorithm (VMaSC) for stable clustering to observe and calculate the mobility, and speed of the clusters. Multiple hops are introduced to determine the speed of nearby vehicles and the cluster is connected directly to form the minimum packets of information. The efficiency, reliability, and stability are enhanced and the clustering information is interchanged. Hence, the uses of the urban traffic framework are investigated.

Azizian et al. (2016) highlighted a D-hop clustering algorithm (DHCV) to classify the clustering vehicles in non-overlapping sizes of mobility. The cluster head hops the vehicle to each cluster from the cluster head. The nearby proposed measures for the mobility of the vehicle network intervals are formulated. By using this algorithm the stability will be more to form the clusters from the clustering algorithm. Moreover, the network performance degrades the wireless networking management.

Duan et al. (2017) has introduced an adaptive transmission scheme based on modulation and power control selection. The vehicle clusters are covered by cluster design and dynamic beam forming to communicate and cluster the network capability. The distribution and aggression decreases the latency to transmit the base station and cluster

head. The latency is decreased to increase the method. Hence, the complexity is higher due to varying network topologies.

Elhoseny et al. (2020) has performed a K-Medoid Clustering model based on clustering the energy and vehicle nodes to recognize the communication. The nodes are adjusted to cluster the vehicle and energy nodes to transfer various methods to each node to process the network of the base station. Since the energy consumption is less it drops minimum energy. However, the performance of clustering should be enhanced for other frameworks.

Host-based intrusion detection (H-ID) model using k-means clustering model was introduced by Zaidi et al. (2015). The huge data set is represented through statistical and graphical methods. Using various traffic conditions, the rogue nodes are quickly found. Cooperative information indicates that the application layer IDS was examined and assessed in light of the most recent findings. The computational complexity was higher since there was more vehicle data.

Kolandaisamy et al. (2021) suggested a cluster-based routing with a Stream Position Performance Analysis (SPPA) approach to monitor information sent by field stations. The vehicle of every weight is accessed to calculate the weight and detection of nodes to examine the detection and intruder of normal nodes. This method decreases the transparency of end-to-delay and it can also be considered as a complex method to enhance network routing. The classification are identified to detect the attack effect.

Ren et al. (2017) evaluated a new dynamic mobility-based and stability-based clustering scheme based on an urban framework to link the estimation, direction, and position. The velocity, distance, direction, and mobility of clustering formation are different in cluster heads. To control the size of the cluster the safe distance threshold formats the performance of the clustering field. The clustering performs the dynamic framework to cluster with higher stability. Moreover, it is not applicable to implement recent techniques.

Bangui et al. (2021) introduced the hybrid data-driven model to diagnose VANET intrusion. The rapid growth in processing power contributes to better IDS performance.

The post-detection step is assisted in the identification of potential new entrants. Through the use of a hybrid data-driven model, the corsets-based clustering and data classification are integrated. Although there is less computational overhead, the process of execution takes longer and more difficult.

The novel clustering algorithm and the multi-layered game theory model were suggested by Subba et al. (2018) for IDs in VANET. The specification rules minimizes the communication overhead. For detecting malicious vehicles, the classifier module of a lightweight neural network was introduced to detect the malicious nodes. The interaction between the malicious vehicle and the IDS modeling minimizes the IDS traffic volume. The experimental outcomes demonstrated higher scalability and dynamic network topology. Based on a wide range of attacks, a higher attack detection rate and accuracy were obtained.

For cluster-based intrusion detection, Muthumeenakshi et al. (2022) suggested the fuzzy C-means (sparse FCM) clustering algorithm in VANET. The intruder in VANET was detected via the adaptive elephant fuzzy system (AEFS) model in which the cluster head was selected. The communication was enabled and detected intruders. The experimental results provided 1.4593 minimal verification delays, 354.4174 minimal transmission overhead, 1.2059 minimal service response and 95.6829 maximal detection rate by using the AEFS model but it needs a strong security concept.

In cluster-based VANETS, an energy-efficient IDS model was introduced by Indira et al. (2015). For the whole network, the audit data was analyzed, logged and collected via IDS. The own log data to determine anomalies were analyzed that run on a local decision engine. The cluster head was selected and monitored and randomly grouped the direct link nodes. Instead of running on each VANET node, an intrusion detection model was executed. It demonstrated a tolerable stage of security and minimum power consumption with limited resources.

In VANET, Sharma et al. (2018) suggested a multi cluster head dolphin swarm optimized IDS-based hybrid fuzzy multi-criteria decision-making model. TOPSIS methods and the Fuzzy Analytic Hierarchy Process (AHP) were combined and used for optimal decision-making. Furthermore, because VANET is associated with life-essential applications,

security architecture to identify various malicious assaults is critical. To enhance their performance, these intruder detection-based mechanisms can indeed be integrated with different existing optimization techniques, including the Dolphins Swarm Algorithm. Better performances can be achieved in terms of detection time, detection rate and false positives in which the communication is hampered by different security issues.

The clustering with a spline-based intrusion diagnosis representation was recommended by Schmidt et al. (2020) for knot flow classification in VANET. IDSs are critical components for detecting and mitigating assaults on computer systems. Because of the evolving environment of their customers and the amount of data transferred between them and their respective infrastructures, VANETs are especially challenging to safeguard. An essential building block IDS has been developed as a potential approach to achieve these objectives. The experimental outcomes accomplished in terms of detection accuracy, precision and recall and it needed more resource allocation.

For efficient and intelligent broadcasting in medical surveillance based on VANET, Ramalingam et al. (2020) introduced a mutated k-means algorithm with a selective reliable broadcast protocol. Various forms of the K-implies computation are commonly used for clumping, but because of the constantly developing topology, such computations could be tied directly to VANET. The strategy works beautifully with both the fixed number of groups in advance and the unknown number of organizations. The customer does have the flexibility to choose the number of bundles or the minimum amount of groups needed. The following conclusions have been drawn regarding the new bunch focus by increasing the group count to one in each concentration till the goal work is completed. This model resolves the relationship between CMs and CHs by expanding the group counter and higher computational complexities.

Kumar et al. (2014) suggested clustering-based collaborative trust-aware intelligent intrusion detection. Learning Automata is believed to be placed on network automobiles to collect data on the various states of passenger vehicles. A Markov Chain Model is built to describe events and subsequent changes in a system. Changes from one state to another are determined by the number of cars in a certain area. A novel classification was created to recognize any malicious activities in the system and is adjusted using a brand-new tagline as the Cooperative Trusted Index to cover all potential sorts of attacks. Compared

to other existing schemes, this model demonstrated good results in terms of communication overhead, detection ratio and false alarm ratio with higher feature dimensionality.

For efficient reprogramming in VANET, Santhosh Kumar et al. (2021) introduced an energy-efficient secured unequal fuzzy and K means clustering algorithm. Furthermore, the RBSP causes an issue with too many senders and receivers and increases network energy usage. The two most difficult challenges in data dissemination were delivering energy security and efficiency. In such a case, the attackers may exploit a flaw in the show's protective measures and engage in unauthorized actions to interrupt the multicast routing process. The experimental results revealed better effective key management, trust-based security enhancement and cluster head selection. But it demonstrated higher delay and energy consumption.

Amirat et al. (2018) introduced fuzzy clustering to detect misbehavior in VANET. For geographic routing protocol, selective forwarding attackers in VANETs were identified to represent lightweight misbehavior detection models. Malicious cars, based on this attack, behave like regular nodes but deliberately drop data. It starts with a previous step that enables it to get a collection of characteristics from a data packet created by the simulation being run. Fuzzified employs the FC-Means technique to generate groups of healthy and attack basis of distance on retrieved attributes. Under the attack's intensity of 25% of the total number of nodes, the low false positive rate and 87% of accuracy were achieved. Many privacy issues may interfere with data reception by discarding, modifying, or delaying communications.

To predict the security index in VANET, Bensaber et al. (2020) established Adaptive Neuro-Fuzzy Inference System (ANFIS) modeling and design. The ANFIS layer manages increasingly complicated variables derived from variable elimination using the APC. This demonstrates the usefulness of the protection index's rapid departure from typical network behavior and its consequences when a vehicle is attacked. If combined with an exceptional situation surveillance system, this prediction model improves attack patterns in the actual period. This model demonstrated a high-level and intuitive mechanism with good stabilization and dynamic performance but it attains higher

computational complexities. The summary analysis based on clustering techniques for collaborative intrusion detection in VANET is depicted in **Table 2.1.**

Table 2.1: Summary analysis based on clustering techniques

Author	Methods used	Advantages	Limitations
Saleem et al. (2019)	Fuzzy cluster head selection strategy	This method is effective, clear, stable, secure, and satisfying.	It takes lot of clustering time
Maan et al. (2021)	Fuzzy logic clustering	Cluster time and false detection detect the higher probability	Cluster head stability needs upgraded for better performance
Ucar et al.(2015)	VMaSC	The Efficiency, reliability, and constancy are embellished and the clustering information is interchanged.	It causes Higher computational cost and complexities
Azizian et al. (2016)	D-hop clustering algorithm	The Non-overlapping sizes of mobility is specified systematically and with good stability mew clusters can be formed.	Hard to manage the network model
Duan et al. (2017)	Adaptive vehicle clustering and beamformed transmission	Higher performance efficiency is achieved with minimum latency.	The Complexity of the cluster is higher due to varying network topologies
Elhoseny et al. (2020)	K-Medoid Clustering model	It recognizes the communication of the energy and vehicle node. Nodes are adjusted to cluster the vehicle and energy nodes and transfer various ways to each node to process. It drops minimum energy.	Low reliability and performance enhancement is required.

Zaidi et al. (2015)	K-means clustering model	It has Good scalability and detection accuracy	Computational period gets higher due to more vehicle data.
Kolandaisamy et al. (2021)	Cluster-based routing and Stream Position Performance Analysis (SPPA)	It access, calculates and detects vehicle nodes. The Transparency of end-to-delay is subsided and network routing is amplified.	It has some Computational difficulties and more unwanted features
Ren et al. (2017)	Dynamic mobility-based and stability-based clustering scheme	Higher stability of cluster heads and it has good clustering performances	New techniques are not applicable so it has Hard implementation processes
Bangui et al. (2021)	Corsets-based clustering	This increased the accuracy of detection with Less computational overhead	Complex and longer execution and no proper security explanation.
Subba e al. (2018)	Novel clustering algorithm and the multi-layered game theory model	A lightweight neural network helps to detect malicious nodes. The reciprocal action minimizes the IDS traffic volume. It has higher scalability and dynamic network topology	It has less attack detection rate and accuracy
Muthumeenakshi (2022)	Fuzzy C-means clustering algorithm	It has a result of minimal verification delays, minimum transmission overhead and least service response.	It has maximal detection rate and hence strong security concept is needed.
Indira et al. (2015)	Energy efficient IDS	As a result of an intrusion detection model enforcement, tolerable stage of security and minimum power consumption was manifested.	It has only limited resources.

Sharma et al. (2018)	Multi cluster head dolphin swarm optimized IDS based hybrid fuzzy multi-criteria decision making model	To enhance their performance an intruder detection-based mechanisms can consolidate with different optimization techniques. So, better performances in terms of detection time, detection rate and false positive is achieved.	Since it combines with many techniques the communication is hampered by different security issues.
Schmidt et al. (2020)	Clustering with spline-based intrusion detection model	An essential building block is developed to meets its objectives. The causatum is superior in terms of detection accuracy, precision and to recall performances.	This method needs more resources allocation
Ramalingam et al. (2020)	Mutated k-means algorithm	Flexibility to choose what is needed. It increases the group count till goal work is completed. It also resolves the relationship amongst CMs and CHs with expanding the group counter.	It has higher computational complexities.
Kumar et al. (2014)	Clustering based collaborative trust aware intelligent IDS	Learning automata is introduced to collect data. Changes are monitored and malicious attacks are detected. It confirms good results in terms of communication overhead, detection ratio and false alarm ratio.	It has higher feature dimensionality

Santhosh Kumar et al. (2021)	Energy efficient secured unequal fuzzy and K means clustering algorithm	It has better and also effective key management. It has a trust based security enhancement and cluster head selection.	Too many senders and receivers increases network energy. It has two main challenges of delivering security and efficiency.
Amirat et al. (2018)	Fuzzy clustering	FC- means technique is employed to spot violation as a result of minimal proposition of false positive and 87% of accuracy are achieved.	Many privacy issues may interfere with data reception by discarding, modifying, or delaying communications.
Bensaber et al. (2020)	Adaptive Neuro-Fuzzy Inference System	It manages complicated variables. It improves attack patterns with high-level and intuitive mechanism with good stabilization and dynamic performance when combines with a n exceptional surveillance system.	It accomplishes higher computational complexities and more time execution

2.2.2. Machine Learning Techniques based Intrusion Detection in VANET

Mehmood et al. (2017) described an intelligent naïve Bayesian probabilistic estimation practice for traffic flow and clustering to employ the traffic flow and intelligent technique. The cluster is stable to determine the cluster head for various traffic flow schemes by connectivity, direction, information, and alteration. The performance and stability are increased when compared with various algorithms. Thus, the stability of the cluster head is increased due to the high movement of vehicles.

Khan et al. (2018) highlighted an Evolutionary Game Theoretic (EGT) framework to nominate the cluster nodes and heads to execute the stability of clusters. The average number of clusters maintains the throughput and clusters balance the sizes. The

equilibrium point is tested and analyzed to perform different clustering functions. The performance is stable and efficient to develop the clustering algorithm. However, the different routing protocols failed to examine the network stimulator.

Bangui et al. (2021) delineated a novel Intrusion detection system (IDS) based on the hybrid ML approach known as the Random Forest approach incorporated with Coresets and clustering approach. The authors utilized the CICIDS2017 dataset for the performance analyzed and achieved efficient performance for the taken dataset; however, the authors failed to verify the system with the real-time dataset.

A trust-based collaborative IDS has been stated by Nandy et al. (2020). The stated approach follows the structure known as the score table of other vehicles to detect the existing network pattern. The real-time data gathered were analyzed with the local IDS agent who utilized the K-nearest neighbor's nonlinear classifier. Following this, the vehicle will update its score table used for future vehicles. The author stated that the proposed work achieved better performances in terms of intrusion detection. The computational cost is high in terms of designing the stated work.

The invalidity ratio of packet transmissions in VANET is demonstrated by Alsarhan et al. (2021) who merged the previous and current evidence to estimate the trustworthiness of nodes and data. It follows four stages such as rule-based security filter, Dempster–Shafer adder, node's history database, and Bayesian learner. The authors stated that the security of the stated work shows higher efficiency for small-scale datasets and low efficiency for big data as well as real-time data.

The betrayal attacks of VANET have been detected with the new approach which was presented by Zhou et al. (2020) as distributive collaborative IDS. The collected data were tracked with the distributive collaborative detection framework and to enable a stable and reliable communication a link has been achieved with the reputation-based cooperative communication approach. Henceforth, the invariant data has been derived with the help of dynamic behavior analysis technology, further; Stochastic Petri Net is used to analyze the security. The detection rate and faster attack detection rate are higher with the reduced false alarm rate. However, the computational complexity regarding field tests is higher.

Bangui et al. (2022) suggested a hybrid machine learning model to diagnose VANET intrusion. The accuracy of IDS was enhanced using the Random Forest (RF) models. It significantly increases the precision of discovery using the CICIDS2017 dataset when compared to the prior approach. Although the computational speed and detection accuracy improved, no security concept was described as a result. Gad et al. (2021) introduced the ML technique based on the ToN-IoT dataset. Using this ToN-IoT dataset, both multi-class and binary classification problems were quickly resolved. Class balancing was achieved by Synthetic Minority Oversampling approach. The complexity overall rose with greater feature dimensionality.

The intrusion detection in VANET is performed using watchdogs, which was suggested by Hortelanoet al. (2010). Because of its protocol independence architecture, the component is interoperable with all common routing ad hoc protocols. When reducing a created false negative and positives, previous properties were guaranteed. There is low recognition latency and better detection coverage is encompassed. In order to attain a satisfactory balance between detection latency and coverage of watchdog, a set of trade-offs were adopted. The overall process is less dynamic and failed to enhance the tolerance threshold method.

Lihua (2022) suggested machine learning methods to detect energy-aware intrusion in VANET. For communication among existing vehicles, the energy-efficient end-to-end points and safe were determined. Based on the NSLKDD dataset, this approach was evaluated by applying the regression algorithm. The execution time was minimized as well as both accuracy and precision performances get increased but it needed higher quality priority and optimal energy consumption as well as accuracy.

Zeng et al. (2018) suggested machine learning-based intrusion detection. The high mobility environment communicated with the Road Side Units (RSUs). While the intruders go beyond superior units such as cluster heads and RSUs, the machine learning-based intrusion detection model is robust to environmental variations. Nevertheless, this model required robust and real-time intrusion detection techniques.

In VANET, Belenko et al. (2018) introduced a generation of synthetic datasets to detect intrusion detection using machine learning techniques. Some specific cyber-attacks were

targeted and the simulation platform NS-3 simulator was used. The artificially created datasets were utilized to train the VANET intrusion detection that employs machine learning to find safety concerns in brand-new car-to-car ad hoc systems. Results from simulations have demonstrated the efficacy of the presented technique. Higher expensive datasets failed to introduce any valuable security concepts to prevent security attacks in VANET.

Gonçalves et al. (2021) created the VANET intrusion detection system context using a machine learning model. The publicly accessible VANET datasets were assessed based on the region. Utilizing conventional technologies that can help in danger and it is the far more preferred security strategy. Alsatian et al. (2021) recommended an SVM-based intrusion detection solution for VANET. In comparison to previous approaches like PSO, ACO, and GA, this technique surpassed accuracy in classification with better intrusion detection model and longer execution time.

For Intrusion Detection System in VANET, Mahalakshmi et al. (2020) suggested N-Bayes algorithm-based feature selection of variables for ML models to identify and sort misbehavior clusters. The usage of selecting features enhanced the overall identification of the believability tests while using the Feature Importance and Additional Trees Classification Classifier. Throughout this approach misbehaving networks were identified which also employed the N-Bayes Method for feature identification. This model outperformed better security and accuracy. But the speed, time and position were within a communication range.

Alshammari et al. (2018) suggested a K-nearest neighbor and support vector machine to detect intrusion in-vehicle systems. Campus Area Network is a highway communication system that establishes a framework for efficient and reliable concurrent transfer within parts. The signal comes from one node to another via the CAN network, but somehow it lacks information about the source and destination addresses for verification. As a result, the hackers can simply insert any signal to cause system failures. This research offers ML strategies using SVM and KNN methods to group and classify intrusions in VANET. This model minimizes the waiting time on the road and improves driving efficiency and comfort but the lack of centralized infrastructure leads to vulnerability to various security attacks.

Ghaleb et al. (2020) introduced distributed ensemble learning to detect on-demand collaborative IDS. Such that, automobiles employ the randomized forest technique to build localized IDS classifications and then communicate them on-demand with several other automobiles in proximity, reducing network costs. Once delivered, the accuracy of a classifier is tested in the recipient vehicles using the regional testing dataset. The experimental studies outperformed communication overhead reduction and better accuracy with higher cost and delay.

For fault detection in VANET, So et al. (2018) introduced a random forest (RF) model to integrate plausibility. Automobiles build local IDS classifications using the RF approach and exchange their qualified local classifications on request. In the receiving vehicle, the local testing dataset evaluates the performances of the classifiers. The assessment results are employed to rate the supplied classifications as a reliability element. Classification techniques that differ substantially from the lower limit of the crate plot are eliminated from the collection of partners. The results reveal that MA-CIDS outperforms other existing systems with respect to efficacy and effectiveness for VANET. It has minimum communication overhead with better effectiveness but it failed to enable security

Ercan et al. (2021) introduced a machine-learning model called Random Forest and k-Nearest Neighbor to detect misbehavior detection in VANET. Ensemble Learning is used to increase detection by combining multiple ML algorithms, in this case, kNN and RF. An intrusion detection system (IDS) is built to allow cars to detect misbehavior in a dispersed manner, whereas the detection technique is taught remotely. The attack detection and classification accuracy was higher and lower feature dimensionality but numerous concerns about privacy can obstruct data receipt by deleting, altering, or postponing communication.

To detect misbehavior in VANET, Sultana et al. (2022) introduced a machine learning model. The risk of misbehavior rises with several faulty messages and inaccurate malicious vehicles broadcast with the increase in the number of vehicles. This model demonstrated superior detection accuracy with minimum energy consumption. It failed to encrypt the data and made many security attacks hence it requires a misbehavior detection mechanism. **Table 2.2** tabulates the literary interpretation based on ML techniques for collaborative intrusion detection in VANET.

Table 2.2: Literary interpretation based on machine learning techniques

Author	Methods used	Advantages	Limitations
Mehmood et al. (2017)	Bayesian probabilistic estimation	The cluster is stable for different traffic flow as regulated. Thus, the strength and performances are raised.	The stability of the cluster head is to be increased. It may cost a lot and minimum security is applied.
Khan et al. (2018)	Evolutionary Game Theoretic (EGT) framework	The average number of clusters maintains the throughput and clusters balance the sizes. The equilibrium point is analyzed with different cluster functions. The efficiency is stable.	The network stimulator failed to examine different routing protocol.
Bangui et al. (2021)	Hybrid ML approach	CICIDS2017 dataset was used to examine the performance of the data. It acquired efficient performance and higher detection accuracy.	The manifestation of the system with the real-time dataset was denied.
Nandy et al. (2020)	K-nearest neighbors nonlinear classifier	The existing network pattern is detected by the score table of other vehicles. The analyzed work resulted in better performances in terms of intrusion detection.	In terms of designing the work has high computational cost.
Alsarhan et al. (2021)	Bayesian learner	The fixedness of data and nodes are estimated following four stages. The security of the work has higher	The security of the work has low efficiency for big data

		efficiency for small-scale datasets.	
Zhou et al. (2020)	Machine learning models	Stochastic Petri Net analysis the security. The performance is stable with detection rate and faster attack detection rate being higher along with reduced false alarm rate and reliable communication link	The computational complexity in the field test and the cost both are higher.
Bangui et al. (2022)	Hybrid machine learning model	It identifies VANET intrusion. The RF model increases the accuracy of detection. The computational speed and detection accuracy are improved.	As a result no security concepts are described.
Gad et al. (2021)	Machine learning models	ML technique was introduced based on ToN-IoT dataset. It quickly resolved both multi-class and binary allocation issues. Class balancing was achieved by the Synthetic Minority Oversampling approach.	Overall complexity rose with greater feature dimensionality.
Hortelanoet al. (2010)	Watchdogs	Low recognition latency and better detection coverage was encircled. A set of trade-offs were adopted to accomplish the satisfactory balance between detection latency and coverage of watchdog.	The complete process is less dynamic but failed to enhance the tolerance threshold procedure.
Lihua (2022)	Machine learning methods	Regression algorithm was applied to evaluate this approach. Minimum	More computational complexity and higher

		execution time, better accuracy and precision, with optimal energy consumption was achieved.	quality priority are expected for this process.
Zeng et al. (2018)	Machine learning-based intrusion detection	The high mobility environment connect with the Road Side Unit. This intrusion detection model is robust to environmental variations.	This model has obtained few errors while implementing in the real-time intrusion detection.
Belenko et al. (2018)	Machine learning technique	The simulation platform NS-3 simulator was used and specific cyber-attacks were targeted. Security concerns in brand-new car-to-car ad hoc systems are detected. This shows good productiveness.	The technique cause higher expensive datasets and have also failed to introduce any valuable security concepts to prevent security attack in VANET.
Gonçalves et al. (2021)	VANET intrusion detection system using Machine learning model	Common technologies are accustomed to prevent from dander is most preferred security strategy.	This model has minimum cost and lower accuracy.
Alsatian et al. (2021)	SVM-based intrusion detection	In comparison with other approaches this model has good classification accuracy with a superior intrusion detection model.	This intrusion detection method takes longer execution time.
Mahalakshmi et al. (2020)	N-Bayes algorithm	This IDS is used to identify and sort misbehavior clusters. This system has better security and accuracy.	Misbehavior networks are found throughout this approach. But speed, time and position are within a communication range.

Alshammari et al. (2018)	K-nearest neighbor and support vector machine	Detects intrusion in-vehicle systems. This model also minimizes the waiting time on road and improves the driving efficiency and comfort.	This system lacks centralized infrastructure which leads to exposure to various security attacks.
Ghaleb et al. (2020)	Distributed ensemble learning.	Detects misbehavior-aware on demand collaborative. The accuracy of a classifier is tested in the recipient vehicles using the regional testing dataset. It has better accuracy and communication overhead reduction.	This model takes time and costs higher.
So et al. (2018)	Random forest	The local testing dataset evaluates the performances of the classifiers. It excels other systems with respect to efficacy and better effectiveness.	This technique failed to enable security.
Ercan et al. (2021)	Random Forest and k-Nearest Neighbor	Ensemble Learning is used to increase detection. The attack detection and classification accuracy were at higher and lower feature range.	Numerous concerns about privacy can obstruct data receipt by deleting, altering, or postponing communication.
Sultana et al. (2022)	Machine learning model	This model confirms superior detection accuracy with minimum energy consumption.	It failed to encrypt the data and made many security attacks. So, a misbehavior detection mechanism is required to rectify this issue.

2.2.3. Deep Learning Techniques based Intrusion Detection in VANET

The LSTM model for the VANETs intrusion detection system was suggested by Yu et al. (2022) which is based on the time series classification approach. The accuracy of identifying false emergency messages was improved by using the classification model of the LSTM. For both traffic assaults and ordinary scenarios, the time series feature vectors train and develop the traffic incident classifier to recognize traffic parameter patterns with increasing computing problems.

Aboelfottoh et al. (2022) introduced a deep-learning model for VANET. Deep learning was used to create IDS, which were more precise and intelligent, offering an effective intrusion detection model but falling short of satisfying the security process.

Based on VANET intrusion detection, deep learning-based Hybrid optimization enabled trust-based secure routing model was introduced by Kaur et al. (2022). While the number of vehicles was maximized, a maximum computational period was needed to evaluate the independent operations. The hybrid optimization algorithm performs the routing process as well as the selection of the Cluster Head. In order to execute effective classification, feature selection is the most important process. The experimental outcomes demonstrated 0.2454J energy consumption, 0.9395% precision, and 0.9462% recall results. The feature selection step failed to select the most relevant features.

Gonçalves et al. (2021) introduced the intelligent hierarchical intrusion detection system for VANET. The experimental works were handled via publicly available datasets. Further, attribute-based encryption and the VANET public key infrastructure highly secure communication among hierarchy entities. This method was unable to detect various kinds of attacks in VANET.

To detect the abnormal node throughout the entire network (Shu et al. (2020)) stated a novel Generative Adversarial Networks incorporated with distributed SDN for the implementation of collaborative structure for the intrusion detection of VANETs. The authors stated that the performance of the work is higher in both Independent Identically Distribution and non-Independent Identically Distribution in the detection of intrusion. However, the tradeoff between communication cost and efficiency is high and should be reduced.

With the increasing anomalies, the detection of anomalies is an intricate process, and to overcome this, Alladi et al. (2021) demonstrated a novel Deep Neural Network based anomaly detection approach. It also utilizes reconstruction sequences and thresholding algorithms incorporated with DNN. The RSUs consist of DNN architecture and demonstrate the forwarding of the VANET information along with the detection of anomalies and classify the sequences accordingly. The detection accuracy of the stated work is about 98.1% with the help of benchmark datasets. Though the accuracy of detection of anomaly is higher, the transferring speed of data over the network is lower.

With the changing behavior of VANET, anomaly detection is a challenging task, and Nie et al. (2019) suggested Convolutional Neural Network-based technique. The authors utilized the Spatio-temporal and sparse features from the VANET and Mahalanobis distance-based loss function. The detection accuracy is higher but the authors utilized only one dataset to analyze the performance.

To overcome two types of issues such as the perspective of an Intrusion Detection System (IDS) and adaptive IDS, Liang et al. (2021) presented a novel Bayesian Game theory and Deep Q-learning Network-based IDS approach. The stated IDS ensure the declined capacity and the adaptation of the yielding efficacy. To analyze the dependency of IDS over the performance and road condition the Nash Equilibra of the game has been used. The self-adaptation of the IDS is analyzed with the deep Q-learning network and for retraining, Error Priority Learning has been used. The authors described that the detection rate and time are optimized with little computational overhead.

To analyze various types of attacks in VANET, Annamalai et al. (2022) presented a novel constancy CNN-based approach that enables trust-based clustering and secured transmission. The authentication of information is achieved with the quantum cryptography approach. The clustering process involves measuring the pace of the vehicle, route, distance, and trust rate of the nodes. The authors stated that the security of the data transmission is higher; however, it takes higher time to process the stated approach.

Software Defined Networks (SDN) provide a solution to major issues in VANET, however, they are easily targeted by the attacks and to overcome the Distributed Denial of Service (DDoS) attacks Türkoğlu et al. (2022) delineated a novel approach. The features of the datasets were derived with the assistance of the Minimum Redundancy Maximum Relevance (MRMR) algorithm. For the hyperparameter optimization Bayesian decision tree classifier-based optimization approach is utilized by the authors. The authors described that the stated approach achieves 99.35% of detection accuracy; however, the security level is lower than the other approaches.

Alladi et al. (2022) deliberately explained the novel approach for the intrusion detection VANET system on the deep learning-based misbehavior classification in IoV networks. The author also utilized Long Short Term Memory (LSTM) and CNN for the detection of intrusion. The stated Deep Learning Classification Engines consists of one to multi-step classification approach. The authors stated that the approach identifies 18 types of vehicle behaviors and achieves an F1-score of 95.68% to 96.76%. Also, the detection accuracy is higher with low detection time. However, it can be used for small-scale datasets and is not applicable to real-time scenarios.

To sight the foray in the Internet of Vehicles (IoV), Nie et al. (2020) designed a novel data-driven IDS with the validation of link load behaviors of the RSUs. For this, the author stated a deep learning architecture incorporated with CNN. The features are derived from the link loads with the help of the stated approach. The convergence of the system is designed with the probabilistic determination of the stated CNN approach. The detection accuracy of the system is higher with higher computational time.

An improved intrusion detection system was introduced by Dadi et al. (2022) and is based on AutoEncoder (AE) network incorporated with the Support Vector Machine (SVM). The authors detected five kind of violations such as DDoS, DoS, Black hole, Wormhole, and Gray hole attack. The features are extracted with the auto encoder and SVM effectively detects the intrusion. The authors stated that the stated approach provides higher detection accuracy and security. However, the challenges occurs when the number of vehicles advances.

To detect the DDoS attack in the VANET system Kadam et al. (2021) delineated a hybrid K-nearest Support Vector machine approach. The authors stated that the approach is sued to provide a secure structure for the communication system in VANET. This stated approach improves the detection accuracy, scalability, and reliability, however, this approach failed to detect other sort of raids such as a Black hole, Wormhole, Gray hole attack, etc.

Flood attack is considered the major daunting threat to the VANET system and to detect that attack Aneja et al. (2018) delineated a novel Artificial Neural Network based hybrid IDS approach. The stated system enhances the accuracy and for optimization of the result genetic algorithm has been imposed. Along with accuracy precision improved and eliminates the false alarm rate. The packet delivery rate and throughput also got improved with the stated system. Nevertheless, the computational complexity is high for a large network.

To recognize the potential risks in the VANET system, Chougule et al. (2022) demonstrated a novel Multi-branch Reconstruction Error IDs (MRE-IDS). This system identifies the intrusion and therein significantly increases the availability, integrity, and authentication. The stated system includes three CNN-based models and the identification of intrusion has been performed with the threshold setting values. The presented system identifies the identity, motion-related behavior, and frequency with an accuracy of 98.9%, 98.39%, and 100% respectively. It can also be used for the cloud and edge environment. However, it failed to increase the flexibility and authenticity of the system.

To identify the attacks in VANET Vitalkal et al. (2022) stated a novel approach known as Deep Belief Neural Network based IDS. The automation of vehicles has increased the risk of loss of packets during transmission. The attackers used to do this due to the absence of the driver. The authors analyzed the performance with the CICIDS2017 dataset and obtained detection accuracy of 90% and 98.1% respectively for the multiclass and two-class classification. The real-time application has a more complicated computing architecture. **Table 2.3** depicts the outline analysis of deep learning techniques for collaborative intrusion detection in VANET.

Table 2.3: Outline on deep learning techniques

Author	Methods used	Advantages	Limitations
Yu et al. (2022)	LSTM model	This model is based on the time series classification approach. The traffic incident classifier is trained and built using the time series feature vectors to identify traffic parameter patterns.	The increasing computational challenges traffic attacks and regular scenarios.
Aboelfottoh et al. (2022)	Deep learning model	More precise and intelligent thereby offering an effective intrusion detection model was created by deep learning.	The security process for this model is does not satisfy the expectation.
Kaur et al. (2022)	Deep learning-based Hybrid optimization	This algorithm performs the routing process as well as the selection of the cluster head. To execute effective classification feature selection is important. The outcome was 0.2454J energy consumption with good precision and recall results.	The feature selection step failed to select the most relevant features
Gonçalves et al. (2021)	Hierarchical intrusion detection	Experiments are handled using publicly available datasets. They highly secure communication among hierarchy entities.	Various kinds of attacks were unable to find out. But it has low reliability and scalability.

Shu et al. (2020)	Generative Adversarial Networks	The performance of the work is high with good efficiency and minimum latency.	The tradeoff between communication cost and efficiency is high and should be reduced.
Alladi et al. (2021)	Deep Neural Network based anomaly	It uses reconstruction sequences and thresholding algorithms incorporated with DNN. The detection accuracy is higher with 98.1%.	The transferring speed of data over the network is lower.
Nie et al. (2019)	Convolutional Neural Network	The Spatio-temporal and sparse features from VANET and Mahalanobis distance-based loss functions are used. The detection accuracy is higher.	Though it has many data only one dataset is analyzed.
Liang et al. (2021)	Bayesian Game theory and Deep Q-learning Network-based IDS approach	The dependency of IDS is analyzed with Nasha Equilibra of the game and the self-adaptation of IDS with deep Q-learning network. It is said that the detection accuracy is higher with a lower detection time.	It has high computational complexity.
Annamalai et al. (2022)	Stability-Assured CNN-based approach.	The approach enables trust-based clustering and secured transmission. Authentication is achieved with quantum cryptography approach.	The time taken to process the approach is higher with high computational time.

		The security of the data transmission is higher.	
Türkoğlu et al. (2022)	Minimum Redundancy Maximum Relevance (MRMR) algorithm and Bayesian decision tree classifier-based optimization	The approach detected accuracy is higher and is equal to 99.35%.	When compared to other approaches the security level is lower.
Alladi et al. (2022)	deep learning-based misbehavior classification in IoV networks, Long Short Term Memory (LSTM), and CNN	The approach has Higher detection accuracy, lower detection time, and attains F1-scores in the range of 95.68% to 96.76% and it identifies 18 types of vehicles.	This can be utilized for small-scale datasets and are not applicable for real-time scenarios.
Nie et al. (2020)	Deep learning architecture incorporated with the CNN	The detection accuracy of the system is higher.	It has higher computational time overhead.
Dadi et al. (2022)	AutoEncoder (AE) network incorporated with the Support Vector Machine (SVM).	The intrusion are detected by SVM and the visage are dislodged by the auto encoder. It also provides higher detection accuracy and security.	When the count of vehicles increases, complication of the stated work will also get increased.
Kadam et al. (2021)	Hybrid K-nearest Support Vector machine approach	This approach provides a secure structure for the communication system. This improves higher detection accuracy, scalability, and reliability.	This failed to detect other types of attacks such as the Black hole, Wormhole, Gray hole attack, etc.

Aneja et al. (2018)	Artificial Neural Network based hybrid IDS approach	Enhances the accuracy of the system and genetic algorithm for optimization. Along with higher detection accuracy, accuracy precision is also improved with throughput, and packet delivery rate.	For larger VANET systems the computational complexity is higher.
Chougule et al. (2022)	Multi-branch Reconstruction Error IDs (MRE-IDS), Convolutional Neural Network	Identifies the intrusion and significantly increases the needs. The system has improved identity, motion-related behavior, and frequency with an accuracy of 98.9%, 98.39%, and 100%.	The system failed to increase its scalability and reliability.
Vitalkal et al. (2022)	Deep Belief Neural Network-based IDS	With the CICIDS2017 the detected accuracy of 90% and 98.1% respectively for the multiclass and two class classification has been achieved.	For real-time applications, the computational complexity is higher.

2.3. RESEARCH GAP IDENTIFICATION

Based on the literature analysis these are the following issues often encountered during intrusion detection in VANET and they are presented as follows:

- The attacks detected using Shannon entropy are mainly based on single features such as source IP address which can be easily modified by the attackers using different tools such as scapy, hyping, etc.
- The contemporary VANET networks' use of several protocols and variety in their data results in a high level of complexity when spotting intrusions.
- To evaluate the trust of the entire VANET network, we need to integrate different attack results, which are often impossible to achieve in real time since a single node cannot collect a huge amount of security-related information.
- The solution identified by a centralized network often crashes if it is compromised or untrustworthy.
- If a single node performs both data collection and intrusion detection it will be overloaded.
- The attack detection accuracy is often questionable when a huge amount of data is processed via a centralized node in the VANET. This frequently leads to a single point of failure, which is avoided by decentralizing the intrusion detection process. Certain existing techniques mainly evaluate the efficiency of their technique using outdated datasets. There is a possibility that there will be no traces of modern attacks such as DDoS, Sybil, and blackmail attacks.
- To identify risks in real-time traffic flow with decreased detection time and computational complexity for analyzing large quantity of event data Novel approach is used.
- The existing techniques can only identify the abnormal packet flow when it is trained with the training samples or else it fails to identify the abnormalities.
- To identify the novel attacks, the generalization of supervised methods alone is not enough. To overcome this problem, the intrusion detection methods need to be trained in a semi-supervised fashion where the model is trained with normal traffic without any details about the abnormalities.
- Existing intrusion detection system implementations frequently extract data from network packets. Textual features of data that have been purposefully identified as critical to the investigation of an attack. Manually selecting features, on the other hand, takes time and requires significant knowledge about the security area.

Furthermore, to categorize between usual and aberrant behavior, supervised learning algorithms require large amounts of labeled legitimate and attack request information, which is often expensive and hard to collect for operational online services.

- The ability to accurately detect attack traffic and recover a system from an attack is a fundamental network security need, thus time and effort should be invested in creating strategies for reducing the effects of recognized DDoS, Sybil, and blackmailing attacks.

2.4. SUMMARY

This chapter summarized the existing literary works based on different techniques to overcome the attacks that are held on VANET. Initially, the different artificial intelligence techniques used for intrusion detection in VANET are briefly reviewed. Next, the different Machine learning, Deep learning techniques, cluster formation, and Autoencoder techniques for intrusion detection in VANET are also analyzed. This chapter also provides the research gap that exists in the existing works which might be a key study issue in future researches. To avoid the complexities observed in existing approaches, we present three novel models for reducing the dimensionality of the dataset and lowering the training time of the model under the premise of ensuring the accuracy of the intrusion detection target in the next chapter. Due to the sophisticated structure of the deep intrusion detection model and a large number of parameters, we look into refining the model neurons and computation methodologies, streamlining the organization topology, and improving model efficiency.

CHAPTER 3
INVESTIGATION OF INTRUSION DETECTION SYSTEMS IN VEHICULAR AD HOC NETWORKS

3.1. STUDY OF INTRUSION DETECTION SYSTEM

One of the cornerstones of cyber security is the intrusion detection system (IDS). IDS supports in identifying and forbidding intrusions in the network, allowing the user to maintain privacy. IDS is also used to detect and correct various network intrusions. It is a program with software capabilities that allows to control and conceal various intruding activities in the network. To communicate with one another, the user must always be alert since the data can be spied on. Hackers utilize a number of methods to break into the systems and interrupt the communication. Because of the involvement of various attackers, the consumer's secrecy are now in jeopardy. Now attempts are taken to reduce various attacks in the network by utilizing IDS. The protection of VANETs (vehicular ad hoc networks) has piqued the curiosity of many investigators. In the case of VANETs, a minor security breach can have far-reaching consequences because human lives are at risk. IDS are used in VANETs to spot and analyze the malicious network activity, prompt actions are taken to stop damages from such activities. The intention of this investigation is to scrutinize the determination, classification, methods, tools, strategies, and dangers in order to identify and mitigate current risks.

Internet security has become an issue for organizations in today's real-time environment. In order to secure sensitive information from hacker’s internet security is very important. Security measures for internet services and digital communications are still in place for a while, including Web Firewalls, cryptography, proof of identity, and Virtual Private Networks (VPN).

A latest arrival to the information security arsenal is intrusion detection. IDS are a change that enhances network security and offers data protection to a company. The IDS aids the system administrator in spotting malware-related network connections and notifies them so they may take the necessary precautions to encrypt the information (Mohit et al. (2017)).

Any illegal activities or harmful utilization of data resources are regarded an intrusion. An intruder is referred as a tangible thing that makes attempts to access data without authorization, do harm, or to start up other crooks. IDS are used to protect the firewall. The firewall prevents an organization from suspicious Internet attacks, and it detects if someone tries to access the security system or manages to breach the firewall security and gain access to any system in the organization, and also notifies the network administrator if there is any unwanted activity in the firewall (Mohit et al. (2017)).

Cyber security has now become extremely germane for all. The details would be at danger due to the increase in breaches, and the systems are susceptible and the private information is non-existent. There are numerous cybersecurity tools available to protect the infrastructure from certain attacks. Among these tools, an important one is the Intrusion Detection System, which protects our data and alerts us when someone is intercepting across our network (Hamza et al. (2021)).

VANETs (vehicular ad hoc networks) are a subset of mobile ad hoc networks (MANETs) (Noh et al. (2020)). VANETs feature a greater transmission frequency over MANETs and constantly changing network configuration (Baqer et al. (2019)). VANETs are an essential element of Intelligent Transport Systems, which provide dependable, ensure security, and effective solutions to all problems (Engoulou et al. (2014)).

A vehicular ad hoc network, in its simplest form, is a wireless carrier made up of number autonomous units, roadside units, or RSUs, and services that make it easy to join the network's occurrences (Chaudhary et al. (2014a)). Although there are many security suggestions and implementation challenges, these networks drastically enhance traffic conditions and accident prevention. The main obstacle is to classify the trespass vehicles and to authenticate the vehicles that join the network. A minor safety gap in VANETs can end in massive losses, even resulting in people's deaths. As a result, VANET policy mechanisms that guarantee traffic are necessary.

A lot of scientists and research organizations have been working tirelessly to create efficient authentication methods for protecting VANETs from intruders and to minimize security breaches. Numerous alternatives have been recommended by VANET security and defense mechanisms researchers (Nandakumar et al. (2016)).

An IDS is a safeguard to take note of access and communication software as a result, it tends to work to evaluate that traffic for potential adversarial attacks from outside the organization as well as system misuse or attacks within the organization (Mohit et al. (2017)).

3.2. INTRUSION DETECTION SYSTEM

Intrusion Detection System (IDS) is a safeguard method that uses clustering to detect any attacks on the network framework. It is used to enforce VANETs in order to control the received information and vehicles from any malicious movements (Chaudhary et al. (2014b)) (Aloqaily et al. (2019)). If any malicious activities are detected, the IDS have the authority to block the appropriate entries from causing future problems in the network. The IDS is introduced as a robber buzzer. For instance, the latch control in the home guards from theft. If someone breaches the lock system and enters the home, the robber buzzer identifies and alerts the landowner by lifting the buzzer. By keeping an eye on network data transfer, firewalls are crucial (Jayesh et al., 2017).

3.3. LITERARY WORKS

According to the study (Tahir et al. (2016)), the supervised machine algorithms is purposed for anomaly detection. To detect anomalies in normal traffic, algorithms such as SVM, J decision tree, decision table, and naive Bayes were used. The model's data is converted into a prediction model using machine learning algorithms. Later, a subset of data from the prediction model is used for testing. To understand the algorithms better the input taken should contain few examples, instances or records and to differentiate these records feature vector is used. A supervised algorithm is one that requires a classification model or a class category, whereas some require semi-supervised algorithms. Unsupervised algorithms do not require a feature vector or class type instead train using patterns or similarities in the input. The author employs the KDD dataset.

According to the study (Hamed et al. (2020)) many algorithms were used for machine learning to identify distractions. Machine learning algorithms such as the Bayesian Network, Naive Bayes classifier, Decision Tree, Random Decision Forest, Random Tree, Decision Table, and Artificial Neural Network were also used to analyze the effects of metrics like precision, recall, f1-score, and accuracy on information security datasets. Only the Random Decision Forest algorithm thrashed the other machine learning

algorithms over all aspects. The ids model, that iterative and incremental development such as set of data exploration, data analysis, and machine learning-based security modeling were frequently used.

According to the study (Subhash et al. (2020)), supervised machine learning techniques were used for anomaly detection. In this prototype, the researcher chooses k features using the Random Forest Algorithm. Later, this k functionality is snared to obtain node d, which is then ruptured to obtain the first node. Constant repetition of the above process leads to the formation of random forests. PCA has also been carried out for classification purposes. Since the dataset has large number of characteristics the dimensions are also very high so this method takes all the inputs. The amount of the data source is reduced by aligning the datasets on the exact axis. The characteristics of the eigenvector and significance are evaluated before being utilized to create a matrix and its structure yields the integral. Once compared to SVM and Naive Bayes, this model has a 90% accuracy.

DCDIV, an intrusion detection approach is built on external stakeholders are groups shared cooperative structure, was highlighted in the study (Zhou et al. (2020)). The purpose of the research is to recognize deception violation in vehicular ad-hoc networks, such as impersonating, Denial of Service attacks, black hole attacks, and so on. In order to detect deception attacks in VANETs, the researchers recommended a detection model based on boundary conditions based on data from flow of communication, traffic, and psychosocial interaction situation.

According to the study (Kolandaisamy et al. (2020)), addressed a flow posture efficiency assessment intrusion detection process that satisfies VANET standards. The proposed framework employs a threat recognition system based on clustering, with the cluster head chosen to use a notoriety technique. To use the log file retained by the recognized clusters, the algorithm assesses flow placement for each node. In the following stage, the Conflict Field, Conflict Data, and Attack Signature Sample Rate are calculated (CCA). To determine whether a node is an invader or not, the genuine mass are compared for each node to the CCA mass.

A based intrusion detection and prevention algorithm for VANETs for DDoS (Distributed Denial of Service) detection was introduced in the study (Adhikary et al. (2020)). The

algorithm detects DDoS using multiple SVM support vectors, including RBFDot and AnovaDot. By integrating the two algorithms, the proposed scheme algorithm functioned. To begin, AnovaDot is often used to validate the algorithm using a dataset containing mixed data both from regular and distributed denial of service attacks. The forecasts from this model are then supplied into the RBFDot, with the identical set of information that was used to validate the algorithm. The combination developed model from the double training sample is then utilised to anticipate and identify Attacks and VANETs. The article needs a number of features, including throughput, latency, jitter, collision, and packet drop. The effectiveness of the proposed hybrid algorithm to single SVM approaches from AnovaDot and RBFDot is discussed further. The experiment's findings show that the combination method is effective at distinguishing DDoS attacks from proper conduct.

According to the study (Nandy et al. (2020)), it described how to program a trustworthy collaborative intrusion detection system to use with vehicular ad hoc networks. It is made up of a communicative way and a localized IDS relying on k-nearest neighbors non-linear classifier. The local IDS carry out three tasks: data collection, pre-processing, and KNN classifier-based intrusion detection. Following the collection of data, three factors—packet transfer interval (PTI), packet transfer delay (PTD), and packet drop count—are used to differentiate the malicious nodes in the pre-processing task (PDC). The preprocessed data is used to perform the intrusion detection. Every car has a score table based on the usage of their network. When a machine attempts to interact with another machine which uses the cooperative learning KNN, the rating chart gets updated automatically. Then, every one of these new scoring tables are combined and distributed to examine any network attacks.

For the purpose of Intrusion Detection on the dynamic and wireless networks a novel was projected by the study (Liang et al. (2019)). It consists of a feature extraction technique that is currently being used and an improved graded systematic map-based classifier (I-GHSOM). From the participating automobiles used for training and testing, this feature extraction technique extracts a variety of messages. This algorithm operates based on two prime factors, the position of the vehicles and the direction of the traffic differ. The first is coherent by computing the distance length between the vehicles. A semi-cooperative method and polling filter mechanism are developed to measure the traffic flow. In order

to obtain accurate verdict recalculation and relabeling mechanisms are suggested. The outcome demonstrates that when compared to other systems the suggested IDS performed significantly with better stability, accuracy, processing, and efficiency.

3.4. COMPARISON OF DIFFERENT LITERARY WORKS

A clear summarization of each reviewed paper is given below in the comparison table (**Table 3.1**). Each method or technique is put out for attack detection, technology deployment, and monitoring.

Table 3.1: Comparing different literary works

Authors & Paper Details	Title of the Research	Significant Contribution	Performance Analysis
Tahir Mehmood, "Machine Learning Algorithms in Context of Intrusion Detection", International Conference on Computer and Information Science, 2016	Algorithms for Machine Learning are used as a Part of Intrusion Detection	Identify anomaly detections	Better to understand best algorithms. Aid to find best patterns
Hamed Alqahtani, "Cyber Intrusion Detection Using Machine Learning Classification Techniques", International Conference on Computing Science, Communication and Security COMS2 2020	Employing effective classification tools to predict cyber intrusions	Assistance with interruption tracking.	Analyze various variations among the machine learning algorithms on cyber-attacks. More effective with the comparison of (Subhash et al. (2020))
Adhikary, "Hybrid Algorithm to Detect DDoS Attacks in VANETs", Wireless Personal Communications, 2020	DDoS Attacks on VANETs Discovered by a Mixed Methodology	Used for validating different algorithms based on security and protection	Better than (Liang et al. (2019)) in terms of distributed denial of service attacks

3.5. SUMMARY

Currently, VANET security is one of substantial issues appealing everyone's attention. In the case of VANETs, even a modest security breach might result in significant damage because human lives are at stake. Malicious activity in VANETs is identified with the help of Intrusion Detection Systems (IDS). It continues to monitor the network to find any intrusions so that timely preventive progress can be made (Chaudhary et al. (2019)). The design of IDS and the categorization of IDS depended on various criteria are all clearly outlined. This report included comparisons of certain modern intrusion detection algorithms. There are still a few open problems with the VANETs system's implementation of IDS. There are numerous intrusion detection systems that make use of machine learning and have enormous amounts of training data and compute power. The task of features extraction is also difficult. As technology advances, attacks are becoming more diverse in their sorts and methods. Therefore, this field needs constant fresh development. Most of the techniques used here are attempts to find intrusions solely in VANETs, though it is difficult to cover all the attacks at once.

CHAPTER 4
COLLABORATIVE BASED VEHICULAR AD HOC NETWORK INTRUSION DETECTION SYSTEM USING OPTIMIZED SUPPORT VECTOR MACHINE

4.1. OVERVIEW

Secured information can be sent to user vehicles using the Vehicular Ad hoc Network (VANET). However, at the present it is challenging to safeguard data from threats and weaknesses. As a result, to strengthen security through the use of new technology, a secure solution must be offered. Hence, a blockchain placed VANET structure that incorporates the improvement of security, scalability, and privacy for protected communication is developed. The cluster formation model is used in k-means clustering. Tabu Search-based Particle Swarm Optimization (TS-PSO) technique is up to choose the cluster head. The proposed strategy tries to reduce the delay by increasing throughput and power efficiency. The implemented blockchain will improve security and dependability. Furthermore, the trust-based collaborative intrusion detection on the VANET is used for innovative War Strategy Optimization (WSO) based Support Vector Machine (SVM) model (Optimized SVM) thereby detecting intrusion in VANET. While this is in action, this work can be applied to stop repetitive detection operations and to improve protection by satisfying the cars. Empirical study show that it may be utilized to better energy utilization, security, and end-to-end latency as well as to detect the malicious node from resource-constrained vehicles.

4.2. PROBLEM STATEMENT

Since most vehicles are created without taking into account the security system, it is one of the most difficult areas to secure. They can communicate instantly, which makes attacks more common (Lihua et al. (2022)). Traditional methods, like encryption and ignoring unnecessary nodes, can be used to handle this. Recently, vehicles have been connected to the VANET, allowing them to detect threats (Xu et al. (2022)).

In order to protect the connection between the cars and RSUs, the existing research developed a Blockchain-based collaborative intrusion detection technique for the VANETs. The search ability, cost, and execution time of various swarm-based optimization models, such as fish swarm optimization, particle swarm optimization,

glowworm swarm optimization, Cuckoo Search algorithm, genetic algorithms, and others, are higher (Soni et al. (2022)). Tabu search develops a metaheuristics search method that can effectively access both the ideal solution and local optimization issues (Yu et al. (2022)). A crucial element of Tabu Search is the use of flexible storage to provide a behavior that is substantially more adaptable. To find intrusions, employ the SVM-based WSO approach.

4.3. PROPOSED METHODOLOGY

In this chapter, collaborative transportation systems will be greatly facilitated by the VANET. Vehicles connected to VANETs share precise data about traffic conditions, congestion, and location. VANETs are nevertheless susceptible to dangers that arise from the current situation. The most used privacy model was IDS, which depends on automotive cooperation to identify intruders in VANET. **Figure 4.1** displays the proposed intrusion detection model's schematic diagram.

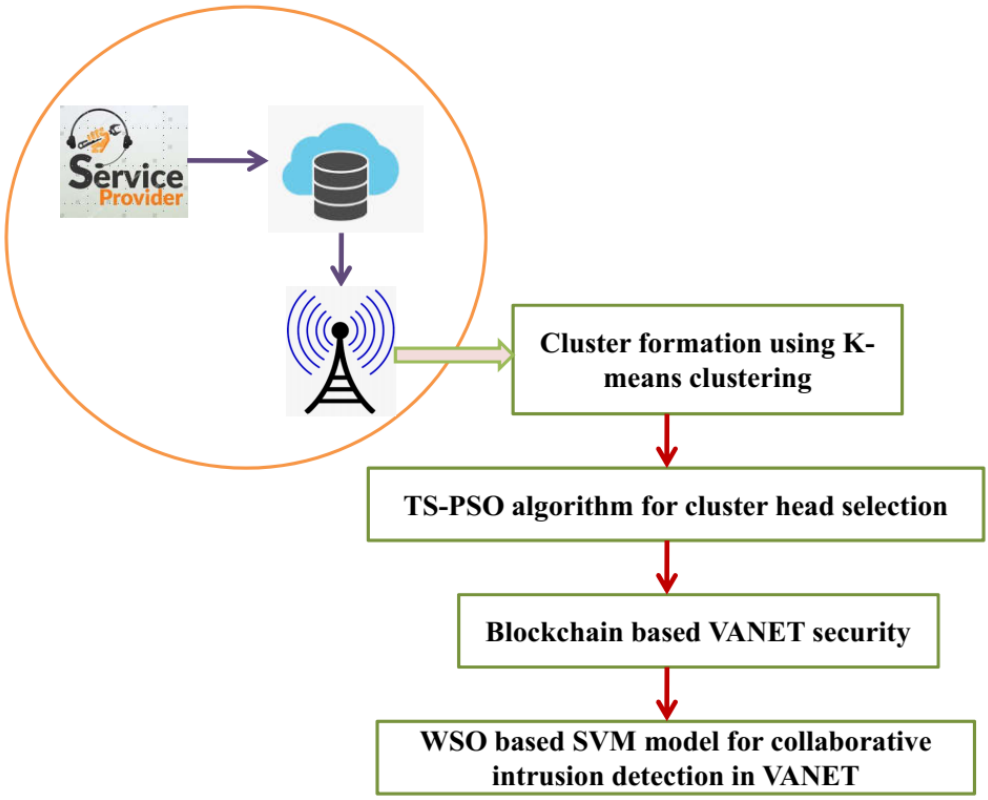


Figure 4.1: Proposed intrusion detection framework

Cluster formation, cluster head selection, VANET security, and collaborative intrusion detection are the four stages of the proposed technique. The k-means clustering replica performs cluster formation and the TS-PSO algorithm prefers the cluster heads.

Blockchain protection is used for privacy preservation. Finally, the optimized SVM model detects the intrusion in VANET. In the section below, each of these phases is described.

4.3.1. Formation of the Cluster

Here, the cluster creation is carried out using the K-means clustering model. The graph vertex serves as each vehicle, and the edges are represented by the distances between the vehicles (Sajini et al. (2022)). The cluster formation of each vehicle based on the RSU transmission region are calculated (Mamdoohi et al. (2022)). Where, $\left(X_1, X_2, .., X_m\right)$ is the observation set with the *d*-dimensional real vector. The *m* mark partition into *K*-sets is used to reduce the $(K \le m) R = \left\{R_1, R_2, ..., R_K\right\}$ within-cluster square sum (WCSS). The point R_j connotes the significance in the cluster formation is Y_j.

$$WCSS = \arg\min_{R} \sum_{j=1}^{K} \sum_{A_i \in s_j} \left\| X_i - Y_j \right\|^2 \tag{4.1}$$

4.3.2. Selection of Cluster Head

Next to cluster formation, the TS-PSO algorithm accurately picks the cluster heads. Tabu Search (TS) is used to depict the investigation, the space solution, excluding local optimality. The TS component which is more effective is an adaptable memory. The corresponding optimum cannot be reached with numerous function within a comparable duration. The TS has challenging combinatorial optimization issues thus choosing the finest key design. Generally, the PSO algorithm (Sengupta et al. (2018)) has greater convergence, resolving optimization problems, less population diversity and converging towards local optima but more time is taken to attain the global minimum, hence, the Tabu search model is combined with PSO (Schmidt et al. (2019)). From this, the TS-PSO algorithm gets enhanced performance thereby providing optimal outputs due to the higher convergence speed of the TS model. By using TS as a local development phase in PSO, the algorithm can retain population diversity and avoid arriving at an inaccurate local optimal solution.

The steps involved in cluster head selection using TS-PSO are explained as,

(i) Initializing the TS-PSO algorithm parameters, base station location and energy nodes.

(ii) Cluster formation calculates the base station with regard to the node's distances and determines the PSO algorithm based optical local position.

(iii) The global best solution is computed during the preparation of the PSO solution using the Tabu list and creating the entry and swapping of routes in the Taby memory.

(iv) Calculates the next position's fitness function and records the result in the Tabu list.

(v) The utmost practical answer on the Tabu list gets dropped and thus selects the correct cluster heads in VANET via the TS-PSO algorithm.

4.3.3. Blockchain-based Security for VANETs

The blocks that make up the blockchain are connected to one another. A block is a concurrently connected decentralized network ledger. The actions inside the block cannot be changed or reversed. The hash of the block serves as a link between each block inside the network. The rest of the network will be affected by any modifications to a single block (Krishna et al. (202)). Additionally, the data that is loaded into the blocks are completely open. The principal security interest in VANET is the transmission of information among vehicles. Before sharing in the VANET task administrator, the cars do not detect any relevant data. As a result, there is a chance that the Vehicular network may receive updated data (Kudva et al. (2021)). To resolve these problems, we used the blockchain security model, which successfully upholded system security. The distributed unchangeable ledger known as blockchain can be used to track assets and record transactions.

The following RSU needs the vehicle users to be permitted whenever they move from one RSU zone to another. This will significantly increase costs and impair the functionality of the VANET system (Chougule et al. (2022)). Both tangible and intangible assets is presented. The danger and expense can be reduced since the authenticated user can virtually trace the values in the blockchain. It also prevents the risk of any assault and failure at one place because of the dispersed data distribution and storage limit.

Additionally, by leveraging the open ledger in the blockchain, the original global strategy's validity and integrity ensured (Dibaei et al. (2021)). The VANET system's automobiles transmit exact data in accordance with a prize and penalties. This prevents the upload of incorrect information. The characteristics of each transaction is easily tracked.

4.3.4. VANET Intrusion Detection

For this study, the VANET collaborative incursion is found using an optimised support vector machine (SVM) model.

A. Support Vector Machine

Broadly used machine learning methods is the support vector machine (SVM), which provides a remarkable generalization capability with a minimal number of data. The proposed framework used SVM, a machine learning technique, to detect intrusions. The proposed framework used a WSO-SVM-based collaboration to identify assaults and legitimate traffic (Cervantes et al. (2020)). The information are depicted in n-dimensional space, and the intrusion is first detected by the hyper-plane, which is used to distinguish between malicious nodes and normal nodes. The SVM basic design is illustrated in **Figure 4.2**, the input data along with the input feature vector processes “n” number of support vectors like k(a, a1), k(a, a2)….k(a, an) additionally a bias function is added to these vectors to acquire the expected output.

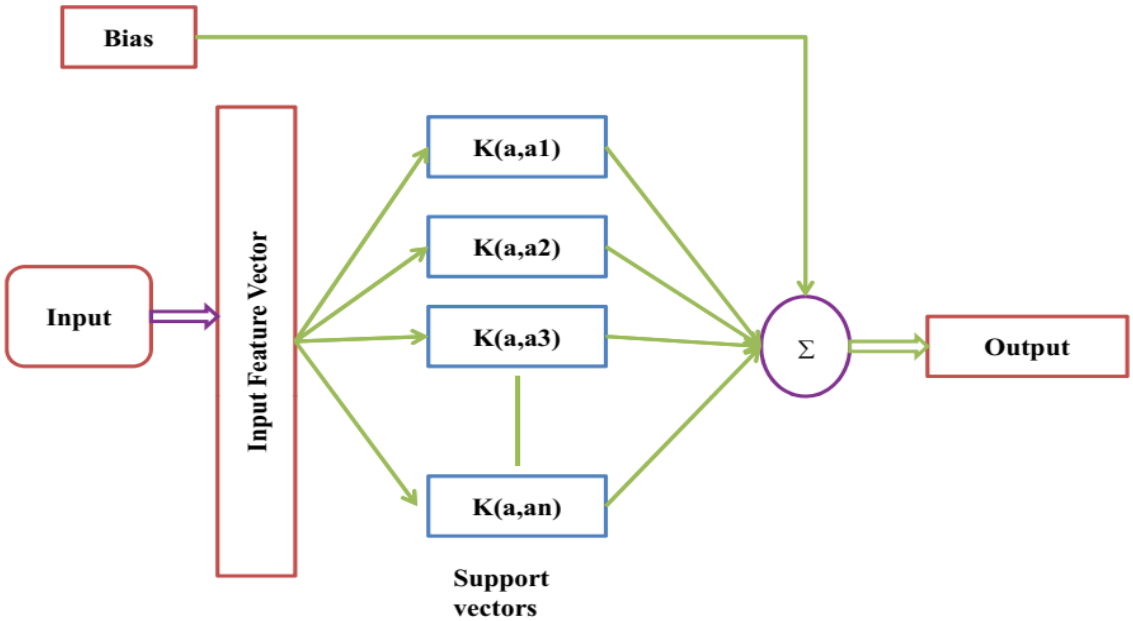


Figure 4.2: The basic model of SVM

This SVM model solves the binary classification problem (Zendehboudi et al. (2018)) such as intrusion or non-intrusion in VANET and it is expressed as follows:

$$\{(y_1, z_1),....,(y_m, z_m)\} \in (\Re^n \times \{\pm 1\})^m \tag{4.2}$$

Where, y_1 and z_1 labels and *n*-dimensional samples are in which the maximum margin with the two parallel hyperplanes are determined via SAVM for such two-class problems (Zhou et al. (2021))

$$G(y) = M^T y + B \tag{4.3}$$

Here, $B \in \Re$ and $y \in \Re^n$, the middle hyperplane separates the VANET training samples into intrusion and non-intrusion. The below minimization issue solves the obtained hyperplane for the separable case. The SVM's separating plane is plotted in **Figure 4.3.**

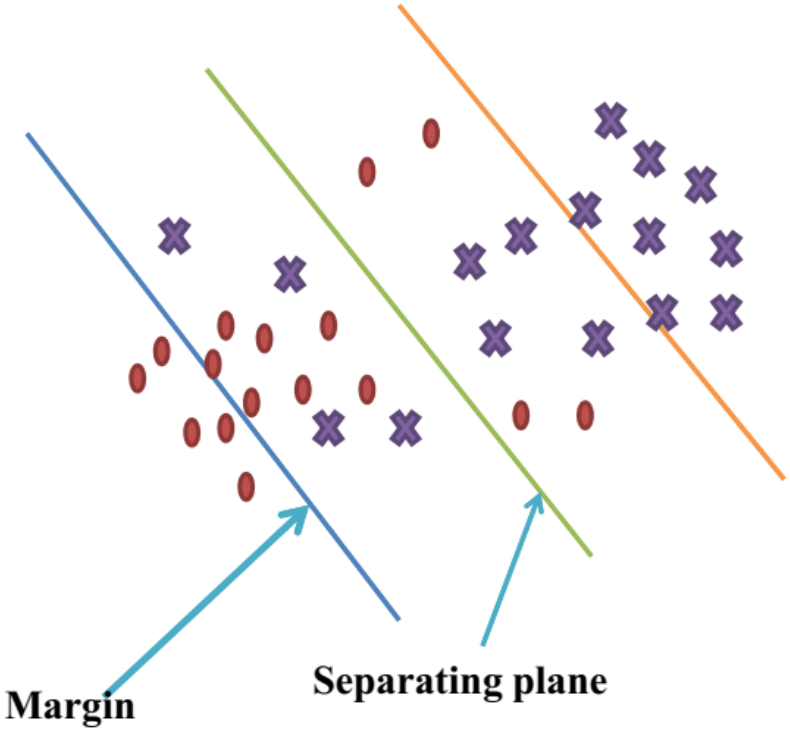


Figure 4.3: SVM's separating plane model

The SVM uses free parameters that depend on the separation margin to generate the individual points from the input.

$$\min imum_{M,B} \frac{1}{2}\|M\|^2 \;\; such \;\; that \, z_j \left(M^T y_j + B\right) \geq 1, \quad j = 1,....,m \tag{4.4}$$

The below expression is for the SVM model in a non-separable case.

$$\min_{M,B,\ell} imum \frac{1}{2}\|M\|^2 \ \ such\ that\ z_j\left(M^T y_j + B\right) \geq 1-\ell_j, \ \ \ell_j \geq 0, \ \ j = 1,....,m \tag{4.5}$$

Here, the tradeoff is controlled using the penalty parameter $C > 0$ and the slack variable is ℓ_j.

However, overfitting problems do occasionally arise and can be corrected by using the WSO technique. The SVM is primarily used for its speed, scalability, and reduced complexity.

B. War Strategy Optimization (WSO)

WSO is based on the military tactics used by ancient rulers and takes into account the goals, challenges, dangers, and opportunities of the operation (El-sadek et al. (2022)). The phrase refers to the tactic of having the army follow the monarch or leader on the battlefield. The soldiers, the king, and the commanders all move in concert to avoid being ambushed by local troops.

(i) Attack Model

There are two models for war strategies, the first of which keeps track of the soldiers' most recent whereabouts in relation to the king's locations. The soldier who has superior attack and fitness skills is regarded as the king (Ayyarao et al. (2022)). All soldiers start out with the same rank and position, and as the war strategy is implemented, the ranking positions are updated. The phrase "soldier, commander, and monarch" can be expressed as, "At the end of the fight, they all pretend to be close to one another."

$$D_i(t+1) = D_i(t) + 2\times\tau\times(A - Lo) + ran\times(CV_i \times Lo - D_i(t)) \tag{4.6}$$

The revised coordinate's weight is V_i as shown, the commander's location is *A* and the king's location is *Lo*, with the present locality of the soldiers $D_i(t+1)$ being D_i.

(ii) Up-gradation of rank and weight

The point of the attack force can be restored together with the soldiers' current locale. The soldier will remain at the previous place if the new fitness site (S*F*) is lower than the existing fitness location (*LF*).

$$D_i(t+1) = \left(D_i(t+1)\right) \times \left(SF \geq LF\right) + \left(A_i(t)\right) \times \left(SF < LF\right) \tag{4.7}$$

The soldier's rank is then updated as stated below.

$$R_i = \left(R_i + 1\right) \times \left(SF \geq LF\right) + \left(S_i\right) \times \left(SF < LF\right) \tag{4.8}$$

The ranking-based estimation of weights can be carried out as follows:

$$CV_i = CV_i \times \left(1 - \frac{R_i}{Max\_iter}\right)\beta \tag{4.9}$$

(iii) Defense concept

The latter tactic relies on upgrading the positions of the commander, the king, and a random soldier. The weight-up gradation and ranking both use the same methodology.

$$D_i(t+1) = D_i(t) + 2 \times \tau \times (Lo - D_{ran}(t)) + ran \times V_i \times (A - D_i(t)) \tag{4.10}$$

(iv) Replacing weak soldiers

Each cycle involves the detection of the worst soldiers, who are then swapped out for a random soldier as seen below.

$$D_v(t+1) = LC + ran \times \left(UC - LC\right) \tag{4.11}$$

The next strategy is to move the weak soldier to the army's median, as seen below.

$$D_v(t+1) = -\left(1 - ran\right) \times \left(D_v(t) - median(A)\right) + Lo \tag{4.12}$$

C. Optimized SVM model for collaborative intrusion detection in VANET

The intrusion detection is carried out using the machine learning method SVM. Here a WSO-SVM-based collaboration is used to identify VANET attacks. The data is presented in n-dimensional space, and the intrusion is detected by first identifying the hyper-plane, which is used to distinguish between malicious nodes and normal nodes (Zeng et al. (2018)).The SVM has used free parameters that depends on the separation margin to connect the multiple input points (Mukkamala et al. (2020)). However, overfitting problems do occasionally arise and can be corrected using the WSO technique. The SVM is primarily used for its speed, scalability, and reduced complexity (Ali et al. (2021)). The

WOA includes different steps like attack strategy, improvement of rank and weight, and defense strategy with weak Soldiers replacement/relocation. The intended optimized SVM for collaborative intrusion detection in VANET is depicted in **Figure 4.4.**

The following is a description of improving WSO-based SVM for intrusion detection

- The intended strategy keeps the ratio of exploitation to exploration in check.
- Regardless of rank, each soldier (solution) keeps a distinct weight.
- The weight of the soldiers was restored when the fitness step was completed.
- The weights fluctuate significantly at the beginning of the iteration and get smaller as it goes on, producing a profit that is considered to be the worldwide choice.
- The proposed method only speeds up convergence and reduces processing complexity.
- The recommended WSO algorithm's fitness funtion updates the position parameters of SVM and detects the VANET attacks.

This WSO is based on the military tactics used by ancient kings and takes into account the goals, challenges, dangers, and opportunities of the mission (Ayyarao et al. (2022)). War is an ongoing process in which armed soldiers merely gather to battle their foes. SVM is a straightforward machine-learning approach that offers effective intrusion detection, rapid implementation, and ease of use. However, it has several drawbacks, such as over fitting difficulties and greater complexity (Deng et al.(2003)). The WSO algorithm addresses these drawbacks by accelerating convergence, improving search ability, and improving detection speed and accuracy. Thus, in the collaborative intrusion detection strategy, both WSO and SVM are combined and put into action. The recommended WSO algorithm's fitness function updates the position parameters of SVM and detects the VANET attacks.

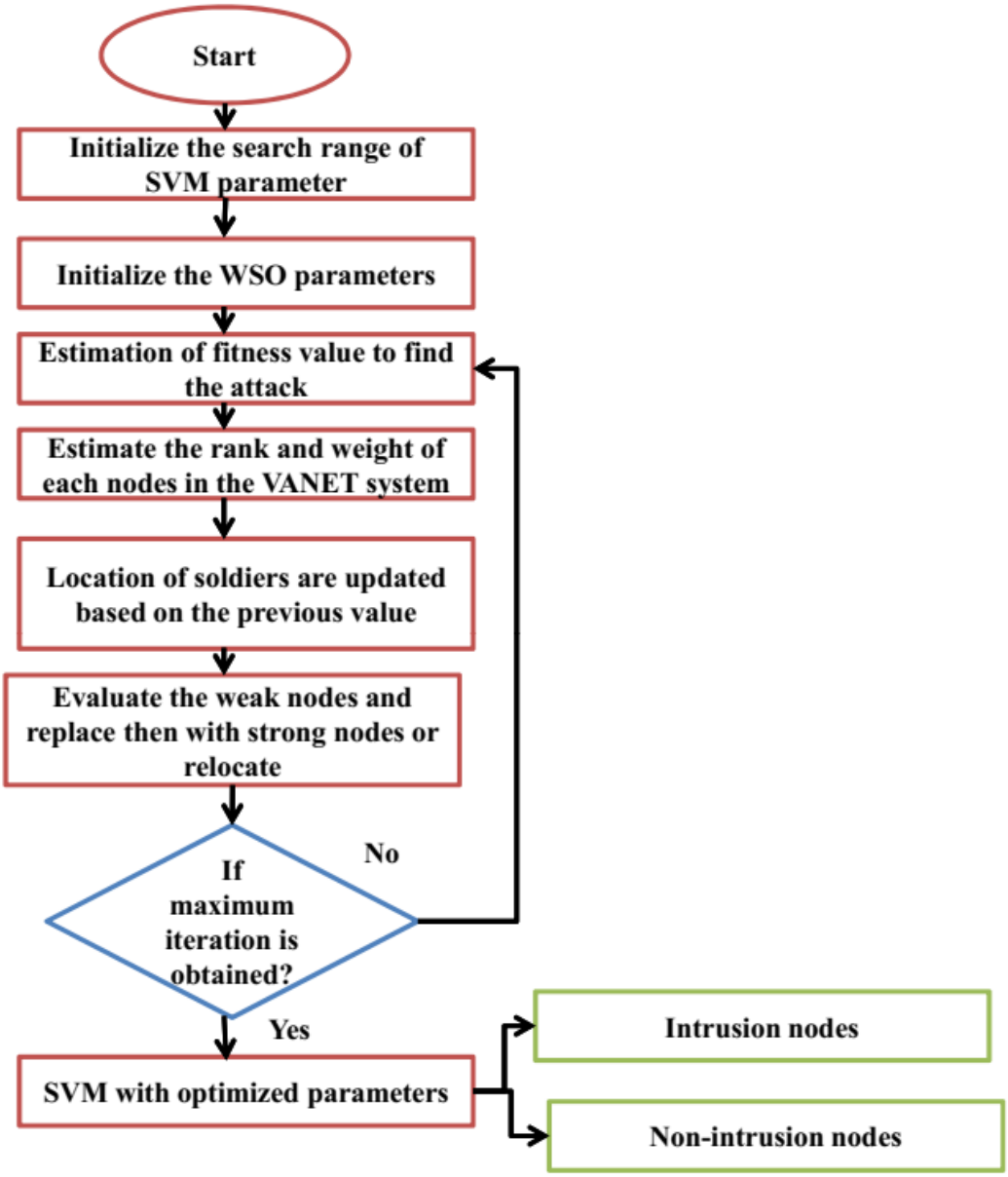


Figure 4.4: Proposed optimized SVM for collaborative intrusion detection in VANET

4.4. RESULT AND DISCUSSION

This section focuses on the experimental examination of a suggested framework for collaborative intrusion detection in VANET. The experimental findings are implemented using a GPU computer based on NS-2 with a GTX1050 GPU at 16GB RAM and an Intel Core i5-8300H CPU running Tensorflow 1.15. The KDD99 dataset is utilized in this study for experimental analysis (Zhang et al. (2018)). The KDD99 dataset consists of five million records that are described by 41 features. From this data, 70% of data is used for training and the balance 30% is used for testing process during intrusion detection. Table 4.1 explains the parametric description based on the suggested framework.

Table 4.1: Description of parameters used in this study

Parameters	Ranges
Number of population	50
Maximum number of iteration	100
Regularization	0.01
Kernel function	Gaussian
Number of nodes	50
Simulation range	$1.5km * 1.5km$
Speed movement	4 m/sec
Penalty factor	$C > 0$

4.4.1. Performance Measures

Accuracy, precision, and recall performance indicators are utilized to verify the usefulness of the proposed framework. All of these performance metrics for intrusion detection performance efficiency are explained by the ensuing equations.

$$Accuracy = \frac{T_N + T_P}{F_N + T_N + F_P + T_P} \tag{4.13}$$

$$\text{Pr}ecision = \frac{T_P}{F_P + T_P} \tag{4.14}$$

$$\text{Re}call = \frac{T_P}{F_N + T_P} \tag{4.15}$$

From this, true positive (T_P) and true negative (T_N) are the amount of successfully anticipated intruding classes and the amount of correctly predicted non-intrusion classes respectively. Additionally, a number of false positive (F_P) and false negative (F_N) categorization for incursion and non-intrusion were predicted wrongly.

4.4.2. Performance Analysis

Figure 4.5 presents the graphic representation of the energy usage outcome. The state-of-the-art approach include (Random Forest) RF, (Hybrid Data Driven Model) HDDM, (Host based Intrusion Detection) H-ID, and (Multi-Layer perceptron) ML with the suggested methodology. For this inquiry, 50 nodes are occupied. The proposed technology consumes less energy than current technologies as RF, HDDM, H-ID, and ML.

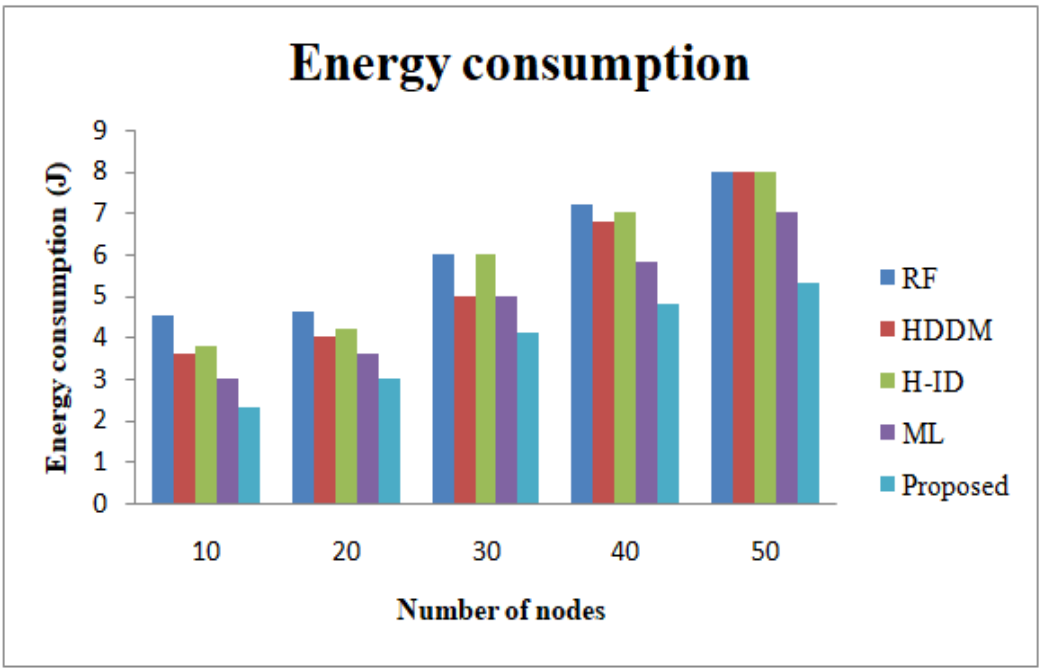


Figure 4.5: Graphical representation of energy consumption results

The linear representation of end-to-end delay consequences are shown in **Figure 4.6**. RF, HDDM, H-ID, and ML are among the cutting-edge approaches, along with proposed methodologies. The latency is indicated in time seconds for this examination using 50 nodes. The proposed method showed the least amount of delay when compared to already-in-use technologies including RF, HDDM, H-ID, and ML.

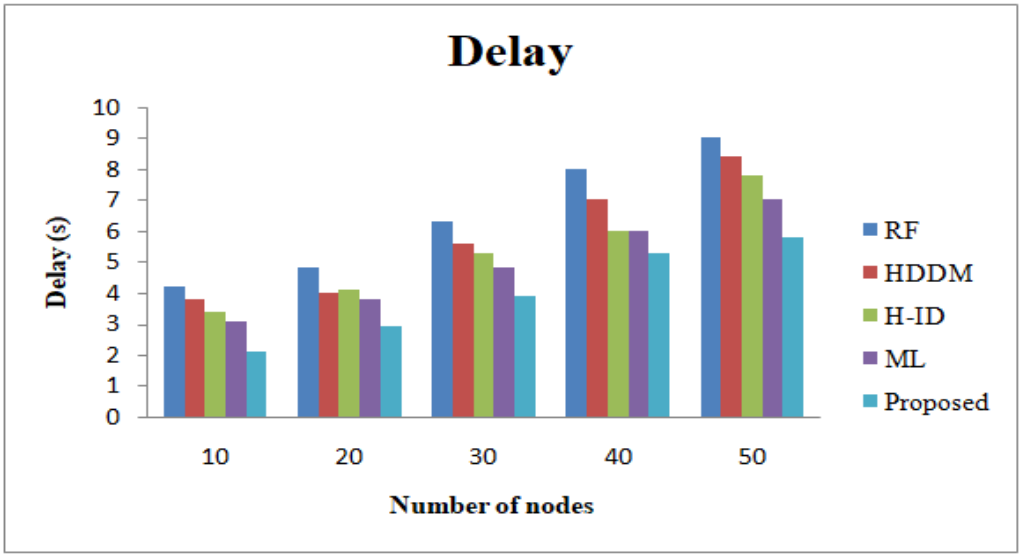


Figure 4.6: Graphical representation of delay

Table 4.2 reports the analysis and comparison of the proposed security-based technique's performance evaluation with state-of-the-artwork in RF, HDDM, H-ID, and ML. The recommended solution effectively protects the VANET system and prevents the cars from intrusion since it uses a collaborative blockchain-based WSO-SVM technique. The proposed approach's security is 95.89%, whereas the security levels for RF, HDDM, H-ID, and ML are, 91.9%, 89.06%, 90.56%, and 93.23% respectively.

Table 4.2: Security assessment

Methods	Security (%)
RF	91.9
HDDM	89.06
H-ID	90.56
ML	93.23
Proposed	95.89

The comparative study of accuracy is shown in **Figure 4.7.** Several node counts such as 10, 20, 30, 40 and 50 are used for the examination of accuracy. The techniques like RF, HDDM, H-ID, and ML are implied. However, these recommended methods are more accurate than previous methods like RF, HDDM, H-ID, and ML in terms of all nodes.

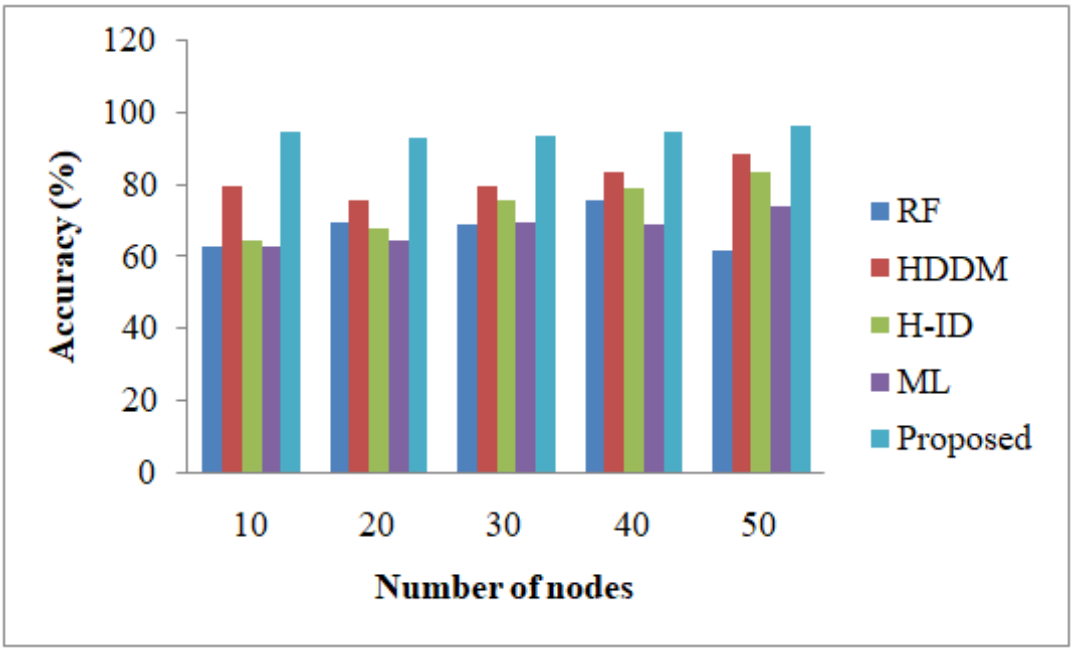


Figure 4.7: Comparative analysis of accuracy

Figure 4.8 exemplify the relative analysis of precision. For the precision analysis, various node counts of 10, 20, 30, 40, and 50 are used. The state-of-the-art techniques like RF, HDDM, H-ID, and ML have been suggested. In terms of all nodes, the proposed method provides greater precision than earlier techniques like RF, HDDM, H-ID, and ML.

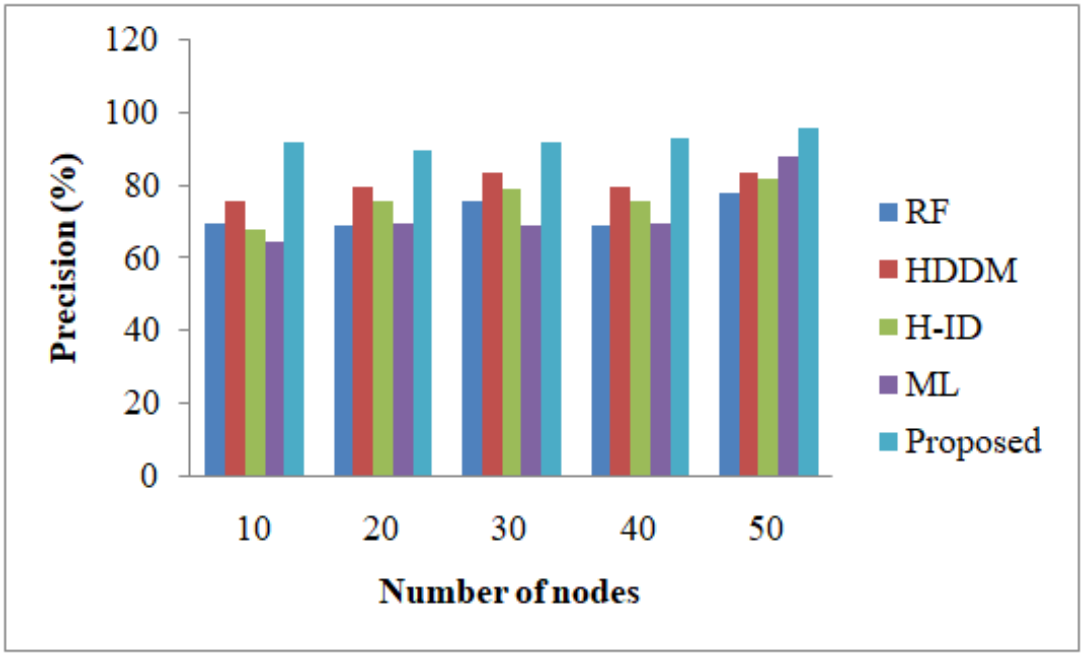


Figure 4.8: Comparative analysis of precision

The comparative study of recall is illustrated **in Figure 4.9.** Different node counts of 10, 20, 30, 40, and 50 are used for the recall analysis. The most recent methods include those that have been proposed, such as RF, HDDM, H-ID, and ML. The hinted mode offers more recall results across all nodes than earlier techniques like RF, HDDM, H-ID, and ML.

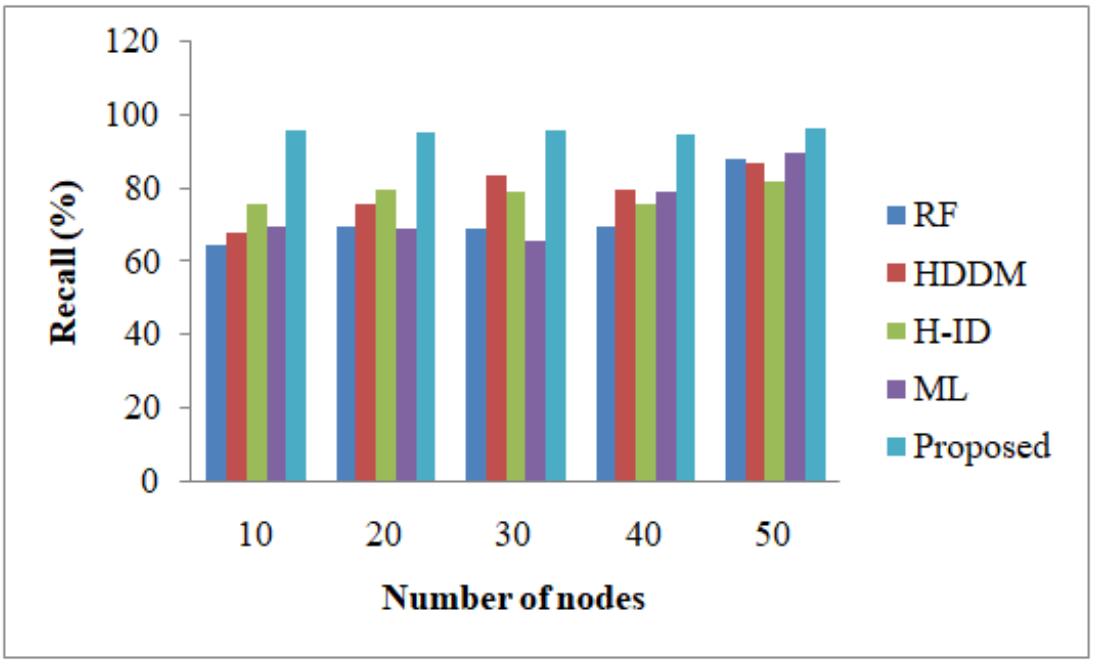


Figure 4.9: Comparative analysis of recall

According to **Table 4.3**, the examination on attainment metrics is evaluated and contrasted with existing works like RF, HDDM, H-ID, and ML. The table shows that our technique offers superior accuracy, precision, and retention of roughly 96.48%, 95.89%, and 96.56% respectively to the use of WSO together with the SVM classifier. In contrast to the proposed strategy, several existing approaches exhibit a lack of strategies for the aforementioned criteria.

Table 4.3: Evaluation based on recall, precision, and accuracy

Methods	Recall (%)	Precision (%)	Accuracy (%)
RF	87.78	89.37	90.38
HDDM	91.09	90.56	92.77
H-ID	89.09	91.45	89.55
ML	93.45	90.76	93.00
Proposed	96.56	95.89	96.48

4.5. SUMMARY

This chapter suggested an improved support vector machine-based collaborative vehicular ad hoc network intrusion detection system. Cluster construction was done by K-means clustering. The cluster heads for the formulated cluster were chosen using the Tabu Search-based Particle Swarm Optimization (TS-PSO) technique. The recommended mode increased throughput and energy efficiency, which decreased the latency in data transfer. By using blockchain, the planned VANET system's security has been achieved, and its dependability has been improved. The enhanced SVM model can also be used to provide trust-based collaborative intrusion detection on the VANET. In order to evaluate the effectiveness of the suggested work, the KDD99 dataset has been used and replicated with NS-2 software. The suggested method utilizes the least amount of energy and has the highest efficiency when 50 nodes are considered in contrast to current techniques like RF, HDDM, H-ID, and ML. The other methods like RF, HDDM, H-ID, and ML offer safety levels of 89.37%, 90.56%, 91.45%, and 90.76%, respectively, whereas the proposed technique has 95.89% protection level.

CHAPTER 5
OPTIMIZED CONVOLUTIONAL NEURAL NETWORK BASED PRIVACY COLLABORATIVE INTRUSION DETECTION SYSTEM FOR VEHICULAR AD HOC NETWORK

5.1. OVERVIEW

The safety of the vehicles during the transmission of data is achieved with the Vehicular Ad-hoc Network (VANET); occasionally the reliability of the data exchanged can be questioned with the lack of trust and privacy. In connection with this, a novel blockchain-based VANET structure is framed to secure the information that is exchanged and to provide enhanced confidentiality, scalability, and privacy. The cluster construction in the VANET network is achieved with the implemented Improved K-Harmonics Mean Clustering (IKHMC) model and cluster head selection is achieved with the novel Hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm and thus enables efficient throughput, energy utilization and reduction in delay. Additionally, blockchain enables reliability, and high security, and the trust-based collaborative intrusion detection in the VANET model is performed using an optimized (Seagull Optimization) Convolutional Neural Network (CNN). The proposed blockchain base collaborative approach has categorized the three classes of intrusion as Distributed Denial of Service (DDoS), Blackmailing, and Sybil attacks. It resolves the security concerns and encourages (rewarding) vehicles cooperation and prevents tedious detection procedures. The experimental findings showed that the suggested approach is efficient to be applied in vehicles with limited resources and also has higher benefits in terms of malicious node detection, overhead, end-to-end delay, and energy utilization.

5.2. PROBLEM STATEMENT

For the last decades, several methods have been stated by many researchers to surmount security vulnerabilities. Various machine learning methods such as support vector machine (SVM), random forest (RF), K-nearest neighbor (KNN), and Ensemble learning techniques were used to analyze the traffic and hackers in the VANET system. Several deep-learning approaches were also utilized to secure the data transformation in the VANET system. Even though ML techniques lead to the improvement of trustable detection techniques, currently there is no short review as to how ML and DL techniques can support academics and professionals traverse dissemination safety in VANET. In

context with these issues, it is ineluctable to propose a novel secured VANET system as well as a detection system. In this study, Blockchain is used for security purposes. For safe agreements, blockchain maintains contracts and processes data more quickly. Information is stored on the blockchain and used to anticipate and analyze data. Artificial intelligence is utilized to do categorization and feature extraction in order to assess the dependability of blockchain settings. The data is shared with clarity, security, and tracking ability to the entire network.

5.3. PROPOSED METHODOLOGY

The recommended study is based on the blockchain-based collaborative intrusion detection model in VANET. This employs four major phases such as:

i. Cluster formation with the improved K- harmonics mean clustering (IKHMC),
ii. A Hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm-based optimal selection of cluster head,
iii. Privacy preservation of VANET with Blockchain, and
iv. Collaborative optimized CNN based intrusion detection.

The schematic flow diagram of the proposed framework is explained in **Figure 5.1.**

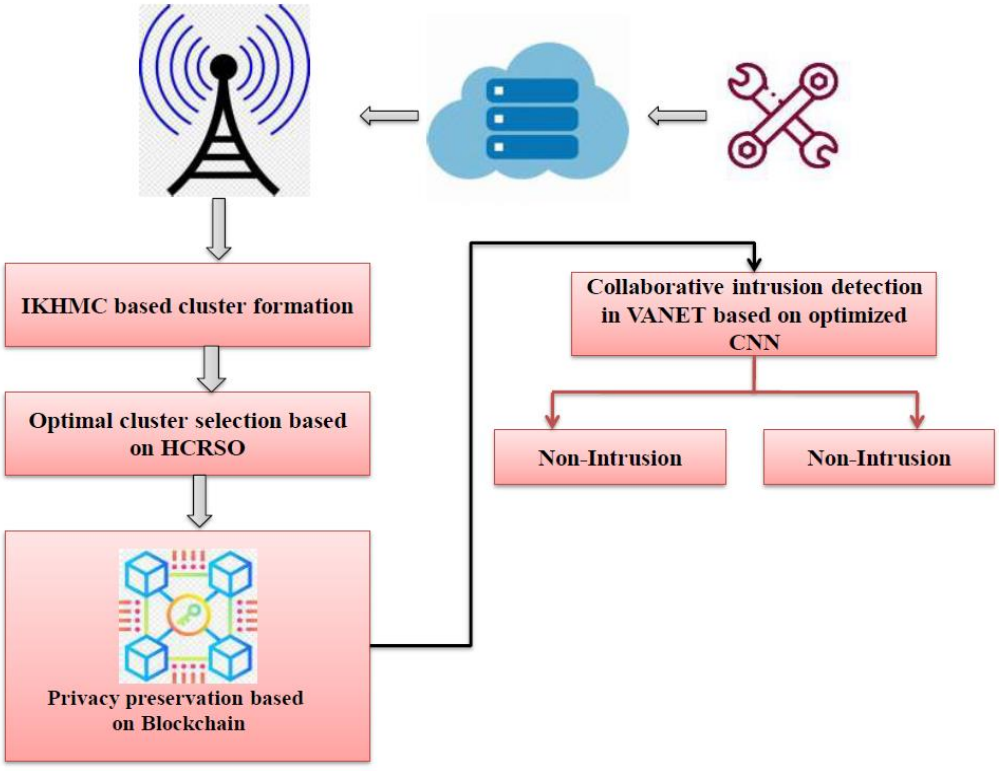


Figure 5.1: Schematic flow structure of proposed work

5.3.1. IKHMC-based cluster formation

The splitting of the VANET area into various clusters is performed by the IKHMC algorithm (Zhang et al. (2020)). This stage improves the delivery ratio with the simplification of routing and bandwidth allocation (Wang et al. (2016)). The negative Euclidean distance of the node's location using the positions y_j and y_j^{ce} and the velocity $VE_{y,j}$ and VE_{ce}^{j} can be expressed as,

$$ED(i,j) = \left(\left\|y_i - y_j\right\| + \left\|y_i^* - y_j^*\right\|\right) \tag{5.1}$$

$$y_i = \begin{bmatrix} y_i \\ z_i \end{bmatrix} (y_i)^* = \begin{bmatrix} y_i + V_{y,i} FT \\ z_i + V_{z,i} FT \end{bmatrix} \tag{5.2}$$

The next position can be predicted with the transfer function FT is denoted as $(y_i)^*$.

$$IKHMC_F = \sum_{i=1}^{M} \frac{J}{\sum_{j=1}^{J} \frac{1}{(d_{i,j})^2}} \tag{5.3}$$

The optimal centroidal position can be mined as

$$\frac{\partial F}{\partial y_j^{cen}} = J \sum_{j=1}^{M} \frac{4\left(y_i - y_j^{cen}\right) + \left(V_{y,i} - V_j^{cen}\right)}{d_{i,j^3}\left(\sum_{j=1}^{J} \frac{1}{d_{i,j^2}}\right)} \tag{5.4}$$

The j^{th} centroid y_j^{cen} with with optimal position is obtained and set $\frac{\partial F}{\partial y_j^{cen}} = 0$.

$$y_j^{cen} = \frac{\sum_{j=1}^{M} \frac{y_j + V_{y,j}}{d_{i,j^3}\left(\sum_{j=1}^{J} \frac{1}{d_{i,j^2}}\right)^2}}{\sum_{j=1}^{M} \frac{1}{d_{i,j^3}\left(\sum_{j=1}^{J} \frac{1}{d_{i,j^2}}\right)^2}} \tag{5.5}$$

5.3.2. HCRSO-based Cluster Head Selection

The cluster head of each cluster is chosen using the HCRSO algorithm and the new CH is updated regularly when new vehicles enter the network with the synchronization. Our approach utilized the features such as velocity and acceleration estimation from Capuchin

Search Algorithm (CSA) and to update the location Rat Swarm Optimizer (RSO) algorithm is used. Following the HCRSO algorithm the optimal CH is selected at unvarying time, and the power used and delay are mitigated with the enhancement of throughputs. The selection of the optimal cluster head is explained in the section below:

A. Capuchin search algorithm

The food-searching characteristics of the capuchin monkey and its strategies are used in this algorithm. The local food-searching strategy and global strategy are explained below (Braik et al. (2021)). Let us assume the movement of one tree to another tree of Capuchins are similar to the projectile motion as expressed

$$a = a_0 + v_0 t + \frac{1}{2} r t^2 \tag{5.6}$$

Here, '*a'* is the distance from the source tree to the destination tree like the source node to the targeted node (Fathy et al. (2022)). The initial location of the node is a_0. The acceleration of the vehicle is denoted as '*r'* under the time instance '*t'*, the velocity of the vehicle is indicated as 'v' and can be determined with the help of the first law of motion as expressed below,

$$v = v_0 + rt \tag{5.7}$$

Based on this algorithm, the initial velocity components of the vehicles are given as *a* and *b* and can be expressed as,

$$v_{0a} = v_0 \cos(\varphi_0) \tag{5.8}$$

$$v_{0b} = v_0 \sin(\varphi_0) \tag{5.9}$$

The initial velocities of the vehicles in the *a* and *b* directions are represented as v_{0a} and v_{0b} correspondingly. The angle concerning the a-direction is given as φ_0. The next step is to estimate the horizontal velocity of the vehicle obtained from equations 4.8 to 4.9.

$$\begin{aligned} v_a &= v_{0a} + r_a t \\ &= v_0 \cos(\varphi_0) \end{aligned} \tag{5.10}$$

The acceleration of the vehicle in the horizontal direction r_a is set as 0. Then the distance can be evaluated as,

$$a = a_0 + v_0 \cos(\varphi_0)t \tag{5.11}$$

B. Rat Swarm Optimizer

This is based on the food-searching characteristics of rats (Dhiman et al. (2021)) and expressed mathematically as shown below:

(i) Chasing the prey

After finding the location of the prey the rat will chase it as agonistic and the locations of the search agents are updated accordingly. Based on the performance of a search agent (vehicle) the positions of the search agents are updated. The upgradation of the locations is delineated as shown below,

$$\vec{D} = X.\vec{D}_i(a) + F.(\vec{D}_o(a) - \vec{D}_i(a)) \tag{5.12}$$

The location of the vehicle is indicated as $\vec{D}_i(a)$ and the best optimal vehicle node is stated as $\vec{D}_o(a)$. The parameters X and F are evaluated using the following equation

$$X = P - a \times \left(\frac{P}{Max_{iter}} \right) \tag{5.13}$$

Here, $a = 0,1,2,....., Max_{iter}$

$$F = 2.ran() \tag{5.14}$$

The *P* and *F* are random integers that fall under the values of 1 to 5 and 0 to 2 correspondingly. During iterations, the parameters X and F are used for the exploration and exploitation stage.

(ii) Fighting with prey

While performing the cluster head selection the location is updated with the features taken from the fighting behaviors of rats for the prey (Zebiri et al. (2022)). It can be expressed mathematically as,

$$\vec{D}_i(a+1) = \left| \vec{D}_o(a) - \vec{D} \right| \tag{5.15}$$

$\vec{D}_i(a+1)$ shows the updated location of the vehicle. The best node is picked based on this and all other nodes are arranged accordingly. Besides, it can also be used to find the optimal vehicle node from n-dimensional search space.

C. HCRSO algorithm for cluster head selection

Primarily HCRSO is focused for the hybridization of CSA and RSO and grasping the main features from both the algorithm to select the cluster head. In accordance with this, the velocity and acceleration features are taken from the CSA and to upgrade the location the features are collected from the RSO algorithm. The steps involved in this hybridization are stated below,

CSA:

- Initialization
- Movement of the vehicles
- Velocity and acceleration of the vehicle nodes

RSO:

- Based on the features collected the location is updated.
- After the completion of evaluating the optimal solution the location of all nodes are updated.

Based on the HCRSO algorithm, the optimal cluster heads are selected by minimizing the delay and energy consumption and thus increasing the throughputs. The schematic framework in **Figure 5.2** elucidates the Hybrid CRSO algorithm that is used for the optimal cluster head selection.

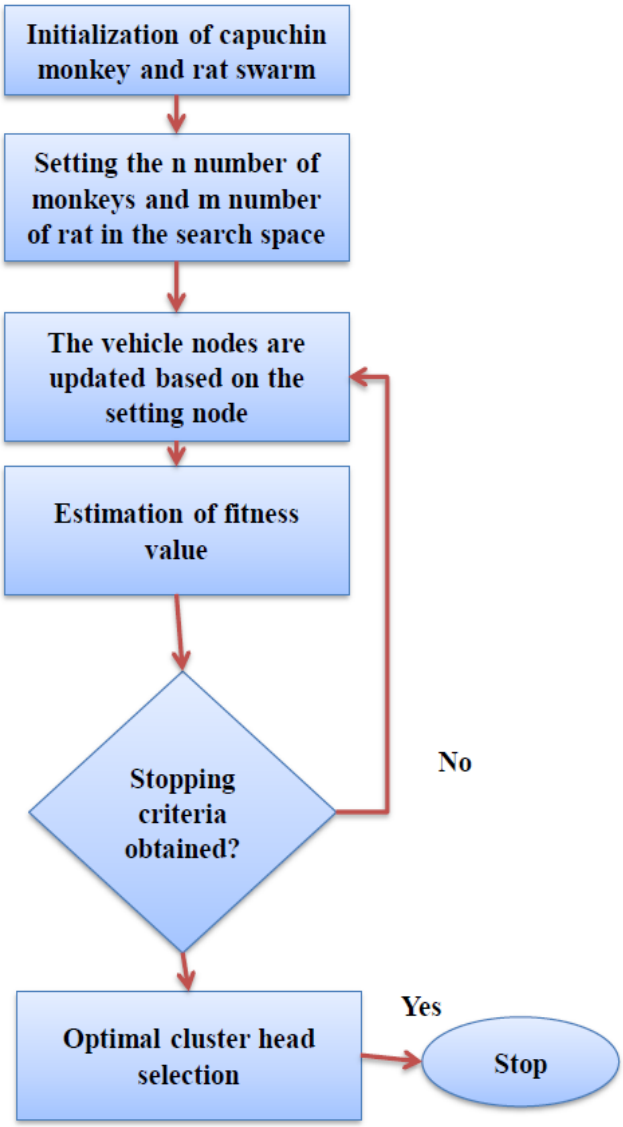


Figure 5.2: Proposed flow diagram of cluster head selection approach

5.3.3. Blockchain-based Privacy Preservation

To avoid the modification of shared data from one vehicle blockchain-based privacy preservation is maintained (Al-Omar et al. (2017)). This approach perpetuates security throughout the entire process. The peer-to-peer network system blockchain uses the duplication of vehicle nodes with the global machine approach. The risk of attack and downtime can be prevented with the feature of distributed sharing and storage capacity. The integrity and authenticity of the work can be ceaseless with the blockchain. With the lure and penalty approach of blockchain, the transfer of fake data is averted. Moreover, the transaction details are easily traceable by the authenticated user for future reference.

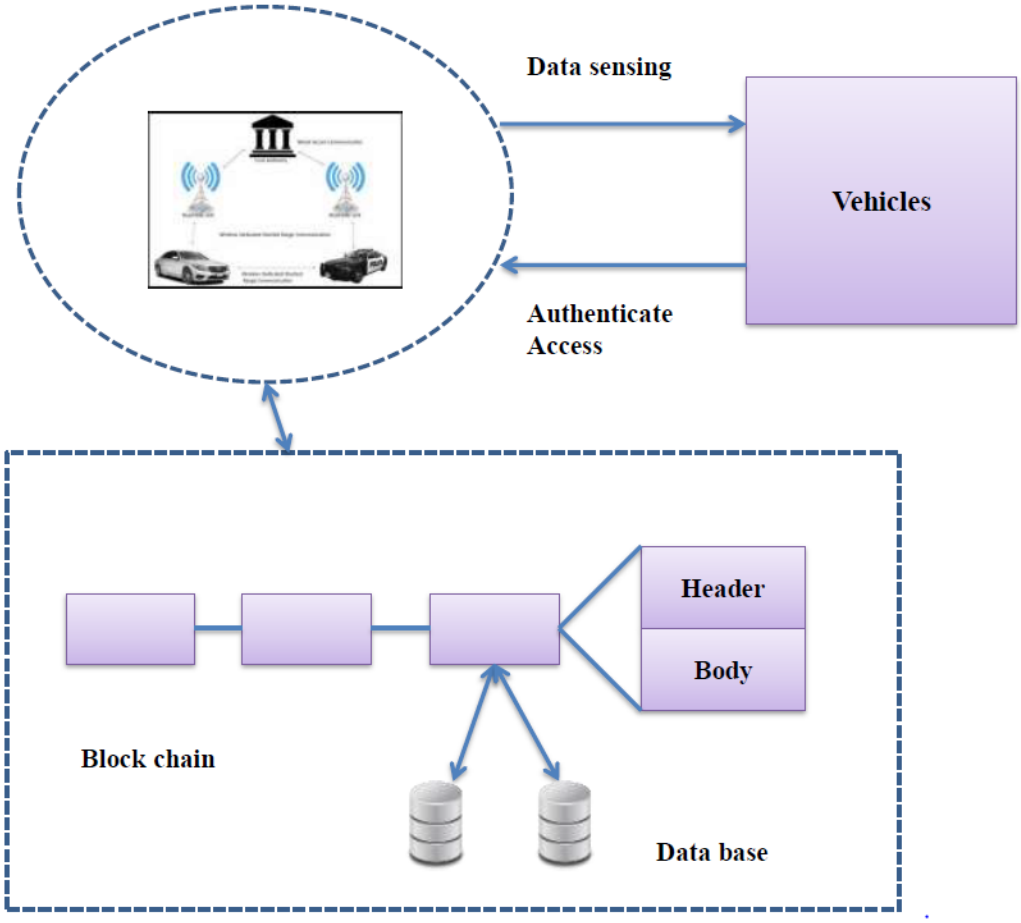


Figure 5.3: Blockchain-based privacy-preserving strategies of the VANET system

The data such as the individuality of the sender, accuracy of the model, and data signature is hoarded in the packets that are sent to the roadside units. With the estimation of metrics such as offset of the trusted RSUs and multiple RSUs incentives, mechanisms are computed with the proposed blockchain-based privacy-preserving policies. The proposed blockchain-based privacy-preserving strategies of the VANET system are illustrated in **Figure 5.3.**

5.3.4. Collaborative Intrusion Detection in proposed VANET

The trust values of VANET nodes are calculated with the CH node with the aid of a collaborative concept for the transmission of normal queries or obstacles. The primary aim of the collaborative aspect is to give feedback on the requested queries of the experimented nodes (Shu et al. (2020)). The recommended system is based on the seagull optimization-based CNN or optimized CNN model as explained below.

A. Convolutional Neural Network

The CNN (Yamshita et al. (2018)) consists of several multi-layer frameworks with neurons and the outputs can be obtained with the weighted sum of the previous layer. From the network data traffic features, the statistical features are significantly acquired. The k[th] neuron in the j[*th*] feature plane of the convolutional layer can be obtained as,

$$Con_{jk}^{O} = H\left(\sum_{j=1}^{FI} W_t^{IN} \times h\_Original_T^{IN} \right) \tag{5.16}$$

The T^{th} convolution kernel weight is W_t^{IN} and the filter length is FI. Based on the input layer, $h\_Original_T^{IN}$ is the weight of the convolutional kernel in the plane features. Where, $H_j(\cdot)\ as\ (j = 1,2,3)$ is the ReLU, *tanh* and sigmoid activation functions, which is explained as follows:

$$H_1(y) = \mathrm{Re}\,LU(y) = \max(0, y) \tag{5.17}$$

$$H_2(y) = \tanh(y) = \left(\exp^{y} - \exp^{-y}\right) \Big/ \left(\exp^{y} + \exp^{-y}\right) \tag{5.18}$$

$$H_3(y) = sig(y) = \frac{1}{\left(1 + \exp^{-y}\right)} \tag{5.19}$$

With the convolutional layer and flattened characteristics of the plane, the original features and advanced data are acquired, and hence the precision and validation rates are higher during the training process (Li et al. (2021)). However, overfitting issues occurred during this process and it was reduced with the above-stated performance by using improving the network generalization capacity. Moreover, the training of each neuron node in each batch is performed in the training cycle.

(i) Input layer

The number of activation mode neurons are set using the hole connection layer and in the fully connected layer, the below equation expresses the n^{th} neurons FLC_n^{Out}.

$$FLC_n^{Out} = H\left(\sum_{m=1}^{cw} \times cw_m + a_n\right) \tag{5.20}$$

After the flattening and dropout, the number of neurons is denoted as cw_m and the connection weight is cw. The offset of n^{th}neuron is a_n.

(ii) Output layer

An output layer transfers the output value of the fully connected last layers. Various kinds of VANET attacks are classified by the expression of softmax.

$$SM(z)_j = \exp^{z_j} \Big/ \sum_{j=1}^{AT} \exp^{z_j} \tag{5.21}$$

Various kinds of attack detection are represented as AT and the output value is y_j.

$$CEL(q,r) = -\sum_{y} APD(y) \log\ EPD(y) \tag{5.22}$$

The distance between the estimated probability distribution $EPD(y)$ and the actual probability distribution $APD(y)$ are measured using the cross-entropy loss function as $CEL(q,r)$.

B. Seagull Optimization (SO) Algorithm

This SO is based on the characteristics and features of an omnivorous seagull that eats earthworms, reptiles, fishes, insects, and amphibians (Dhiman et al. (2021)). In general, it is called Laridae and seagull is its scientific name. The numerical expressions are shown below,

(i) Exploration or Migration:

During migration the seagulls' get shifted from one location to another, however, three factors are considered during this process: collision avoidance, motion to the optimal nearer direction, and closer remain to the optimal search agent. To circumvent the collision with the neighbors an additional parameter AV has been considered while evaluating the new search agent.

$$\overrightarrow{SC} = AV \times \overrightarrow{PS}(y) \tag{5.23}$$

The *y*-search agent position and current search agent position are $\overrightarrow{SC}$ and $\overrightarrow{PS}$. The current iteration is *y*. The frequency variable is controlled using the factor CF .

$$AV = CF - \left(y \times \left(CF / Itr_{\max}\right)\right), \quad where,\ y = 0,1,2,..., Itr_{\max} \tag{5.24}$$

After neglecting the collision among the neighbors the search agent moves in the best neighbor's direction (Panagant et al. (2020)). The search agent position $\vec{S}_P$ and the best search agent $\vec{B}_P$ are represented as $\overrightarrow{SM}$. The randomization behavior is K . The random number falls into the interval [0, 1].

$$\overrightarrow{SM} = K \times \left(\vec{B}_P(y) - \vec{S}_p(y)\right)$$

$$K = 2 \times AV^2 \times random$$

The locations of the best search agent and the respective seagulls; are updated based on the best search agent. $\vec{SD}$ is used to evaluate the distance between the search agent and the optimal best fit.

$$\vec{SD} = \left|\overrightarrow{SC} + \overrightarrow{SM}\right| \tag{5.25}$$

(ii) Exploitation or Attacking:

The location of the search agents are upgraded using the following equations. The best solution is stored by using $\vec{S}_p(y)$ and the other search agent position is updated.

$$\vec{S}_p(y) = \left(\overrightarrow{SD} \times y` \times z` \times x`\right) + \overrightarrow{B_P}(y) \tag{5.26}$$

The pseudocode of the proposed algorithm is elucidated in **Algorithm 1**.

Algorithm 1: Pseudocode of the seagull optimization algorithm

Input: Initialize the Population of seagull $\vec{S}_p$

With the maximum number of iterations, the parameters AV and K are initialized.

set $CF \leftarrow 2$

While (y< max_iteration) **do**

$\vec{B}_P \leftarrow fitnesscalculation\left(\vec{S}_p(y)\right)$

$random \leftarrow random(0,1)$

$x \leftarrow random(0, 2\pi)$

Calculate the distance the distance $S\vec{D} = \left|\overrightarrow{SC} + \overrightarrow{SM}\right|$

$S = y` \times z` \times x`$

$\vec{S_p}(y) \leftarrow \left(\left(\overrightarrow{SD} \times S\right) + \overrightarrow{B_P}\right)$

$y \leftarrow y + 1$

End While

Return $\vec{S_p}(y)$

C. Optimized CNN model for collaborative intrusion detection in VANET

The advantages of CNN are precise classification and detection outcomes which are easy to implement and understand. However, improper hyper-parameter tuning might have pushed this to increase computational complexity and lower detection outcomes. This can be surmounted with the assistance of a novel Seagull Optimization algorithm which finely tunes the hyper parameters with the features of efficient searchability and convergence speed. Accordingly, this approach utilizes the collaborative CNN-SO for the detection of intrusion as depicted in **Figure 5.4.** The CNN structure related to every seagull's position and continuous iteration determines the optimal network structure parameter. In order to determine various kinds of attacks, analyze the actual requirements and the necessity to predict the effect of optimal prediction. The predicted and real value difference is

evaluated via the loss function. It encodes the actual labels in the CNN model and the softmax layer obtains every class (intrusion and non-intrusion) prediction probability.

In the initial training cycle, the HCRSO algorithm provides less cross-entropy loss function, which is set as the fitness function. Determine the minimum loss function value depending on the variable structure parameters of every layer via the HCRSO algorithm (Braik et al. (2021)). The cross-entropy loss function is calculated by obtaining each seagull fitness value in the current iteration. An average fitness value is calculated and stores the minimum fitness value of every seagull. The migration or exploration step of the seagull is initialized to optimize the CNN parameters. The optimal solution or optimal intrusion detection results are obtained if the SO algorithm meets the maximum number of iterations otherwise it repeats the entire process. Finally, the collaborative intrusion and non-intrusion classes in VANET are classified. From this, the three intrusion classes in VANET such as Distributed Denial of Service (DDoS), Blackmailing and Sybil attacks are further divided.

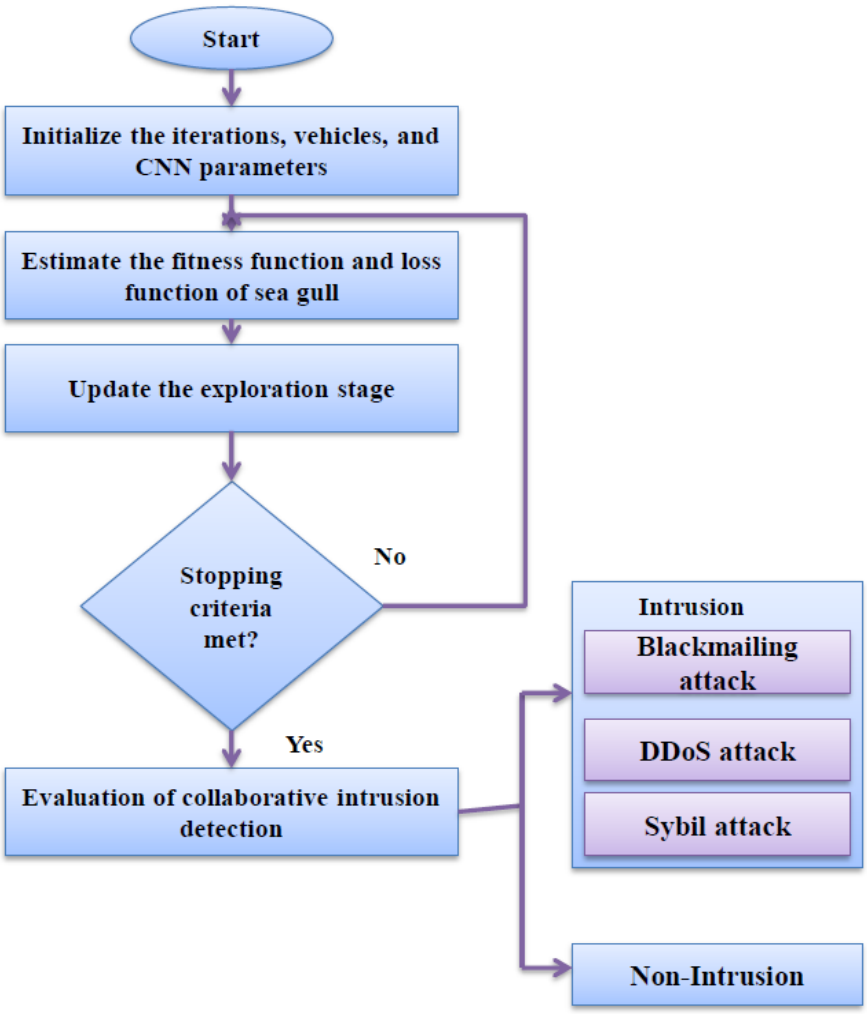


Figure 5.4: Proposed collaborative intrusion detection structures

5.4. RESULT AND DISCUSSION

In this section, the performance of the proposed model and its respective comparative analysis are discussed. The effectiveness is analyzed with different parameters and compared with existing approaches. For analyzing purposes the dataset are taken from the https://www.kaggle.com/bigquery/ethereum-blockchain with the recoverable sample. From this data, 70% of data is used for training and the balance 30% is used for testing process during intrusion detection. The simulation is carried out in the NS-2 simulator and the parameters used are listed in **Table 5.1.**

Table 5.1: Parameter settings for simulation

Parameters	Values
Initialized population	50
Iterations used in maximum	100
Nodes taken	100
Simulation range	$1.5km * 1.5km$
Transmission range	280 m
Speed movement	4 m/sec

5.4.1. Performance Metrics

The metrics taken for the effective assessment of the frame work are delay, throughput, accuracy, energy consumption, decryption time and encryption time, and detection rate.

$$Accuracy = \frac{T^{-ve} + T^{+ve}}{T^{+ve} + T^{-ve} + F^{+ve} + F^{-ve}} \quad (5.27)$$

In the meantime, the total number of attacks detected with the metric is known as detection rate. The detection rate is the rate from which the intrusion and non-intrusion are classified accurately. It can be expressed as,

$$Detection\ rate = \frac{T^{+ve}}{T^{+ve} + F^{-ve}} \quad (5.28)$$

From the above equations, the true positive and negative classes are depicted as T^{+ve} and T^{-ve}. Further, F^{+ve} and F^{-ve} are the false positive and negative classes.

(i) Delay:

Delay is the extra time taken by the packets to reach the destination than the expected time in the VANET system.

(ii) Throughput:

At the determined time, the number of units travelled to the destination is measured as throughput.

(iii) Energy consumption:

The total energy consumed to progress from point of supply to target is taken as energy consumption.

5.4.2. Performance Analysis

The acquisition analysis based on the detection rate is visually illustrated in **Figure 5.5.** It implies the comparative outcomes of the recommended methods like (Decentralized based key management system) DB-KMM (Ma et al. (2020)), (Fine grained access control) FADB (Li et al. (2020)), (Cipher text policy attribute based encryption) CP-ABE (Horng et al. (2020)), and (Practical byzantine fault tolerance) PBFT (Meshcheryakov et al. (2021)). The effectiveness of detecting the intrusion and non-intrusion of the proposed technique is high due to the addition of collaborative approaches and is not depended on the number of nodes. The proposed approach shows a detection accuracy of 94.3% and other state-of-art approaches such as DB-KMM, FADB, CP-ABE, and PBFT shows 89%, 89.76%, 90.12%, and 91.8% respectively. This shows better efficacy in terms of detection accuracy for more nodes too.

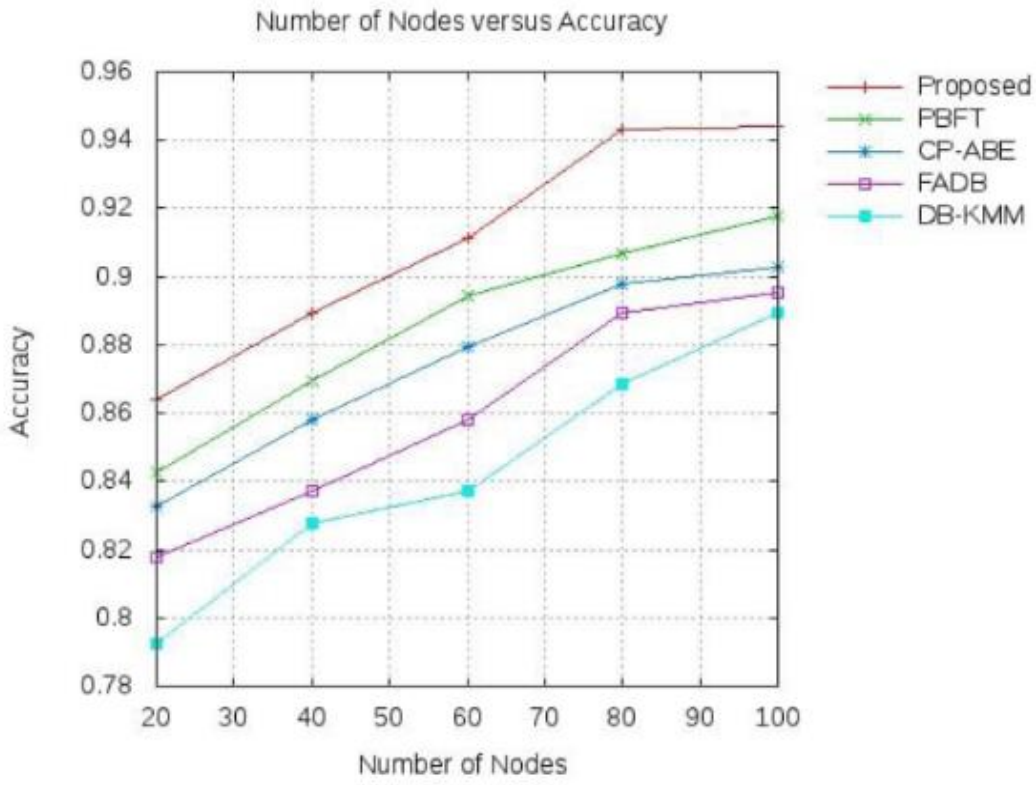


Figure 5.5: Performance analysis based on the detection accuracy

The common screenshots for VANET nodes are given in **Figure 5.6, Figure 5.7** depicts the screenshots for VANET nodes initialization process. **Figure 5.8** illustrates the screenshots for cluster head selection.

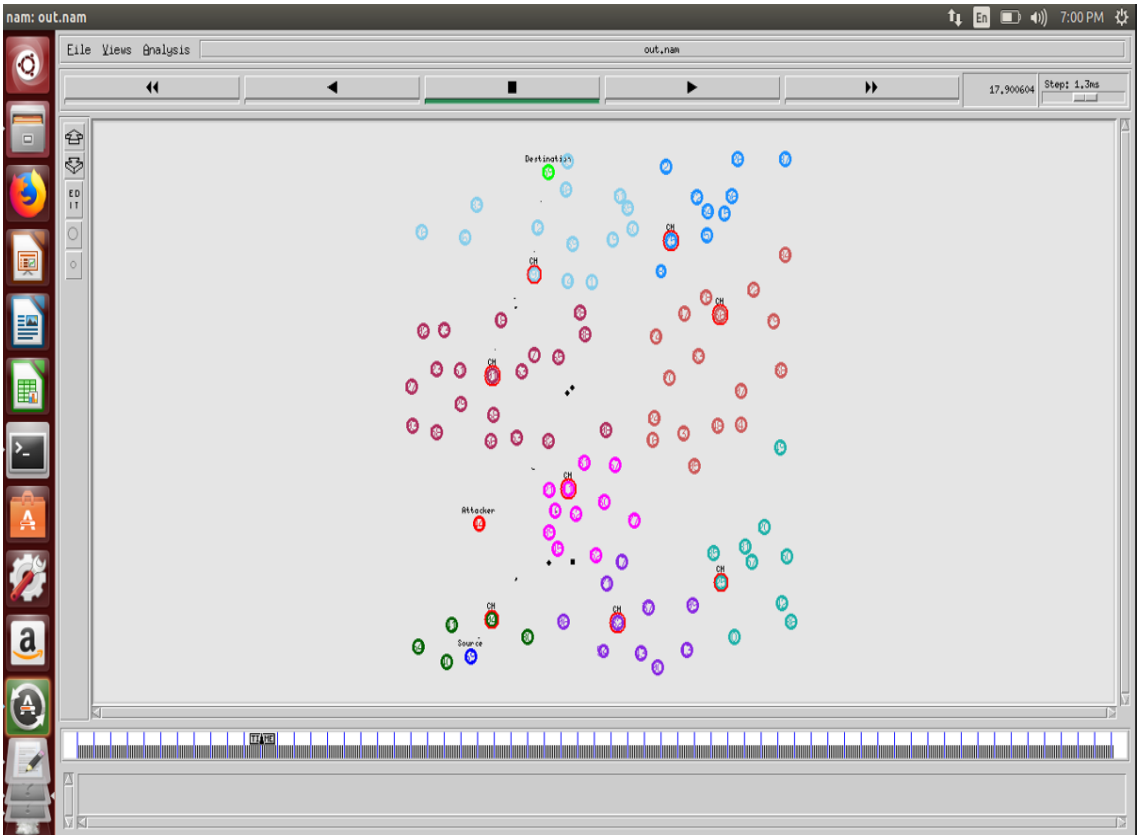


Figure 5.6: The common screenshot for VANET nodes

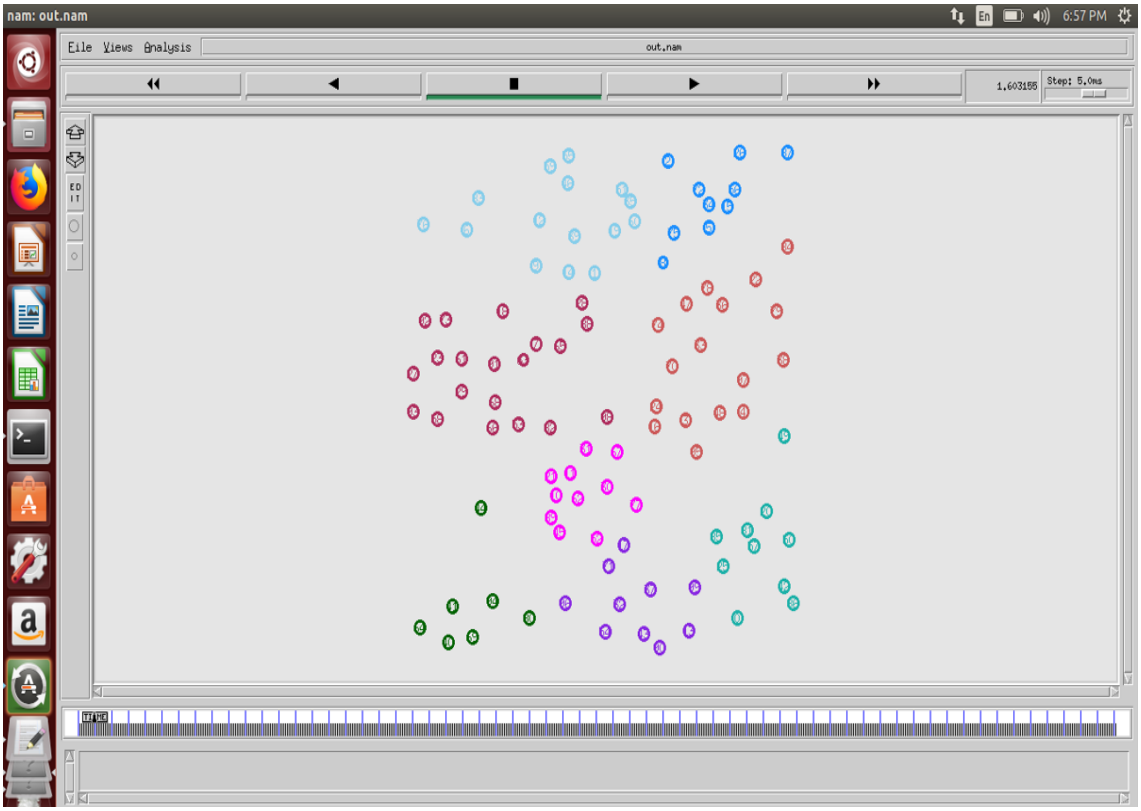


Figure 5.7: The screenshot for VANET nodes initialization process

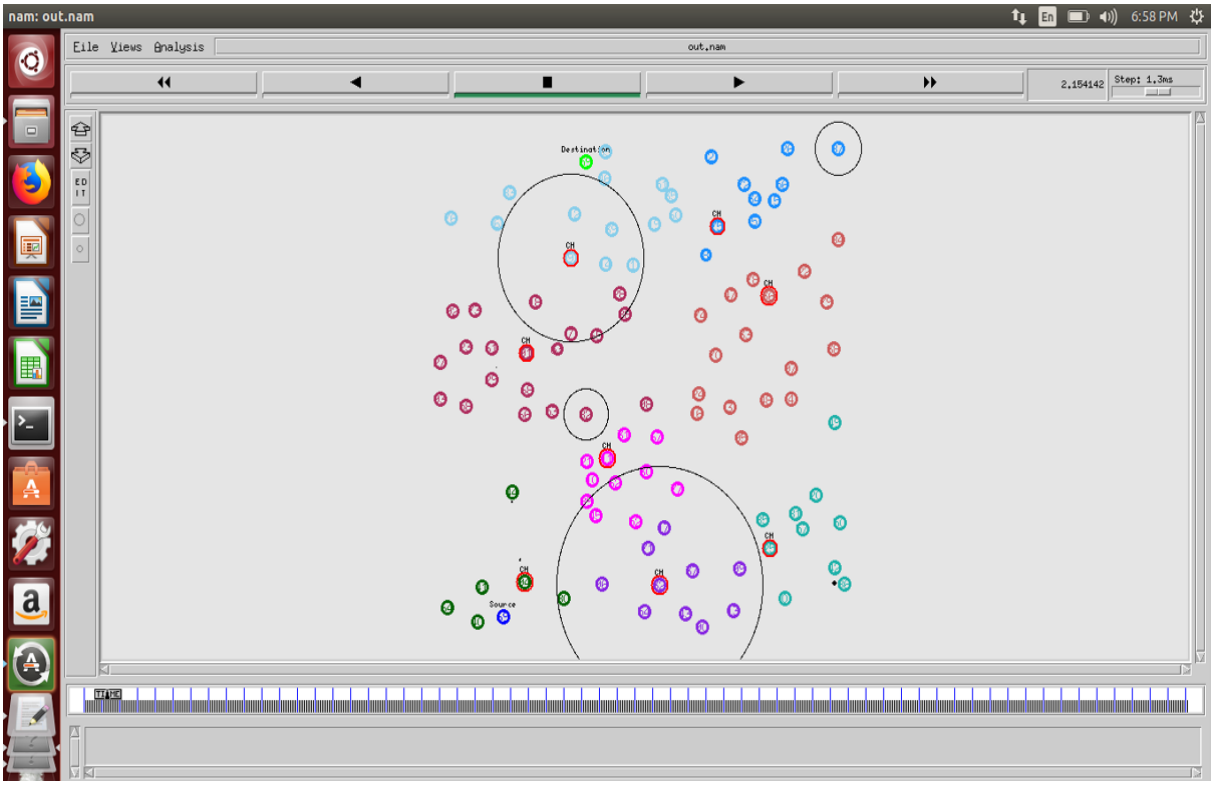


Figure 5.8: The screenshot for cluster head selection

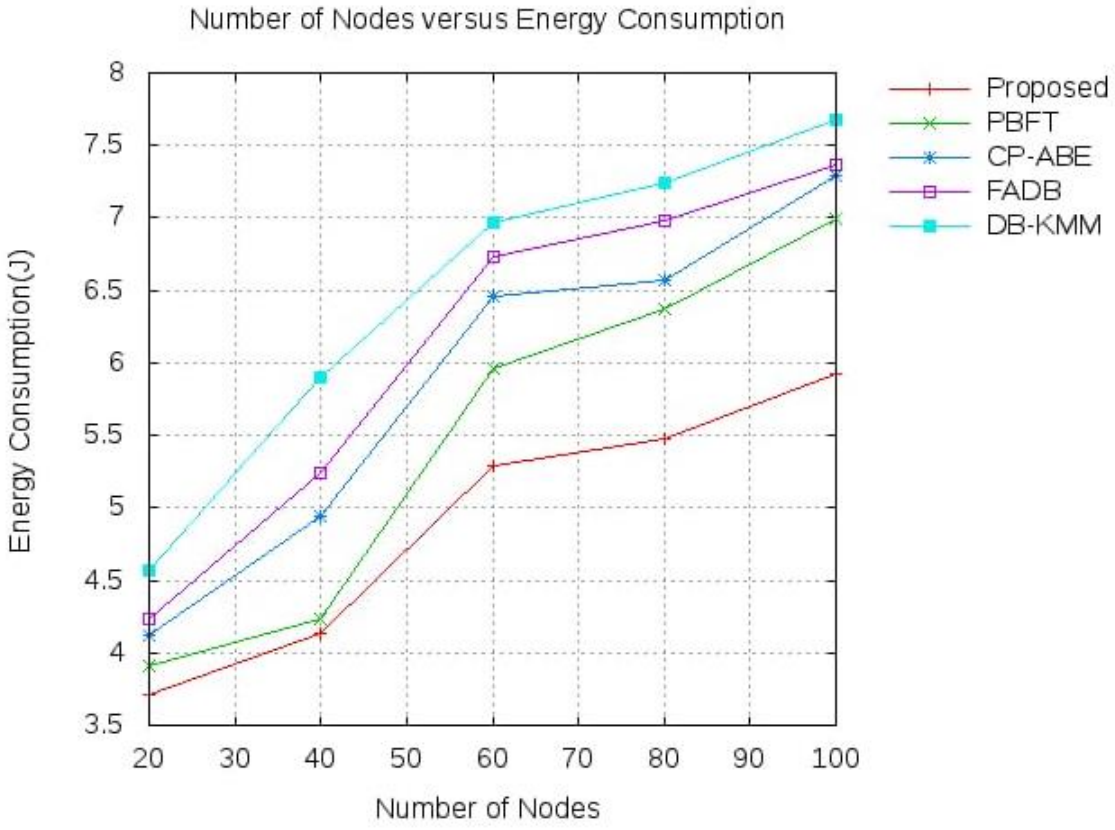


Figure 5.9: Performance analysis based on the energy consumption

The visual representation of effectiveness based on power consumption is illustrated in **Figure 5.9**. Here, the energy consumption by different approaches with varying nodes is observed. The amount of energy consumed likewise rises with the number of nodes. The energy consumption of different methods such as DB-KMM, FADB, CP-ABE, and PBFT are analyzed with the prompted approach. The nodes are selected as 20, 40, 60, 80, and 100. From the visual itself it is clear that the preferred proposal consumes low energy when compared to other. Since the CH is selected with the optimal approach and by using an effective approach the cluster formation was made, the routing path has been reduced, and it also removes the unwanted nodes and hacking nodes. This automatically reduces the energy consumption of the proposed approach more than the other approaches.

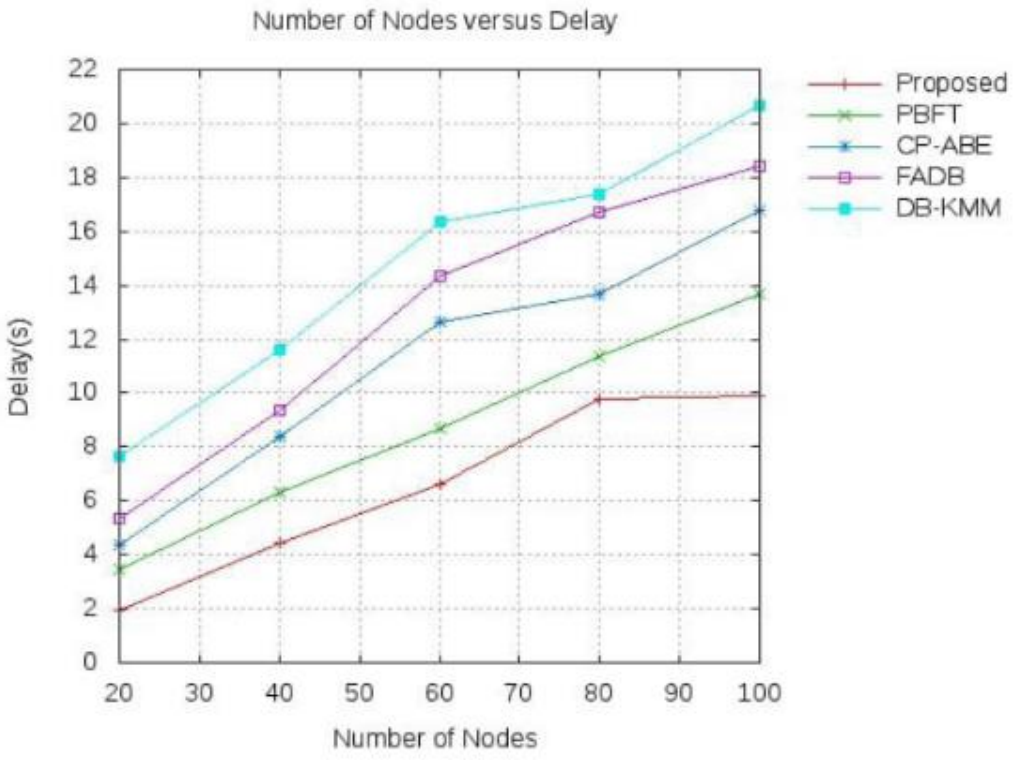


Figure 5.10: Performance analysis based on the delay

Delay might have occurred due to various reasons such as a longer routing path, malicious nodes in the path, and improper selection of CH. Since, the proposed approach effectively chooses the CH and cluster formation, the delay while passing packets from source to destination is lower as shown in the visual representation in **Figure 5.10**. The delay occurred by the proposed approach while using 100 nodes is less than 10 sec while other approaches such as DB-KMM, FADB, CP-ABE, and PBFT have higher delays of 20.65 sec, 13.9 sec, 16.4 sec, and 18.3 sec respectively.

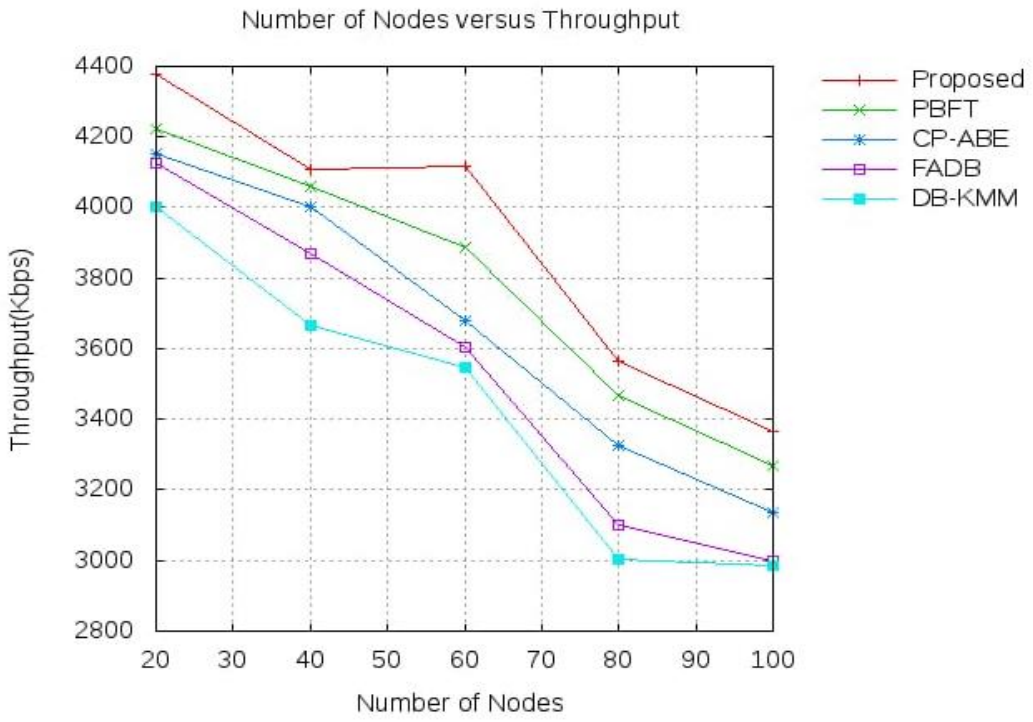


Figure 5.11: Performance analysis based on the throughput

The performance analysis on the throughput is visually plotted in **Figure 5.11**. Since the blockchain-based security system provides better security it helps in neglecting the malicious nodes and protects the information shared between the source and destination. As shown in **Figure 5.11**, the loss of packets is low for the proposed approach than the other approaches. Upto 100 nodes are taken and analyzed for the throughput.

Further, the screenshots for VANET attack is displayed in **Figure 5.12, Figure 5.13** describes the screenshots for attack.

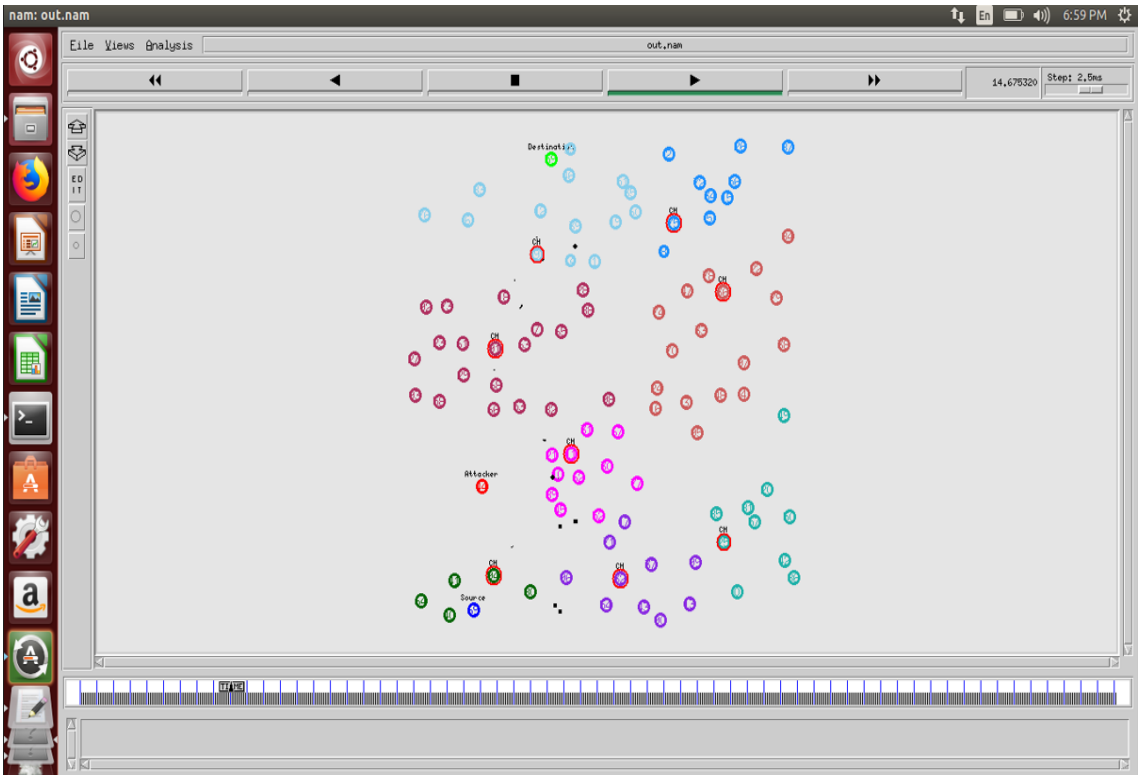


Figure 5.12: Screenshot for VANET node communication

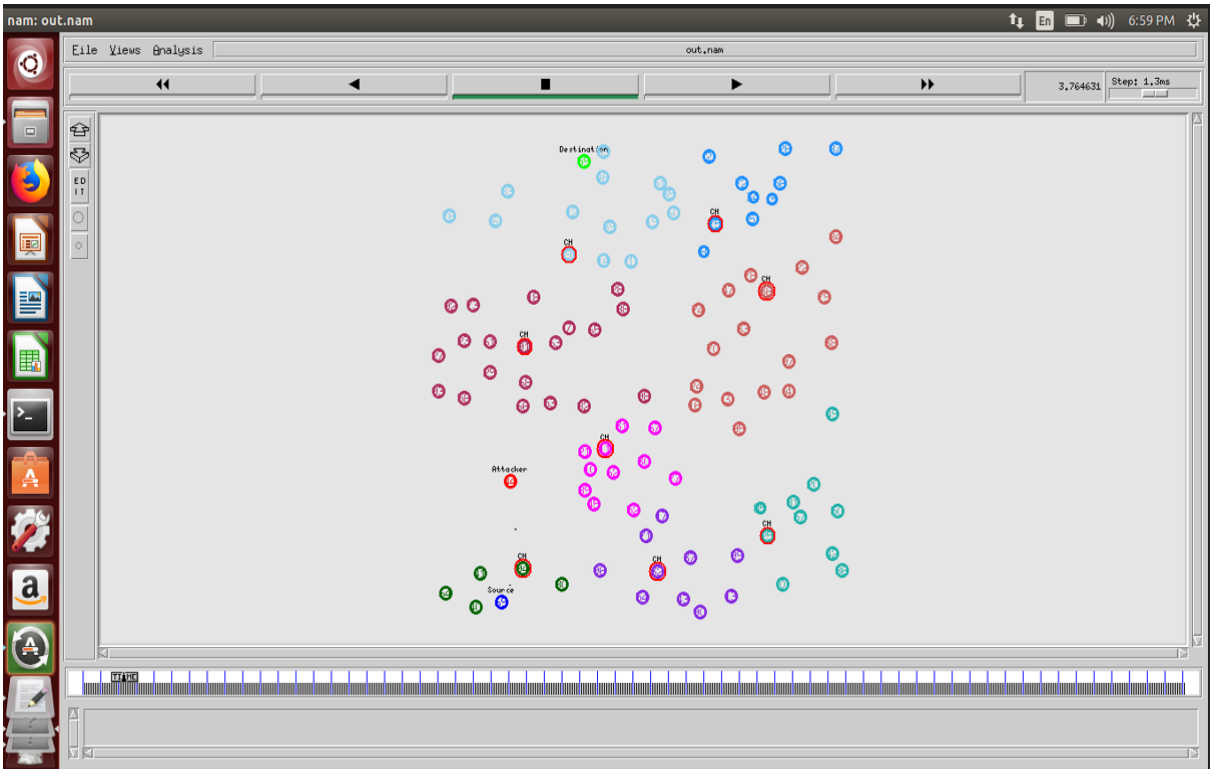


Figure 5.13: The screenshot of attack

The visual illustration based on the detection ratio and the amount of nodes is shown in **Figure 5.14**. According to the implementation result, the suggested technique identifies the intrusion more successfully than the other approaches. When the node is equal to 100, our suggested method identifies the intrusion with a ratio of 94. 25%. The DB-KMM, on the other hand has the lowest a detection ratio of 86.97%. Further, the PBFT, CP-ABE, and FADB achieve a detection ratio of 91. 67.2%, 89.36%, and 87.26% respectively.

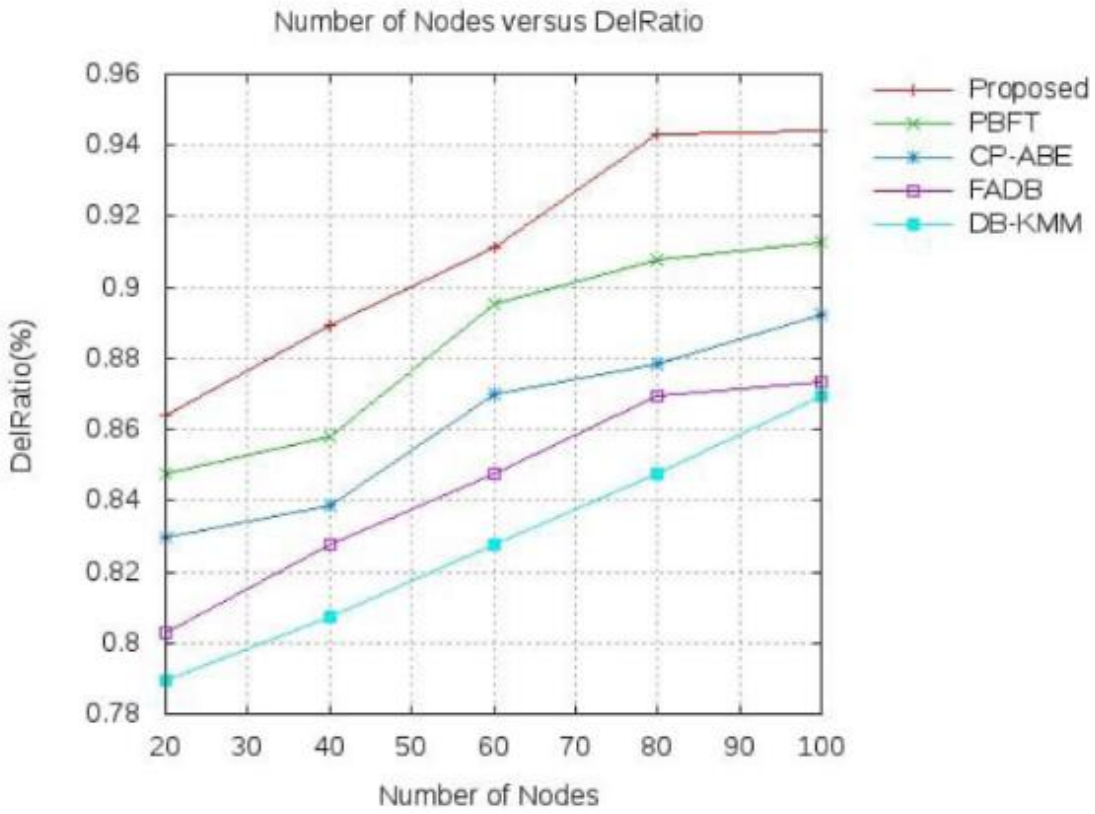


Figure 5.14: Performance analysis based on the detection ratio vs. number of nodes

The next important parameter is security analysis which is indexed in **Table 5.2.** The security of the suggested approach is high due to the inclusion of blockchain-based privacy preservation and the optimized CNN technique. The protection of the suggested method is 97.6% and the security of the other methods like DB-KMM, PBFT, CP-ABE, and FADB is 89.3%, 93.7%, 92.1%, and 94.4% respectively. This shows that the proposed approach can be used for the secured VANET system.

Table 5.2: Performance analysis in terms of security level

Methods	Security level
DB-KMM	89.3%
PBFT	93.7%
CP-ABE	92.1%
FADB	94.4%
Proposed	97.6%

5.5. SUMMARY

In this work, Seagull Optimization-based CNN approach is used for the detection of intrusion. The intrusions such as blackmailing, DDoS, and Sybil attacks are also detected. Apart from this it also provides better security with the inclusion of a blockchain-based security system. Collaborative intrusion detection was used to differentiate the intrusion and non-intrusion nodes. The cluster formation is achieved with the novel IKHMC and the CH was selected with HCRSA approaches that were utilized to form the effective clusters to pass the packets throughout the network. The implementation was carried out in the NS-2 simulator. The suggested method outperforms all current efforts in terms of throughput, accuracy, attack detection ratio, and security level when results are compared. The results were compared with the approaches such as DB-KMM, PBFT, CP-ABE, and FADB for 100 nodes. The outcomes depicted that the proposed approach consumes less energy, delay, higher throughput, accuracy, and detection ratio. The security of the proposed work was higher and shown in percentage as 97.6% and the detection accuracy as 94.3%.

CHAPTER 6
RESULT AND DISCUSSION

6.1. OVERVIEW

This chapter discusses the comparative experimental investigation of IDS in VANET. The proposed framework is enhanced with three novel techniques. The experimental results are implemented on an NS-2 GPU-based computer with a GTX1050 GPU and 16GB RAM, as well as an Intel Core i5-8300H CPU running Tensorflow 1.15. The experimental data collected from two datasets namely KDD99 dataset and Kaggle dataset, which is simulated under NS-2 platform. The comparative analysis is performed via proposed SVM-WSO and CNN-SO methods are effectuated with the state-of-art works such as Fuzzy C-means (Sparse FCM) clustering algorithm, Adaptive Neuro-Fuzzy Inference System (ANFIS) modeling methods.

6.1.1. Dataset Description

Table 6.1: Dataset details

Dataset Names	**Features**	**Total number of Instances**
KDD99	41	5 million records
Kaggle	57	50000 public records of IDS

The **table 6.1** represents the datasets KDD99 and Kaggle values for performing this research. Where KDD99 dataset is a widely used benchmark dataset for intrusion detection systems. It contains network traffic data from a simulated environment, including both normal and attack traffic. Also kaggle is a platform that hosts a variety of datasets to cover a wide range of topics, including healthcare, finance, and social media.

6.2. EVALUATION MEASURES

Accuracy, precision, recall, detection rate, energy consumption, delay and throughput performance indicators are utilized to verify the usefulness of the proposed framework. All of these performance metrics for intrusion detection performance efficiency are explained by the ensuing equations.

$$Accuracy = \frac{T_N + T_P}{F_N + T_N + F_P + T_P} \tag{6.1}$$

$$\text{Pr}ecision = \frac{T_P}{F_P + T_P} \tag{6.2}$$

$$\text{Re}call = \frac{T_P}{F_N + T_P} \tag{6.3}$$

Meanwhile, the total count of assaults is identified by detection rate metric. The rate at which intrusions and non-intrusions are successfully identified is known as the detection rate. One way to put it is as follows:

$$Detection\ rate = \frac{T_P}{T_P + F_N} \tag{6.4}$$

From this, true positive (T_P) and true negative (T_N) are the quantity of successfully predicted intrusion classes and the number of correctly predicted non-intrusion classes respectively. Additionally, a number of false positive (F_P) and false negative (F_N) classifications for incursion and non-intrusion were predicted wrongly.

Delay: In the VANET system, delay is the extra time packets take to reach their destination compared to the expected time.

Throughput: The number of units travelled to the destination at the specified time is measured as throughput.

Energy consumption: Energy consumption is calculated as the total energy consumed to forward packets from source to destination.

6.3. COMPARATIVE ANALYSIS

In this part, the comparative study of the suggested SVM-WSO and CNN-SO is effectuated with the state-of-art works such as Fuzzy C-means (Sparse FCM) clustering algorithm, Adaptive Neuro-Fuzzy Inference System (ANFIS) modeling and design, Multi-branch Reconstruction Error IDS (MRE-IDS). For the analysis, the criterion like Delay, Throughput, Accuracy, DelRatio, Energy consumption, and security analysis were considered.

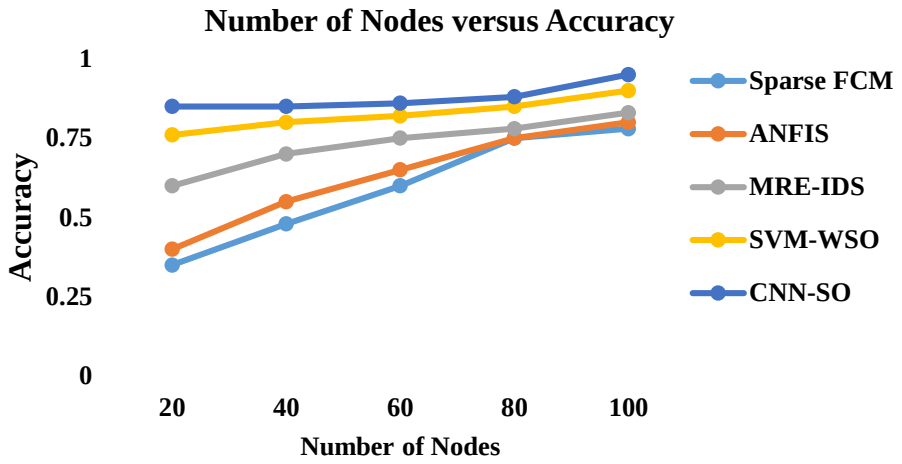


Figure 6.1: Comparative assessment based on accuracy

The comparative assessment of proposed approaches SVM-WSO and CNN-SO are made with the state-of-art works such as Sparse FCM, ANFIS and MRE-IDS and is outlined in **Figure 6.1**. The proposed approaches use the collaborative approach and hence the detection accuracy is higher than the other approaches. Moreover, the CNN-SO depicts better outcomes due to the usage of deep learning CNN which is best method to detect the intrusion than other approaches. The inclusion of SO might had increases the detection accuracy by tuning the hyper parameter of CNN. The accuracy of methods changes with the quantity of vehicles used. For smaller count of vehicles the accuracy is lower and it gradually increases with increasing number. When the count of nodes is equal to 100 the detection accuracy of CNN-SO is 94.3%, whereas, SVM-WSO depicts 93.5%. Other approaches show lower detection accuracy.

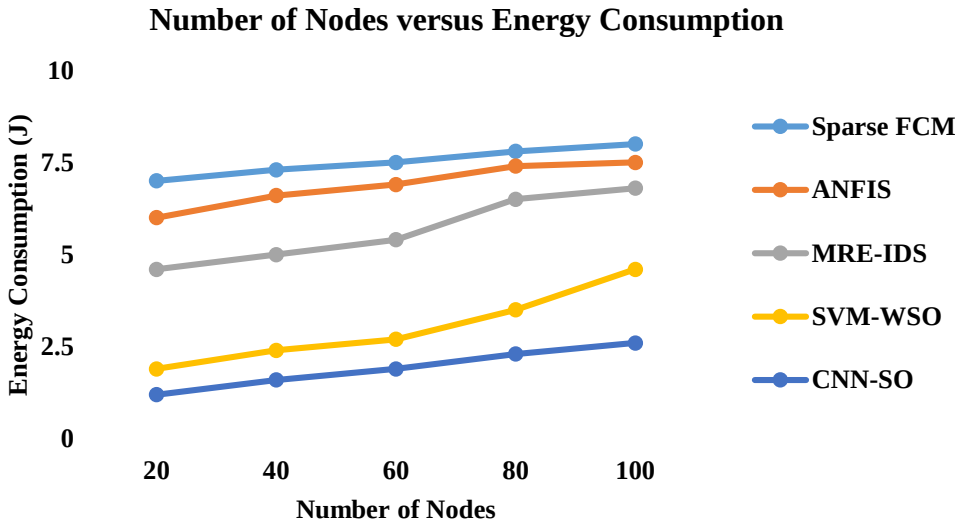


Figure 6.2: Comparative assessment based on energy consumption

Figure 6.2 illustrates the comparative assessment of proposed with state-of-art works in terms of Energy consumption. The energy consumption of proposed is lower than the other approaches. Meanwhile, the vitality rises with count of nodes and the proposed approach consumes limited power and for 100 nodes the energy consumption is 2.53J and for SVM-WSO the energy consumption is 4.23J.

The parallel study on the delay is pictorized in **Figure 6.3.** The delay of the recommended approach is smaller due to the usage of effective methods and blockchain based security. The delay rises with the increasing number of nodes. The method CNN-SO has the delay of 8.12 s for 100 nodes and SVM-SO has delay of 10.67s for the same.

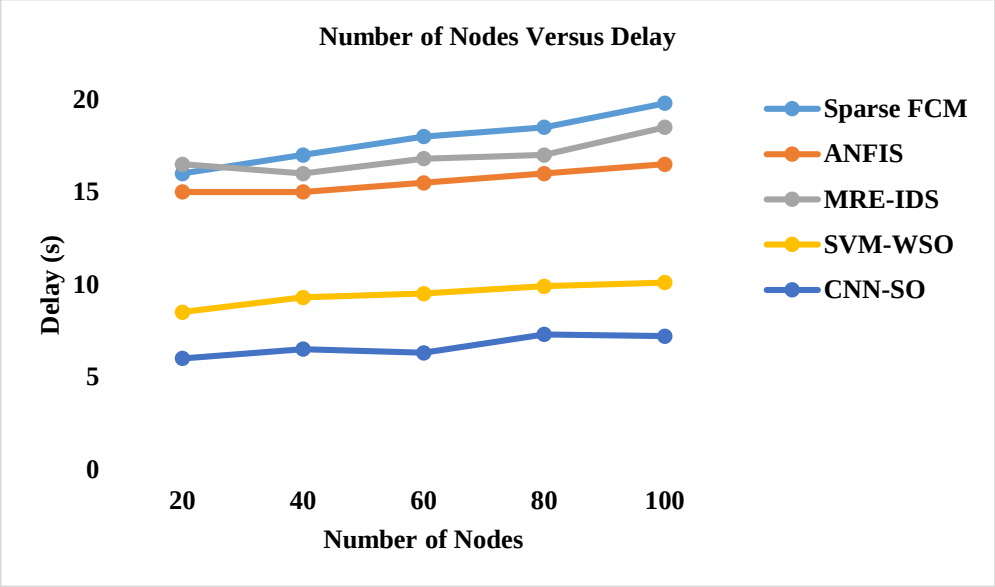


Figure 6.3: Comparative assessment based on delay(s)

Throughput of the network weakening with the total of nodes as illustrated in **Figure 6.4**. the proposed approaches CNN-SO and SVM-WSO possess higher throughput of 4400kbps and 4100kbps for 20 nodes and for the nodes of 100 they possess 3900kbps and 3300kbps which is higher than the other state-of-art methods. This is because that proposed approaches explicitly increases the throughput with the exact technique selection.

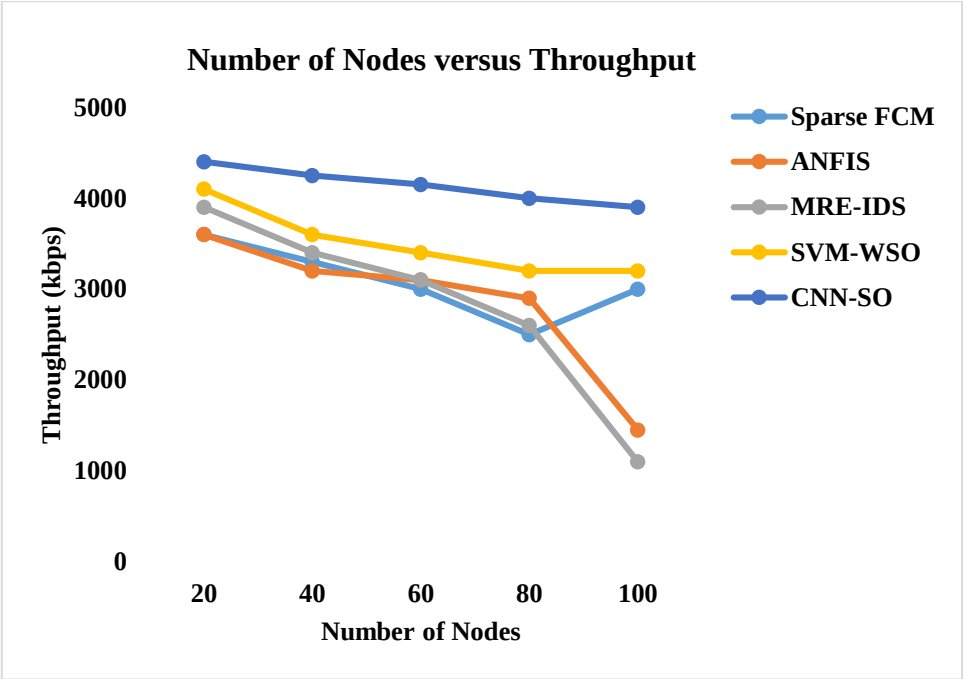


Figure 6.4: Comparative assessment based on throughput (kbps)

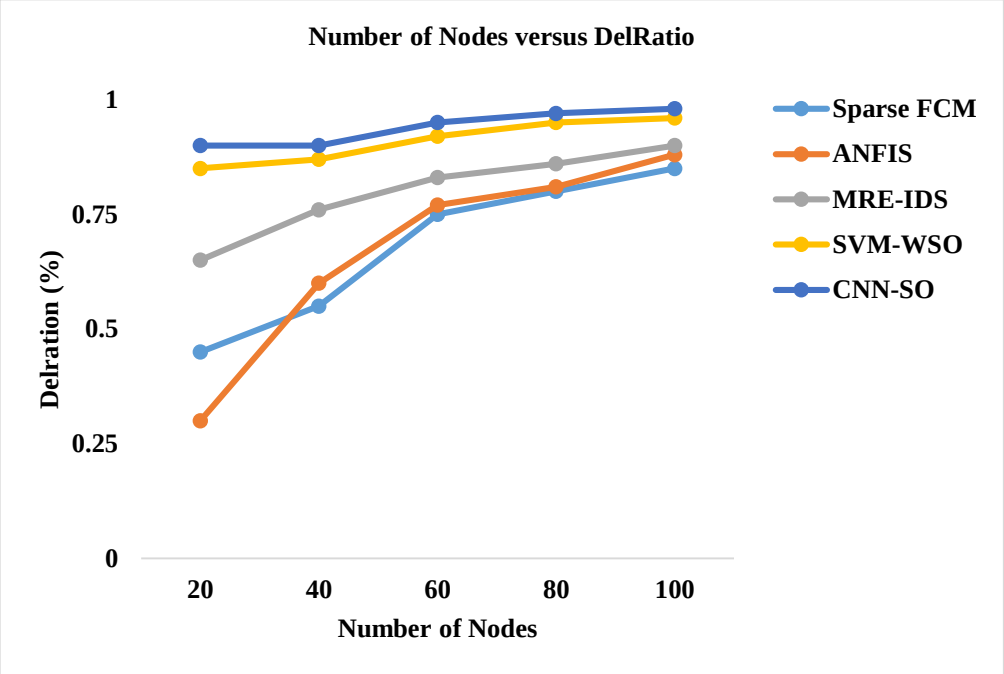


Figure 6.5: Comparative assessment based on delratio (kbps)

Comparative analysis based on the Delratio for various numbers of nodes is depicted in **Figure 6.5**. The Del ratios of preferred approaches are higher and increases with the sum of nodes. For number of nodes 100 the Del ratio of proposed approach CNN-SO is 0.96 and for SVM-WSO it possesses 0.94.

Performance evaluation based on security is illustrated in **Table 6.2**. In this analyze, the security level of proposed frameworks is validated and compared with the previous methods such as Sparse-FCM, ANFIS and MRE-IDS. The Sparse-FCM, ANFIS, MRE-IDS, SVM-WSO and CNN-SO methods outperformed 78.54%, 80.30%, 89.43%, 95.89% and 97.6% security level. While comparing to other methods, the proposed method outperformed higher security level during intrusion detection in VANET.

Table 6.2: Performance evaluation based on security

Methods	**Level of security (%)**
Sparse-FCM	78.54%
ANFIS	80.30%
MRE-IDS	89.43%
SVM-WSO	95.89%
CNN-SO	97.6%

6.4. SUMMARY

This chapter discusses the comparative analysis result of proposed VANET intrusion detection model. The proposed methods such as (i) Investigation of intrusion detection system in vehicular ad-hoc networks is used to understand the existing researchers, (ii) An optimized convolutional neural network based privacy based collaborative intrusion detection system for vehicular ad hoc network and (iii) collaborative-based vehicular ad hoc network intrusion detection system using optimized support vector machine are compared and validated using different studies such as Fuzzy C-means (Sparse FCM) clustering algorithm, Adaptive Neuro-Fuzzy Inference System (ANFIS) modeling methods. However, the acquisition measures of Accuracy, precision, recall, detection rate, energy consumption, delay and throughput indicates the performances. The CNN-SO detection accuracy is 94.3%, 4.23J energy consumption, 10.67s delay, 0.94% Del ratio and 97.6% security level compared to the other methods like SVM-WSO, Sparse-FCM, ANFIS and MRE-IDS techniques.

CHAPTER 7
CONCLUSION AND FUTURE WORKS

7.1. CONCLUSION

This study represents a novel collaborative intrusion detection model in VANET. It has three phases such as (i) Investigation of intrusion detection system in vehicular ad-hoc networks, (ii) Collaborative-based vehicular ad hoc network intrusion detection system using an optimized support vector machine and (iii) Optimized convolution neural network based privacy collaborative intrusion detection system for vehicular ad hoc network. The proposed work's experimental findings are implemented in this work using a GPU-based computer based on NS-2 software with a GTX1050 GPU at 16GB RAM and an Intel Core i5-8300H CPU running TensorFlow 1.15. In this study, the KDD99 and https://www.kaggle.com/bigquery/ethereum-blockchain datasets are used for experimental analysis. The KDD99 dataset has five million records with 41 characteristics each. The blockchain-based security method improves security by ignoring hostile nodes and protecting information transmitted between the source and destination. A more reliable and secure replacement for conventional security measures is provided by blockchain technology. The integrity and security of data are ensured by its decentralized and transparent design, which makes it difficult for hackers to breach the system. The blockchain technology deployed in this study is used in the privacy-preserving VANET system techniques to mitigate attack risk and downtime might be avoided with the feature of distributed sharing and storage capacity. With the blockchain, the work's validity and integrity can continue forever. When compared to state-of-the-art approaches, performance matrices such as accuracy, precision, recall, detection rate, security, delay, and energy consumption are utilized to validate the proposed model's effectiveness, resulting in good and accurate results. The CNN-SO detection accuracy is 94.3%, 4.23J energy consumption, 10.67s delay, 0.94% Del ratio and 97.6% security level compared to the other methods like SVM-WSO, Sparse-FCM, ANFIS and MRE-IDS techniques.

7.1.1. Contribution Summary

This study analyzed the blockchain based Intrusion Detection System in VANET. It concluded with the three-phases of result given below.

- It identified various types of attacks in Intrusion Detection System in VANET.

- Collaborative based Vehicular Ad Hoc Network Intrusion Detection System using Optimized Support Vector Machine is used.
- It outlined an Optimized Convolutional Neural Network based Privacy Collaborative Intrusion Detection System for Vehicular Ad Hoc Network.

Keeping the above aspects into considerations, the research works of this study has been divided into three phases.

Phase I (Chapter 3: Investigation of Intrusion Detection Systems in Vehicular Ad Hoc Networks).

Phase II (Chapter 4: Collaborative based Vehicular Ad Hoc Network Intrusion Detection System using Optimized Support Vector Machine).

Phase III (Chapter 5: Optimized Convolutional Neural Network based Privacy Collaborative Intrusion Detection System for Vehicular Ad Hoc Network).

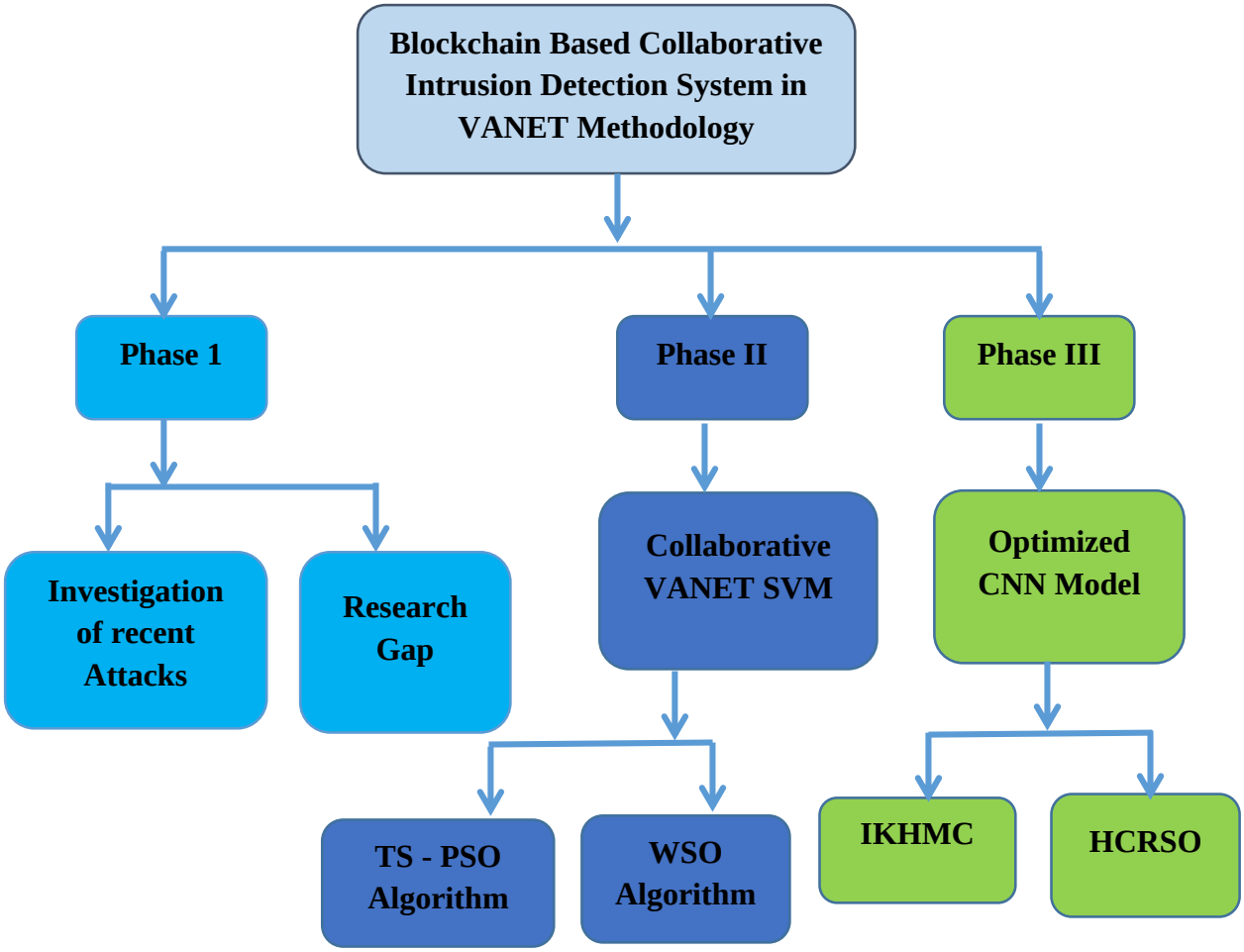


Figure 7.1: Flow chart for blockchain based collaborative intrusion detection system with appropriate methodology

Phase I – Investigation of Intrusion Detection System

Defamation activity in VANET is detected here. Comparison of certain intrusion detection systems are also included. This system needs to been updated regularly according to the development of the technologies.

Phase II – Collaborative based Vehicular Ad Hoc Network Intrusion Detection System using Optimized Support Vector Machine

Here, K-means algorithm and Tabu Search-based Particle Swarm Optimization (TS-PSO) algorithm are adopted to accomplish cluster formation and cluster head selection in VANET. The trust-based collaborative intrusion detection on the VANET can be performed using the innovative War Strategy Optimization (WSO) based Support Vector Machine (SVM) model (Optimized SVM).

Phase III – Optimized Convolutional Neural Network based Privacy Collaborative Intrusion Detection System for Vehicular Ad Hoc Network

In this phase, an improved K- harmonics mean clustering (IKHMC) and hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm are implemented to perform cluster formation and cluster head selection in VANET. After collaboration VANET intrusion detection is achieved with optimized CNN.

7.2. FUTURE WORKS

The contemporary VANET networks' use of several protocols and variety in their data results in a high level of complexity when spotting intrusions. To evaluate the trust of the entire VANET network, we need to integrate different attack results, which are often impossible to be achieved in real-time since a single node cannot collect a huge amount of security-related information. The solution identified by a centralized network often crashes if it is compromised or untrustworthy. In future, different kinds of attacks will detect using various kinds of deep learning techniques and encryption models for security. Another area is integrating the system with other technologies, such as artificial intelligence, to enable more sophisticated intrusion detection and response.

References

A. Ghaleb, F., Saeed, F., Al-Sarem, M., Ali Saleh Al-rimy, B., Boulila, W., Eljialy, A.E.M., Aloufi, K. and Alazab, M., 2020. Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET. Electronics, 9(9), p.1411.

Aboelfottoh, A.A. and Azer, M.A., (2022 May), Intrusion Detection in VANETs and ACVs using Deep Learning. In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 241-245). IEEE.

Akhter, A.S., Ahmed, M., Shah, A.S., Anwar, A. and Zengin, A., (2021), A secured privacy-preserving multi-level blockchain framework for cluster based VANET. Sustainability, 13(1), p.400.

Al Junaid, M.A.H., Syed, A.A., Warip, M.N.M., Azir, K.N.F.K. and Romli, N.H., 2018. Classification of security attacks in VANET: A review of requirements and perspectives. In MATEC web of conferences (Vol. 150, p. 06038). EDP Sciences.

Al Omar, A., Rahman, M.S., Basu, A. and Kiyomoto, S., 2017, December. Medibchain: A blockchain based privacy preserving platform for healthcare data. In International conference on security, privacy and anonymity in computation, communication and storage (pp. 534-543). Springer, Cham.

Al-Heety, O.S., Zakaria, Z., Ismail, M., Shakir, M.M., Alani, S. and Alsariera, H., (2020), A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. IEEE Access, 8, pp.91028-91047.

Ali, I. and Li, F., 2020. An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. Vehicular Communications, 22, p.100228.

Ali, L., Wajahat, I., Amiri Golilarz, N., Keshtkar, F. and Bukhari, S.A.C., 2021. LDA–GA–SVM: improved hepatocellular carcinoma prediction through dimensionality reduction and genetically optimized support vector machine. Neural Computing and Applications, 33(7), pp.2783-2792.

Alimohammadi, M. and Pouyan, A., 2014. Performance analysis of cryptography methods for secure message exchanging in VANET. International Journal of Scientific & Engineering Research, 5(2), p.912.

Alladi, T., Gera, B., Agrawal, A., Chamola, V. and Yu, F.R., 2021. DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANETs. IEEE Transactions on Vehicular Technology, 70(11), pp.12013-12023.

Alladi, T., Kohli, V., Chamola, V. and Yu, F.R., 2022. A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. Digital Communications and Networks.

Alrehan, A.M. and Alhaidari, F.A., 2019, May. Machine learning techniques to detect DDoS attacks on VANET system: a survey. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

Alsarhan, A., Alauthman, M., Alshdaifat, E., Al-Ghuwairi, A.R. and Al-Dubai, A., (2021), Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-10.

Alsarhan, A., Al-Ghuwairi, A.R., Almalkawi, I.T., Alauthman, M. and Al-Dubai, A., 2021. Machine learning-driven optimization for intrusion detection in smart vehicular networks. Wireless Personal Communications, 117(4), pp.3129-3152.

Alshammari, A., Zohdy, M.A., Debnath, D. and Corser, G., 2018. Classification approach for intrusion detection in vehicle systems. Wireless Engineering and Technology, 9(4), pp.79-94.

Amirat, H., Lagraa, N., Kerrach, C.A. and Ouinten, Y., 2018, October. Fuzzy clustering for misbehaviour detection in VANET. In 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT) (pp. 200-204). IEEE.

Aneja, M.J.S., Bhatia, T., Sharma, G. and Shrivastava, G., 2018. Artificial intelligence based intrusion detection system to detect flooding attack in VANETs. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 87-100). IGI Global.

Aneja, M.J.S., Bhatia, T., Sharma, G. and Shrivastava, G., 2018. Artificial intelligence based intrusion detection system to detect flooding attack in VANETs. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 87-100). IGI Global.

Annamalai, T., Anton, J.L. and Yoganathan, P., Secured data transmission for VANETS using CNN based trust aware clustering. Journal of Intelligent & Fuzzy Systems, (Preprint), pp.1-15.

Anyanwu, G.O., Nwakanma, C.I., Lee, J.M. and Kim, D.S., (2022), Optimization of RBF-SVM Kernel using Grid Search Algorithm for DDoS Attack Detection in SDN-based VANET. IEEE Internet of Things Journal.

Anzer, A. and Elhadef, M., 2018, October. A multilayer perceptron-based distributed intrusion detection system for internet of vehicles. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC) (pp. 438-445). IEEE.

Ayyarao, T.S., RamaKrishna, N.S.S., Elavarasan, R.M., Polumahanthi, N., Rambabu, M., Saini, G., Khan, B. and Alatas, B., 2022. War strategy optimization algorithm: a new effective metaheuristic algorithm for global optimization. IEEE Access, 10, pp.25073-25105.

Ayyarao, Tummala SLV, and Polamarasetty P. Kumar (2022), Parameter estimation of solar PV models with a new proposed war strategy optimization algorithm." International Journal of Energy Research 46, no. 6, 7215-7238.

Azam F, Kumar S, Yadav KP, Priyadarshi N, Padmanaban S. An outline of the security challenges in VANET. In2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) 2020 Nov 27 (pp. 1-6). IEEE.

Azizian, M., Cherkaoui, S. and Hafid, A.S., (2016), April. A distributed D-hop cluster formation for VANET. In 2016 IEEE wireless communications and networking conference (pp. 1-6). IEEE.

Bangui, H., Ge, M. and Buhnova, B., (2021), A hybrid data-driven model for intrusion detection in VANET. Procedia Computer Science, 184, pp.516-523.

Bangui, H., Ge, M. and Buhnova, B., (2022), A hybrid machine learning model for intrusion detection in VANET. Computing, 104(3), pp.503-531.

Baqer, M., & Krings, A. (2019). Reliability of VANET bicycle safety applications in malicious environments. 2019 27th Telecommunications Forum (TELFOR). doi:10.1109/telfor48224.2019.8971200.

Belenko, V., Krundyshev, V. and Kalinin, M., (2018), September. Synthetic datasets generation for intrusion detection in VANET. In Proceedings of the 11th international conference on security of information and networks (pp. 1-6).

Bensaber, B.A., Diaz, C.G.P. and Lahrouni, Y., 2020. Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET. Journal of Computational Science, 47, p.101234.

Bouabdellah, M., El Bouanani, F. and Ben-Azza, H., 2016, October. A secure cooperative transmission model in VANET using attribute based encryption. In 2016 international conference on advanced communication systems and information security (ACOSIS) (pp. 1-6). IEEE.

Braik, M., Sheta, A. and Al-Hiary, H., 2021. A novel meta-heuristic search algorithm for solving optimization problems: capuchin search algorithm. Neural computing and applications, 33(7), pp.2515-2547.

Canetti, R., Halevi, S. and Katz, J., 2004. Chosen-ciphertext security from identity-based encryption. In Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23 (pp. 207-222). Springer Berlin Heidelberg.

Cervantes, J., Garcia-Lamont, F., Rodríguez-Mazahua, L. and Lopez, A., 2020. A comprehensive survey on support vector machine classification: Applications, challenges and trends. Neurocomputing, 408, pp.189-215.

Chaudhary, Alka, Anil Kumar, and V. N. Tiwari. "A reliable solution against packet dropping attack due to malicious nodes using fuzzy logic in MANETs." 2014 International Conference on Reliability Optimization and Information Technology (ICROIT). IEEE, 2014b.

Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "A new intrusion detection system based on soft computing techniques using neuro fuzzy classifier for packet dropping attack in Manets." International Journal of Network Security 18.3 (2016): 514-522.

Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks." 2014 IEEE International Advance Computing Conference (IACC). IEEE, 2014a.

Cheng, H., Fei, X., Boukerche, A. and Almulla, M., 2015. GeoCover: An efficient sparse coverage protocol for RSU deployment over urban VANETs. Ad Hoc Networks, 24, pp.85-102.

Chougule, A., Kohli, V., Chamola, V. and Yu, F.R., 2022. Multibranch Reconstruction Error (MbRE) Intrusion Detection Architecture for Intelligent Edge-Based Policing in Vehicular Ad-Hoc Networks. IEEE Transactions on Intelligent Transportation Systems.

Chougule, A., Kohli, V., Chamola, V. and Yu, F.R., 2022. Multibranch Reconstruction Error (MbRE) Intrusion Detection Architecture for Intelligent Edge-Based Policing in Vehicular Ad-Hoc Networks. IEEE Transactions on Intelligent Transportation Systems.

Dadi, S. and Abid, M., 2022. Enhanced Intrusion Detection System Based on AutoEncoder Network and Support Vector Machine. In Networking, Intelligent Systems and Security (pp. 327-341). Springer, Singapore.

Dak, A.Y., Yahya, S. and Kassim, M., 2012. A literature survey on security challenges in VANETs. International Journal of Computer Theory and Engineering, 4(6), p.1007.

Deng, H., Zeng, Q.A. and Agrawal, D.P., (2003, October). SVM-based intrusion detection system for wireless ad hoc networks. In 2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484) (Vol. 3, pp. 2147-2151). IEEE.

Dhiman, G., Garg, M., Nagar, A., Kumar, V. and Dehghani, M., 2021. A novel algorithm for global optimization: rat swarm optimizer. Journal of Ambient Intelligence and Humanized Computing, 12(8), pp.8457-8482.

Dhiman, G., Singh, K.K., Soni, M., Nagar, A., Dehghani, M., Slowik, A., Kaur, A., Sharma, A., Houssein, E.H. and Cengiz, K., 2021. MOSOA: A new multi-objective seagull optimization algorithm. Expert Systems with Applications, 167, p.114150.

Dibaei, M., Zheng, X., Xia, Y., Xu, X., Jolfaei, A., Bashir, A.K., Tariq, U., Yu, D. and Vasilakos, A.V., 2021. Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey. IEEE Transactions on Intelligent Transportation Systems, 23(2), pp.683-700.

Duan, X., Liu, Y. and Wang, X., (2017), SDN enabled 5G-VANET: Adaptive vehicle clustering and beamformed transmission for aggregated traffic. IEEE Communications Magazine, 55(7), pp.120-127.

Elhoseny, M. and Shankar, K., (2020), Energy efficient optimal routing for communication in VANETs via clustering model. In Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks (pp. 1-14). Springer, Cham.

El-sadek, D.M., 2022. Solve global optimization problems based on metaheuristic algorithms. Bulletin of Faculty of Science, Zagazig University, 2022(3), pp.29-42.

Elsadig, M.A. and Fadlalla, Y.A., 2016. VANETs security issues and challenges: A survey. Indian Journal of Science and Technology, 9(28), pp.1-8.

Ercan, S., Ayaida, M. and Messai, N., 2021. Misbehavior detection for position falsification attacks in VANETs using machine learning. IEEE Access, 10, pp.1893-1904.

Fabian de Ponte Müller, 2017, Survey on Ranging Sensors and Cooperative Techniques for Relative Positioning of Vehicles, Sensors.

Fathy, A., Yousri, D., Rezk, H. and Ramadan, H.S., 2022. An efficient capuchin search algorithm for allocating the renewable based biomass distributed generators in radial distribution network. Sustainable Energy Technologies and Assessments, 53, p.102559.

Gad, A.R., Nashat, A.A. and Barkat, T.M., (2021), Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. IEEE Access, 9, pp.142206-142217.

Gonçalves, F., Macedo, J. and Santos, A., (2021 September), Evaluation of VANET Datasets in context of an Intrusion Detection System. In 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-6). IEEE.

Gonçalves, F., Macedo, J. and Santos, A., (2021), Intelligent Hierarchical Intrusion Detection System for VANETs. In 2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 50-59). IEEE.

Hamdi, M.M., Audah, L., Rashid, S.A., Mohammed, A.H., Alani, S. and Mustafa, A.S., 2020, June. A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs). In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-7). IEEE.

Hamed Alqahtani, Iqbal H., Sarker Asra Kalim, Syed Md. Minhaz Hossain ,Sheikh Ikhlaq, Sohrab Hossain "Cyber Intrusion Detection Using Machine Learning Classification Techniques" International Conference on Computing Science, Communication and Security COMS2 2020.

Hamza Nachan, Dristi Poddar, Sambhaji Sarode, Pratik Kumhar, "Intrusion Detection System: A Survey", International Journal of Engineering Research & Technology, Vol. 10, Issue 05, May 2021.

Hasrouny, Hamssa, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti (2017), "VANet security challenges and solutions: A survey." Vehicular Communications 7, 7-20.

Horng, S.J., Lu, C.C. and Zhou, W., 2020. An identity-based and revocable data-sharing scheme in VANETs. IEEE Transactions on Vehicular Technology, 69(12), pp.15933-15946.

Hortelano, J., Ruiz, J.C. and Manzoni, P., (2010), May. Evaluating the usefulness of watchdogs for intrusion detection in VANETs. In 2010 IEEE international conference on communications workshops (pp. 1-5). IEEE.

Huang, D. and Verma, M., 2009. ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks. Ad Hoc Networks, 7(8), pp.1526-1535.

Hussain, R., Hussain, F. and Zeadally, S., (2019), Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems, 101, pp.843-864.

Hussain, R., Rezaeifar, Z., Lee, Y.H. and Oh, H., 2015. Secure and privacy-aware traffic information as a service in VANET-based clouds. Pervasive and Mobile Computing, 24, pp.194-209.

Indira, K. and Joy, E.C., 2015. Energy efficient IDS for cluster-based VANETS. Asian Journal of Information Technology, 14(1), pp.37-41.

J. Liang, J. Chen, Y. Zhu, and R. Yu, “A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position”, Applied Soft Computing, 75, 712-727, 2019.

Jabar Mahmood, Zongtao Duan, Heng Xue 2021, Secure Message Transmission for V2V Based on Mutual Authentication for VANETs, Volume 2021, Wireless Communications and Mobile Computing.

Jayesh Surana, Jagrati Sharma, Ishika Saraf, Nishima Puri, Bhavana Navin, “A Survey on Intrusion Detection System”, International Journal of Engineering Develoment and Research, Vol.5, Issue 2, 2017.

K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, “Hybrid Algorithm to Detect DDoS Attacks in VANETs”. Wireless Personal Communications, 114(4), 3613-3634, 2020.

Kadam, N. and Krovi, R.S., 2021. Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET. International Journal of Advanced Computer Science and Applications, 12(7).

Kanazawa, S., Sugiyama, Y., Yang, T. and Goto, M., 2019. A Study of Feature Clustering Analysis based on the Hidden Layer Representation of an Autoencoder. Total Quality Science, 5(1), pp.11-22.

Kaur, G. and Kakkar, D., (2022). Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET. Ad Hoc Networks, 136, p.102961.

Kebande, V.R., Karie, N.M. and Ikuesan, R.A., (2021), Real-time monitoring as a supplementary security component of vigilantism in modern network environments. International Journal of Information Technology, 13(1), pp.5-17.

Khan, A.A., Abolhasan, M. and Ni, W., (2018), An evolutionary game theoretic approach for stable and optimized clustering in VANETs. IEEE Transactions on Vehicular Technology, 67(5), pp.4501-4513.

Khan, A.R., Jamlos, M.F., Osman, N., Ishak, M.I., Dzaharudin, F., Yeow, Y.K. and Khairi, K.A., 2022. DSRC technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT system for Intelligent Transportation System (ITS): a review. Recent Trends in Mechatronics towards Industry 4.0, pp.97-106.

Khayat, G., Mavromoustakis, C.X., Mastorakis, G., Batalla, J.M., Maalouf, H. and Pallis, E., (2020), VANET clustering based on weighted trusted cluster head selection. In 2020

International Wireless Communications and Mobile Computing (IWCMC) (pp. 623-628). IEEE.

Kolandaisamy, R., Noor, R.M., Kolandaisamy, I., Ahmedy, I., Kiah, M.L.M., Tamil, M.E.M. and Nandy, T., (2021), A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. Journal of Ambient Intelligence and Humanized Computing, 12(6), pp.6599-6612.

Krishna, A.M. and Tyagi, A.K., 2020, February. Intrusion detection in intelligent transportation system and its applications using blockchain technology. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-8). IEEE.

Kudva, S., Badsha, S., Sengupta, S., La, H., Khalil, I. and Atiquzzaman, M., 2021. A scalable blockchain based trust management in VANET routing protocol. Journal of Parallel and Distributed Computing, 152, pp.144-156.

Kumar, N. and Chilamkurti, N., 2014. Collaborative trust aware intelligent intrusion detection in VANETs. Computers & Electrical Engineering, 40(6), pp.1981-1996.

Li, H., Pei, L., Liao, D., Chen, S., Zhang, M. and Xu, D., 2020. FADB: A fine-grained access control scheme for VANET data based on blockchain. IEEE Access, 8, pp.85190-85203.

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

Li, Z., Liu, F., Yang, W., Peng, S. and Zhou, J., 2021. A survey of convolutional neural networks: analysis, applications, and prospects. IEEE transactions on neural networks and learning systems.

Liang, J., Ma, M. and Tan, X., 2021. GaDQN-IDS: A Novel Self-Adaptive IDS for VANETs Based on Bayesian Game Theory and Deep Reinforcement Learning. IEEE Transactions on Intelligent Transportation Systems.

Lihua, L., (2022). Energy-Aware Intrusion Detection Model for Internet of Vehicles Using Machine Learning Methods. Wireless Communications and Mobile Computing, 2022.

Lihua, L., 2022. Energy-Aware Intrusion Detection Model for Internet of Vehicles Using Machine Learning Methods. Wireless Communications and Mobile Computing, 2022.

Limbasiya, T. and Das, D., 2016, November. Secure message transmission algorithm for Vehicle to Vehicle (V2V) communication. In 2016 IEEE Region 10 Conference (TENCON) (pp. 2507-2512). IEEE.

Lipowsky, F., Rakoczy, K., Pauli, C., Drollinger-Vetter, B., Klieme, E. and Reusser, K., 2009. Quality of geometry instruction and its short-term impact on students' understanding of the Pythagorean Theorem. Learning and instruction, 19(6), pp.527-537.

M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh,. "An intrusion detection system for connected vehicles in smart cities". Ad Hoc Networks, 90, 101842, 2019.

M. Zhou, L. Han, H. Lu, and C. Fu, "Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant". Computer Networks, 172, 107174, 2020.

Ma, Z., Zhang, J., Guo, Y., Liu, Y., Liu, X. and He, W., 2020. An efficient decentralized key management mechanism for VANET with blockchain. IEEE Transactions on Vehicular Technology, 69(6), pp.5836-5849.

Maan, U. and Chaba, Y., (2021), Accurate cluster head selection technique for software defined network in 5G VANET. Wireless Personal Communications, 118(2), pp.1271-1293.

Mahalakshmi, G. and Uma, E., 2020. Machine Learning based Feature Selection for Intrusion Detection System in VANET. In International Conference on Artificial Intelligence, Network Security and Data Science (IeCAN).

Mahbooba, B., Timilsina, M., Sahal, R. and Serrano, M., 2021. Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model. Complexity, 2021.

Mamdoohi, S. and Miller-Hooks, E., 2022. Identifying the Impact Area of a Traffic Event Through k-Means Clustering. Journal of Big Data Analytics in Transportation, pp.1-18.

Mehmood, A., Khanan, A., Mohamed, A.H.H., Mahfooz, S., Song, H. and Abdullah, S., (2017), ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET. IEEE Access, 6, pp.4452-4461.

Meshcheryakov, Y., Melman, A., Evsutin, O., Morozov, V. and Koucheryavy, Y., 2021. On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices. IEEE Access, 9, pp.80559-80570.

Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan, "Intrusion Detection System", International Journal of Technical Research and Applications, Volume 5, Issue 2 (March - April 2017).

Mu, D., Ge, X. and Chai, R., 2013, October. Vertical handoff modeling and simulation in VANET scenarios. In 2013 International Conference on Wireless Communications and Signal Processing (pp. 1-6). IEEE.

Muthumeenakshi, R., 2022. An adaptive approach for cluster-based intrusion detection in VANET. International Journal of Bio-Inspired Computation, 20(1), pp.58-69.

Nandy, T., Noor, R.M., Idris, M.Y.I.B. and Bhattacharyya, S., (2020), February. T-BCIDS: Trust-based collaborative intrusion detection system for VANET. In 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA) (pp. 1-5). IEEE.

Narayanan, P.S. and Joice, C.S., 2019, March. Vehicle-to-vehicle (V2V) communication using routing protocols: a review. In 2019 International Conference on Smart Structures and Systems (ICSSS) (pp. 1-10). IEEE.

Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J. and Li, Y., 2020. Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method. IEEE Transactions on Network Science and Engineering, 7(4), pp.2219-2230.

Nie, L., Wang, H., Gong, S., Ning, Z., Obaidat, M.S. and Hsiao, K.F., 2019, December. Anomaly detection based on spatio-temporal and sparse features of network traffic in VANETs. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

Noh, J., Jeon, S., & Cho, S. (2020). Distributed blockchain-based message authentication scheme for connected vehicles. Electronics, 9(1), 74. doi:10.3390/electronics9010074.

Palas, M.R., Islam, M.R., Roy, P., Razzaque, M.A., Alsanad, A., AlQahtani, S.A. and Hassan, M.M., 2021. Multi-criteria handover mobility management in 5G cellular network. Computer Communications, 174, pp.81-91.

Paliwal, S., Cherukuri, A.K. and Gao, X.Z., 2022. Dynamic private modulus based password conditional privacy preserving authentication and key-agreement protocol for VANET. Wireless Personal Communications, 123(3), pp.2061-2088.

Panagant, N., Pholdee, N., Bureerat, S., Kaen, K., Yıldız, A.R. and Sait, S.M., 2020. Seagull optimization algorithm for solving real-world design optimization problems. Materials Testing, 62(6), pp.640-644.

Punal, O., Pereira, C., Aguiar, A. and Gross, J., 2014. Experimental characterization and modeling of RF jamming attacks on VANETs. IEEE transactions on vehicular technology, 64(2), pp.524-540.

Qian, M., Wang, Y., Zhou, Y., Tian, L. and Shi, J., 2015. A super base station based centralized network architecture for 5G mobile communication systems. Digital communications and Networks, 1(2), pp.152-159.

R. G. Engoulou, M. Bellaíche, S. Pierre, A. Quintero, "VANET security surveys". Computer Communications, vol. 44, pp. 1–13, 2014.

R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah, M. E. M., Tamil, and T. Nandy, "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET". Journal of Ambient Intelligence and Humanized Computing, 1-14, 2020.

R. Nandakumar K. Nirmala "Security Challenges in Mobile Ad Hoc Networks - A Survey" Australian Journal of Basic and Applied Sciences, Vol. 10(1), pp. 654-659, January 2016.

Raja, G., Anbalagan, S., Vijayaraghavan, G., Theerthagiri, S., Suryanarayan, S.V. and Wu, X.W (2020), SP-CIDS: Secure and private collaborative IDS for VANETs. IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4385-4393.

Ramalingam, M. and Thangarajan, R., 2020. Mutated k-means algorithm for dynamic clustering to perform effective and intelligent broadcasting in medical surveillance using selective reliable broadcast protocol in VANET. Computer Communications, 150, pp.563-568.

Raw, R.S. and Das, S., 2011. Performance comparison of Position based routing Protocols in vehicle-to-vehicle (V2V) Communication. International Journal of Engineering Science and Technology, 3(1), pp.435-444.

Ren, M., Khoukhi, L., Labiod, H., Zhang, J. and Veque, V., (2017), A mobility-based scheme for dynamic clustering in vehicular ad-hoc networks (VANETs). Vehicular Communications, 9, pp.233-241.

Sajini, S., Anita, E.A. and Janet, J., 2022. Improved Security of the Data Communication in VANET Environment Using ASCII-ECC Algorithm. Wireless Personal Communications, pp.1-18.

Saleem, M.A., Zhou, S., Sharif, A., Saba, T., Zia, M.A., Javed, A., Roy, S. and Mittal, M., (2019), Expansion of cluster head stability using fuzzy in cognitive radio CR-VANET. IEEE Access, 7, pp.173185-173195.

Santhosh Kumar, S.V.N., Palanichamy, Y., Selvi, M., Ganapathy, S., Kannan, A. and Perumal, S.P., 2021. Energy efficient secured K means based unequal fuzzy clustering

algorithm for efficient reprogramming in wireless sensor networks. Wireless Networks, 27(6), pp.3873-3894.

Schmidt, D.A., Khan, M.S. and Bennett, B.T., (2019 April), Spline based intrusion detection in vehicular ad hoc networks (VANET). In 2019 SoutheastCon (pp. 1-5). IEEE.

Schmidt, D.A., Khan, M.S. and Bennett, B.T., 2020. Spline-based intrusion detection for VANET utilizing knot flow classification. Internet Technology Letters, 3(3), p.e155.

Sengupta, S., Basak, S. and Peters, R.A., 2018. Particle Swarm Optimization: A survey of historical and recent developments with hybridization perspectives. Machine Learning and Knowledge Extraction, 1(1), pp.157-191.

Sharma, D., Gupta, S.K., Rashid, A., Gupta, S., Rashid, M. and Srivastava, A., 2021. A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. Transactions on Emerging Telecommunications Technologies, 32(7), p.e4114.

Sharma, S. and Kaul, A., 2018. Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET. Vehicular Communications, 12, pp.23-38.

Shu, J., Zhou, L., Zhang, W., Du, X. and Guizani, M., (2020), Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach. IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4519-4530.

Shu, J., Zhou, L., Zhang, W., Du, X. and Guizani, M., 2020. Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach. IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4519-4530.

Singh, G. and Khare, N., 2022. A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. International Journal of Computers and Applications, 44(7), pp.659-669.

So, S., Sharma, P. and Petit, J., 2018, December. Integrating plausibility checks and machine learning for misbehavior detection in VANET. In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 564-571). IEEE.

Soni, G., Chandravanshi, K., Jhariya, M.K. and Rajput, A., 2022. An IPS approach to secure V-RSU communication from blackhole and wormhole attacks in VANET. In Contemporary Issues in Communication, Cloud and Big Data Analytics (pp. 57-65). Springer, Singapore.

Soni, M., Rajput, B.S., Patel, T. and Parmar, N., 2021. Lightweight vehicle-to-infrastructure message verification method for VANET. In Data Science and Intelligent Applications (pp. 451-456). Springer, Singapore.

Subba, B., Biswas, S. and Karmakar, S., (2018). A game theory based multi layered intrusion detection framework for VANET. Future Generation Computer Systems, 82, pp.12-28.

Subhash Waskle, Lokesh Parashar and Upendra Singh "Intrusion Detection System Using PCA with Random Forest Approach" International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020.

Sultana, R., Grover, J., Meghwal, J. and Tripathi, M., 2022. Exploiting machine learning and deep learning models for misbehavior detection in VANET. International Journal of Computers and Applications, pp.1-15.

Syed Mohd Faisal and Taskeen Zaidi, 2020, Timestamp Based Detection of Sybil Attack in VANET, International Journal of Network Security.

T. Nandy, R. M. Noor, M. Y. I. B. Idris, and S. Bhattacharyya, ""TBCIDS: Trust-Based Collaborative Intrusion Detection System for VANET". 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA) (pp. 1-5). IEEE.0, February 2020.

Tahir Mehmood and Helmi B Md Rais, "Machine Learning Algorithms in Context of Intrusion Detection" 3rd International Conference on Computer and Information Sciences (ICCOINS), 2016.

Türkoğlu, M., Polat, H., Koçak, C. and Polat, O., 2022. Recognition of DDoS Attacks on SD-VANET Based on Combination of Hyperparameter Optimization and Feature Selection. Expert Systems with Applications, p.117500.

Ucar, S., Ergen, S.C. and Ozkasap, O., (2015), Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination. IEEE Transactions on Vehicular Technology, 65(4), pp.2621-2636.

Vitalkar, R.S., Thorat, S.S. and Rojatkar, D.V., 2022. Intrusion detection for vehicular ad hoc network based on deep belief network. In Computer Networks and Inventive Communication Technologies (pp. 853-865). Springer, Singapore.

Wang, B. and Ho, P.H., 2016. Energy-efficient routing and bandwidth allocation in OFDM-based optical networks. Journal of Optical Communications and Networking, 8(2), pp.71-84.

Wantoro, J. and Mustika, I.W., 2014, November. M-aodv+: an extension of aodv+ routing protocol for supporting vehicle-to-vehicle communication in vehicular ad hoc networks. In 2014 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT) (pp. 39-44). IEEE.

Waters, B., 2005. Efficient identity-based encryption without random oracles. In Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24 (pp. 114-127). Springer Berlin Heidelberg.

Xu, X., Wang, Y. and Wang, P., 2022. Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks. Journal of Advanced Transportation, 2022.

Yamashita, Rikiya, Mizuho Nishio, Richard Kinh Gian Do, and Kaori Togashi. "Convolutional neural networks: an overview and application in radiology." Insights into imaging 9, no. 4 (2018): 611-629.

Yu, X., Guo, H. and Wong, W.C., 2011, July. A reliable routing protocol for VANET communications. In 2011 7th international wireless communications and mobile computing conference (pp. 1748-1753). IEEE.

Yu, Y., Zeng, X., Xue, X. and Ma, J., (2022). LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection. IEEE Transactions on Intelligent Transportation Systems.

Yu, Y., Zeng, X., Xue, X. and Ma, J., 2022. LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection. IEEE Transactions on Intelligent Transportation Systems.

Zaidi, K., Milojevic, M.B., Rakocevic, V., Nallanathan, A. and Rajarajan, M., (2015), Host-based intrusion detection for VANETs: A statistical approach to rogue node detection. IEEE transactions on vehicular technology, 65(8), pp.6703-6714.

Zebiri, I., Zeghida, D. and Redjimi, M., 2022. Rat Swarm Optimizer for Data Clustering. Jordanian Journal of Computers and Information Technology (JJCIT), 8(03).

Zendehboudi, A., Baseer, M.A. and Saidur, R., 2018. Application of support vector machine models for forecasting solar and wind energy resources: A review. Journal of cleaner production, 199, pp.272-285.

Zeng, N., Qiu, H., Wang, Z., Liu, W., Zhang, H. and Li, Y., 2018. A new switching-delayed-PSO-based optimized SVM algorithm for diagnosis of Alzheimer's disease. Neurocomputing, 320, pp.195-202.

Zeng, Y., Qiu, M., Ming, Z. and Liu, M., 2018, December. Senior2local: A machine learning based intrusion detection method for vanets. In International conference on smart computing and communication (pp. 417-426). Springer, Cham.

Zhang, G., Li, Y. and Deng, X., 2020. K-means clustering-based electrical equipment identification for smart building application. Information, 11(1), p.27.

Zhang, T. and Zhu, Q., 2018. Distributed privacy-preserving collaborative intrusion detection systems for VANETs. IEEE Transactions on Signal and Information Processing over Networks, 4(1), pp.148-161.

Zhang, Z., Beck, M.W., Winkler, D.A., Huang, B., Sibanda, W. and Goyal, H., 2018. Opening the black box of neural networks: methods for interpreting neural network models in clinical applications. Annals of translational medicine, 6(11).

Zhou, J., Cao, Z., Qin, Z., Dong, X. and Ren, K., 2019. LPPA: Lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs. IEEE Transactions on Information Forensics and Security, 15, pp.420-434.

Zhou, J., Qiu, Y., Zhu, S., Armaghani, D.J., Li, C., Nguyen, H. and Yagiz, S., 2021. Optimization of support vector machine through the use of metaheuristic algorithms in forecasting TBM advance rate. Engineering Applications of Artificial Intelligence, 97, p.104015.

Zhou, M., Han, L., Lu, H. and Fu, C., (2020). Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant. Computer Networks, 172, p.107174.

Appendix A
Used Datasets Description

A.1 Collaborative based Vehicular Ad Hoc Network Intrusion Detection System using Optimized Support Vector Machine & Optimized Convolutional Neural Network based Privacy Collaborative Intrusion Detection System for Vehicular Ad Hoc Network.

The KDD99 and https://www.kaggle.com/bigquery/ethereum-blockchain datasets are utilized in this study for experimental analysis. The KDD99 dataset consists of five million records that are described by 41 features.

List of Publications

Journal Papers

1. M. Azath and V. Singh, “Collaborative based vehicular ad-hoc network intrusion detection system using optimized support Vector Machine,” International Journal of Advanced Computer Science and Applications, E-ISSN: 2156-5570, Print ISSN: 2158-107X, vol. 14, no. 3, 2023. doi:10.14569/ijacsa.2023.0140327 **(ESCI & Scopus Indexed).**
2. M. Azath and V. Singh, “Optimized convolutional neural network based privacy based collaborative intrusion detection system for Vehicular Ad Hoc Network,” International Journal of Electrical and Electronics Engineering, E-ISSN: 2348-8379, vol. 10, no. 2, pp. 143–156, 2023. doi:10.14445/23488379/ijeee-v10i2p114 **(Scopus Indexed).**
3. M. Azath and V. Singh, “An approach to preventing vehicular ad-hoc networks from malicious nodes based on blockchain,” Review of Computer Engineering Research, Print ISSN: 2412-4281, E-ISSN: 2410-9142, vol. 10, no. 1, pp. 16–27, 2023. doi:10.18488/76.v10i1.3324 **(Scopus Indexed).**

Conference Papers

1. M. Azath, Vaishali Singh, “Investigation of Intrusion Detection Systems in Vehicular Ad-Hoc Networks”, International Conference on Advanced Communication Control and Computing Technology (ICACCCT), 28-30 June 2022.